Fingerprint Recognition

Maria Villa and Abhishek Verma

CONTENTS

9.1 FINGERPRINT RECOGNITION IN MOBILE DEVICES

This chapter highlights the most important mechanisms for fingerprint liveness recognition in mobile phones. The structure of this chapter is as follows: Section 9.2 introduces a general definition and an overview of fingerprint recognition methods. Public databases for fingerprint recognition are presented in Section 9.3. Section 9.4 details liveness detection on fingerprints and discusses the following techniques: pore detection,

perspiration, skin deformation, image quality, temperature, and skin resistance. Finally, the conclusions are drawn in Section 9.5.

9.2 INTRODUCTION

Fingerprint recognition has been considered the most efficient, popular, and widely acceptable identification method [1]. Currently, it is indisputably the most reliable evidence in the court of law [2]. Fingerprints are unique, not even identical twins have the same set of ridges and lines. Fingerprints stay the same from time one is born until death. This distinctiveness makes fingerprints one of the best ways to identify an individual [3].

Per the *Encyclopedia Britannica* fingerprints are "impressions made by the papillary ridges on the ends of the fingers and thumbs" [4]. The practice of fingerprinting as a means of identification is also known as dactyloscopy and is widely used in current law enforcement [4]. Sweat pores are located on each ridge of the epidermis which is anchored to the dermis by papillae [4]. The fingerprints have patterns that look like loops, arches, or whorls. These forms and outlines evolved onto eight basic patterns, which are still used by the FBI today [5]. The eight patterns can be observed on Figure 9.1. The distribution in the population of the fingerprint patterns is described as follows: 65% have loops, 30% have whorls, and 5% have arches. The most frequent pattern is the ulnar loop [5].

Fingerprinting methods have some challenges, however, they are still very popular and widely used. Numerous fingerprinting methods and

| Plain arch | Tented arch | Ulnar loop | Radial loop |

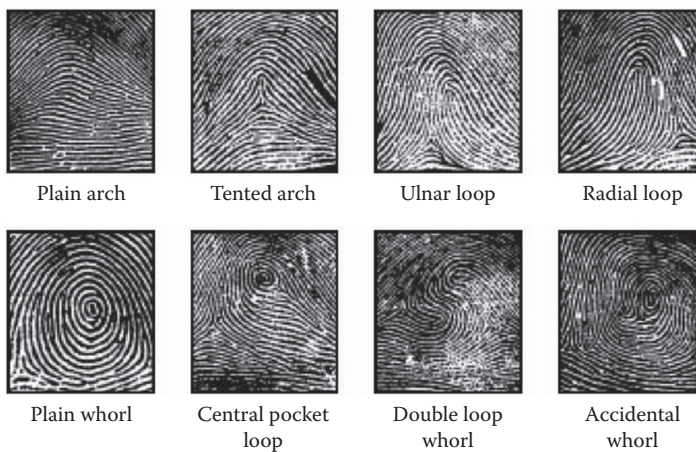| Plain whorl | Central pocket loop | Double loop whorl | Accidental whorl |

FIGURE 9.1   Fingerprint patterns. (From viewzone.com.)

enhancements are under development. Some advantages and disadvantages prepared are listed as follows [6]:

Advantages	Disadvantages
• Very high accuracy • Is the most economical biometric PC user authentication technique • It is one of the most developed biometrics • Easy to use • Small storage space required for the biometric template, reducing the size of the database memory required • It is standardized	• It is considered an intrusive method for some people as it seems related to criminal investigations • It can make mistakes with the dryness or dirty of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly) • Image captured at 500 dots per inch (dpi). Resolution: 8 bits per pixel demands a large memory space

Biometric fingerprint recognition is used in several important areas such as forensics, government, immigration border control, identification cards, commercial applications, credit cards, computer login access, and more [1]. Identifying fingerprints can be performed with hardware or software. Hardware methods capture characteristics of life such as temperature, electrical conductivity, and pulse oximetry. Furthermore, hardware systems require additional hardware to be connected and integrated to the biometric sensors. Conversely, software base fingerprint liveness detection uses a "static" approach. This means that a single fingerprint is used and features of multiple frames of the same fingerprint are analyzed [7].

Biometric fingerprint systems can be misled. An attacker may gain entry into a fingerprint system using a false fingerprint sample, this is known as a "spoof attack" [8]. There are numerous methods of fingerprint forgery. For the most part, the moisture-based approach has been able to deceive many fingerprint-based identification systems [1].

Synthetic fingerprints can be produced by two methods: (1) the cooperative process and the (2) noncooperative process.

1. *Cooperative process.* In the cooperative method, the individual presses his finger into a molding material, then the mold is filled with a gelatin-like substance [9]. Creating a fake finger with Play-Doh is economical, simple, and easily available. First, the finger is wrapped around with Play-Doh to create a cast. The cast will then be filled with liquid silicon, gelatin, silicon rubber, wax, or clay and

FIGURE 9.2   Play-Doh method. (Photo by biometricbits.com.)

is let dry for a couple of hours [1,9]. The spoofed fingerprint is now a replica of the original one [10]. See an example in Figure 9.2.

2. *The noncooperative process.* The inherent fingerprint is left on a surface in the noncooperative method [9]. In order to obtain a sample of the fingerprint, the surface is enhanced, digitized with a photograph, then the negative is printed on a transparency sheet. The resulted printed image can be used as a mold to duplicate the fingerprint [9]. In the non-cooperative approach, it has been reported that dissected fingers have been used to gain access to systems. BBC News in Malaysia informed that members of a violent gang chopped off a car owner's finger with a machete to steal a Mercedes S-class car, worth about $75,000 [11].

Fingerprint recognition is growing, and along with this growth the use of false fingerprints continues to threaten the security of fingerprint authentication systems. The remarkable popularity fingerprint authentication has gained with mobile phones makes cellphones' users a significant target of spoofing attacks. Ongoing solutions rely upon liveness detection as the main "anti-spoofing mechanism" [7].

9.3 PUBLIC DATABASES FOR FINGERPRINT RECOGNITION

9.3.1 LivDet

An important database used for the creation of liveness detection biometric mechanisms is LivDet Databases. Liveness Detection Competition

(livDet.org) organizes a competition every year. The organizers provide biometric fingerprint and iris databases for the competitors. The database contains a total of 17,000 images with "live" and "spoof" fingerprints. The samples are acquired with four different sensors listed below [7]:

- *Biometrika FX2000.* Optical sensor with 569 dpi resolution and 312×372 pixels image size.

- *Italdata ET10.* Optical sensor with 500 dpi resolution and 640×480 pixels image size.

- *Crossmatch L Scan Guardian.* Optical scanner with 500 dpi resolution and 800×750 pixels image size.

- Swipe sensor with 96.

The purpose of the competition is to increase the probability to develop high biometric security mechanisms [7].

9.3.2 CASIA-FingerprintV5

CASIA-FingerprintV5 is a public fingerprint database sponsored by Biometrics Ideal Test (BIT) in China. The database is used for research and educational purposes. This database has the fingerprints of about 500 volunteers (students, workers, waiters, graduate students, and more) adding up to about 20,000 fingerprint images. These images were obtained using a URU4000 fingerprint sensor [12]. BIT focuses on facilitating biometrics research and development to researchers and organizes competitions on fingerprint recognition among other biometrics.

9.3.3 Repository for Individuals of Special Concern

The FBI implemented the Repository for Individuals of Special Concern (RISC), a mobile system to check for fingerprints of suspects. This system is part of the Next Generation Identification system. RISC is free, but agencies provide their own mobile devices to obtain the fingerprints [13]. Law enforcement officers use the RISC system to match the fingerprints against a national registry of about 2.5 million sets of fingerprints [14]. RISC's registry includes

- Wanted Persons including the Immigration Violator File

- National Sexual Offender Registry Subjects

- Known or Suspected Terrorists

- Other Persons of Special Interest

RISC is distinguished for quick identification. It only takes 10 s for the system to send a response to the officer [14]. The responses are red = highly probable, yellow = possible, and green = no candidate in RISC. RISC's official flyer for the FBI [13] reports a success story of the mobile fingerprint identification system. An individual was wanted by the Gwinnett county sheriff's office in Georgia for murder and aggravated assault. He had an outstanding warrant for 8 years and was finally arrested when stopped by an officer for driving with headlights off.

9.4 LIVENESS DETECTION ON FINGERPRINTS

One method to detect spoofed fingerprints is by reading the physiological signs of life (liveness or vitality detection) on templates for enrollment, verification, and identification into biometric systems [1]. A system designed to protect against attacks with spoofed fingerprints must also check if the presented biometric sample matches with the sample originally enrolled in the system. Most biometric systems today have a decision process which first checks liveness [16]:

if data = live

perform acquisition and extraction

else if data = not live

do not perform acquisition and extraction

Some physiological features that can be monitored to detect the physiological signs of life are perspiration, pulsation detection, pulse oximetry, temperature sensing, electrical conductivity, EGC, active sweat pores, and among other attributes [1,10].

- *Perspiration*. Detects the change of moisture level in areas around the sweat pores which spread across the ridges over some time [1,13]. Perspiration is also known as sweat. Sweat is a dilute sodium chloride solution secreted by the sweat glands of the skin on to the surface of the skin through small pores. In live fingers, the perspiration

starts from the pores then diffuses along the ridges during time. This makes the semidry areas among the pores moister or darker in an image. The human skin has about 600 sweat glands per square inch. The perspiration process does not occur in cadavers or artificial fingerprints [17].

- *Pulsation detection*. The pulsation detection focuses in the fine movements of the skin. Pulsation differs from person to person, the emotional state, and previous activity. A normal pulse rate ranges between 200 and 220 heart beats per minute [13]. Changes in the pulse generate problems [17].

- *Pulse oximetry*. Measures the saturation of oxygen in hemoglobin and the heart pulse of the tip of the finger. The blood oxygenation involves hardware with two light sources: infrared (940 nm) and red (550 nm) [13]. Recognition of pulse oximetry can be tricked by means of a translucent false fingerprint, for example, one made with gelatin, on top of an impostor's live finger. The pulse oximetry will measure the saturation of oxygen of hemoglobin in the blood of the trespasser's finger [17].

- *Temperature sensing*. The average temperature of the human epidermis in fingertips ranges between 26°C and 30°C [13]. This is a simple method, however, some physiological variation in persons may make this method difficult to detect liveness. For example, a person with poor blood circulation can change the body's temperature and the finger sensor may read a wrong vitality signal [18].

- *Electrical conductivity*. Measures the dielectric constant property of human living skin [13]. The conductivity or resistance in human skin depends on the humidity. Humidity is also dependent on the person's biological characteristics and the environment. For example, some persons have dry fingers and others have sweaty ones. The seasons also affect the moisture [18]. Live fingers have a 16% moisture level whereas a gelatin fingerprint has a 23% [17]. The difference in moisture level between gelatin fingerprints and living fingers is insignificant enough to be able to fool sensors with gelatin prints [17].

- *Active sweat pores*. The pores discharge sweat fluid drops as part of a thermoregulation process. The openings and closing of the sweat

pores can be used for liveness detection in fingerprint images [1]. A fingerprint sensor with a very high resolution camera can capture the sweat pores in a fingerprint [17]. Those details might be very difficult to reproduce in an artificial fingerprint. Intraridge pores can be made with gelatin, but not good enough to reproduce the exact size and position of the pores on the mold and the print [17].

Fingerprint liveness detection can be grouped in five categories: (1) pore detection-based, (2) skin deformation-based, (3) image quality-based, (4) perspiration-based, and (5) combined approaches [10]. In this section, we describe some emerging approaches of fingerprint liveness detection that include one or more of the previously listed categories.

9.4.1 Pore Detection-Based

Pore detection-based procedures sense pores as a sign of fingerprint liveliness. Usually, the detection of pores encompasses locating the pores' position and the extraction of active sweat pores [10]. Other methods use pore quantity to distinguish between a query image and a reference image (real or false) [10]. The pore detection process is usually combined with the perspiration-based approach.

9.4.2 Perspiration-Based

Perspiration-based fingerprint detection schemes study perspiration shapes existing in the fingerprint. Pores are defined as the "openings of subcutaneous eccrine sweat glands located in the epidermis" [1]. A pore detection-based approach aims to distinguish active pores from inactive ones. Active pores tend to be bigger than inactive finger pores by a factor of 5–10. Moreover, active pores discharge sweat fluid drops [1] as can be seen in Figure 9.3 (sweat fluid).

Liveness detection for pores in fingerprints can be performed by various methods. Some methods are as follows:

- *Fingerprint pore extraction* aims to locate the sweat pores in fingerprint images and uses the location as a unique identification [20].

- *Pores and ridge contours extraction* in which wavelength transform and Gabor filters are used to extract the pores with ridge counters [21].

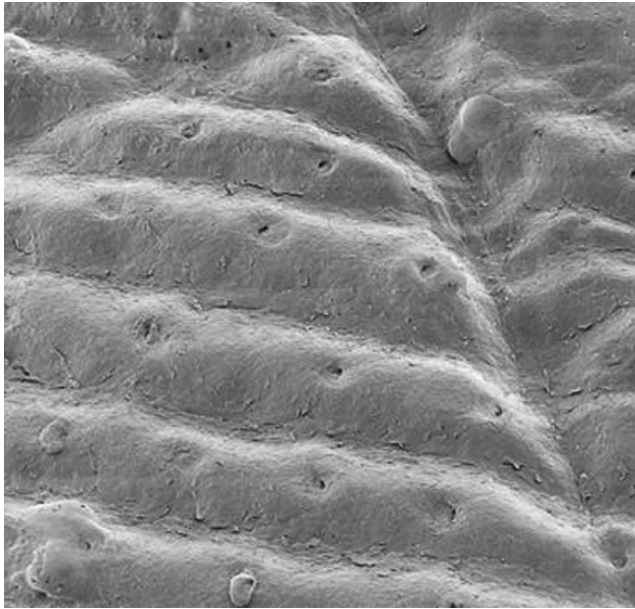- *Analysis of pore's location* analyzes the distribution of pores [22].

FIGURE 9.3   Sweat pores with fluid in ridges. (From Wordpress, image of pore.)

A method proposed by Memon, Manivannan, and Balachandran implements an advanced image processing algorithm named high-pass and correlation filtering (HCFA) [1]. HCFA uses high-pass filtering from the image of a fingerprint and then performs a correlation filtering and then binarization [1].

The HCFA first takes an original color image of high resolution of at least 800 dpi. Then, the image is converted into gray scale, inverted, and normalized. This enhanced image is passed through a high-pass filter stage which uses a high-pass filter transfer function [1]. Once the image is passed through the filter, the low frequency ridge-valley structures are removed, leaving the small active pore-like shapes that will provide a number of correlation peaks in the output. In the final stage, a binarized black image with white spots is generated in which the white spots indicate the presence of active pores [1].

The tests were performed with 20 images. The results compared manual identification of active pores against the HCFA method. The statistics of the results were very positive. The correlation coefficient of the four measured thresholds was very close to one as displayed in Table 9.1. In this case, one means there is a perfect match between the two sets—manual and HCFA.

TABLE 9.1   Statistical Measures for Four Threshold Values: 0.05, 0.1, 0.15, and 0.2

		Type of Statistical Measure	Threshold			
			0.05	**0.10**	**0.15**	**0.20**
1		Coefficient	0.90	0.83	0.81	0.79
2		Mean	62.4	53.2	42.0	38.0
3		Median	63.6	50.0	40.0	35.0
4		LQ	48.9	42.4	28.3	19.4
5		UQ	74.2	66.8	51.7	51.7
6	DE	IQR	25.3	24.4	23.4	32.3
7		Mean	59.8	70.9	73.5	72.7
8		Median	60.0	75.0	80.0	75.0
9		LQ	41.3	52.8	54.9	54.2
10		UQ	74.2	85.4	97.2	97.2
11	DA	IQR	32.9	32.6	42.3	42.5

9.4.3 Skin Deformation-Based

The skin deformation technique uses the information about how the fingertip's skin deforms when pressed against a scanner surface. This approach exploits the elasticity properties of the skin [10]. A method to capture finger distortion is the use of a thin plate spline model with different angles of rotation [23]. Another approach to detect skin deformation in fingerprint is via the correlation coefficient and standard deviation based on the elasticity of the skin [24].

Nonetheless, a thin fake fingerprint attached on a live finger is able to produce comparable nonlinear deformation as a live finger would. Another disadvantage is that the skin deformation-based systems need special training and well-calibrated scanners to deliver frames at a proper rate to identify spoofs [10].

9.4.4 Image Quality-Based

Image-based techniques to identify liveness of fingerprints concentrate on finding the difference between the image of a live and a fabricated fingerprint.

9.4.4.1 Profiling and Wavelet: Joint Time Frequency Analysis

An image processing technique for detecting liveness on fingerprint images is joint time frequency analysis using profiling and wavelet [10]. In a proposal by Bhanarkar and Doshi [25], a single-image-based method was used for liveness detection. This procedure assumes that the

fingerprint images of a live person are different from spoofed ones. The individual characteristics of live and spoofed fingerprints are analyzed using profiling method and wavelet-based analysis techniques.

This method is performed in the following sequence: (1) the subject trying to access the system scans the finger, (2) an image of the fingerprint is obtained, and (3) the fingerprint image is processed in two stages: profiling and wavelet-based profiling [10]. This technique tested 50 samples of live and 50 samples of silicon fake fingerprint images. The result of the tests indicated that the live fingerprint samples are identified as live by indicating 1, but the spoof fingerprint images indicated 0 as fake [10].

This approach is a software-based application thus allows for a high level of customization and reduces the cost of the fingerprint biometric system. Furthermore, there is no need for additional hardware [10].

The joint time frequency analysis based on liveness fingerprint detection has numerous advantages: (1) only a single image of a fingerprint is used, (2) it only takes 1 s for liveness detection, and (3) it can be used in real time applications [10]. These advantages make this method very promising for mobile phone biometric applications.

9.4.4.2 3D Image Quality: FPCLiveTouch™

There are numerous innovative commercial solutions for fingerprint liveness detection. A commercial option for fingerprint liveness detection Fingerprint Cards (FPC) created FPCLiveTouch as a solution to enhance the security for fingerprint sensors to recognize spoofs. The new fingerprint recognition system including liveness detection was released in February 2016. This technology was created in response to the increased demand for secure mobile payments. The accuracy rate ranges from 96.5% to 99.5% to catch and reject "fake fingers" using different sensors including touch, swipe, optical, and capacitance [26]. This biometric equipment offers "unique image quality, extreme robustness, and low power consumption" [26]. FPC technology is implemented in smartphones, tablets, and biometric cards. A distinctive advantage of FPC fingerprint liveness identification is that does not need additional hardware for a fast and secure verification. The latest release mobile with FPCLiveTouch technology is a flagship mobile model Mi5 with an FPC1245 sensor. It includes ceramic coating, 360° finger rotation capability, fast response, and a three-dimensional (3D) image. This innovative mobile phone was released on February 26, 2016 and it has already reached its expected revenues for 2016. Figure 9.4 shows the touch sensor verification.
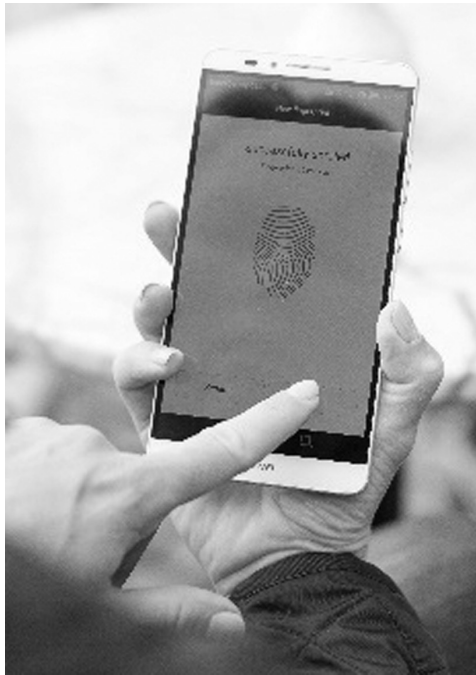
FIGURE 9.4   Touch sensor verification. (From Fingerprints.com.)

9.4.5 Temperature-Based

Temperature is considered an involuntary generated body signal [18]. The temperature on a fingertip is easy to measure, though, it is also easy to be deceived. The average temperature on fingertips ranges between 26°C and 30°C [18]. A thin silicone artificial fingerprint can be used on top of the finger. The temperature on the silicone is only 2°C below the live finger. Since 2°C is within the range of acceptance by the sensor, it will not be difficult to have the temperature of an artificial fingertip within the margins of the sensor [17].

Trials measuring human skin's temperature were performed with a FLIR ThermoCAM PM545G. Ten healthy users contributed and all 10 fingers were measured four times. All the trials were made at room temperature of 26°C and humidity of about 64% within the same day. The results of the trials provided a skin temperature range from 21.5°C to 35.7°C. In addition, the difference between the right and left fingers was roughly 0.6°C. The wide-ranging temperatures in this approach are not effective to detect liveness [18]. Thus, this methodology is not suitable for liveness detection implementation on mobile devices.

9.4.6 Skin Resistance-Based

The resistance or conductivity of the human skin is based on humidity. The electrical properties of the human body can be used as a possible solution to detect liveness. Moisture, in turn, depends on an individual's biological features and environmental conditions. With respect to biological features, some persons have very dry skin which results in high resistance (low conductivity), and other persons have sweaty skin which leads to low resistance (high conductivity) [18]. Environmental conditions are related to the seasons which influence humidity variations as well. Consequently, the extent of acceptable resistance levels has to be large enough to be used by fingerprint liveness detection systems [18].

In a trial on Reference 17, the electric resistance in a live finger measured 16 Mohms/cm. A fabricated fingerprint made out of gelatin measured 20 Mohms/cm. Figure 9.5 displays a recently made gelatin fingerprint. The difference between the live and artificial electrical resistance was very minor. Moisture levels of live fingers and gelatin made ones were taken as well. The results indicated that live fingers have a moisture level of 16%, while gelatin ones have a moisture level of 23% [17]. Furthermore, it is easy to add a salty solution of similar concentration of sweat or saliva on a fake finger to add moisture and imitate the humidity of a real finger.
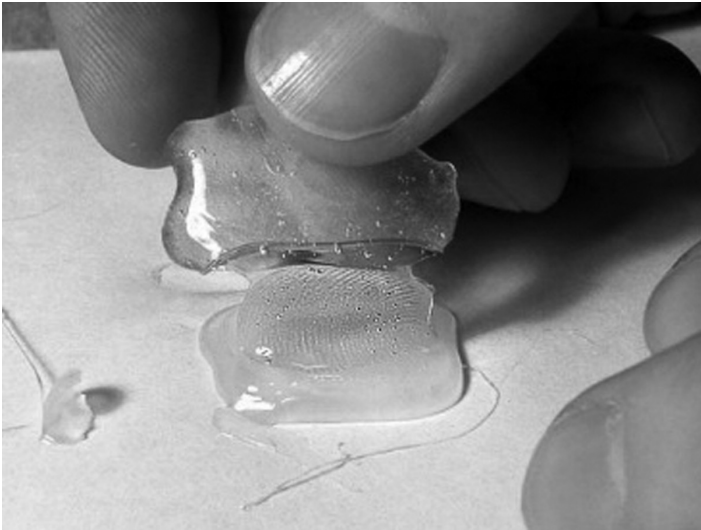

FIGURE 9.5 Making a gelatin fingerprint. (From Kaseva, A., and Stén, A. 2003. Creating an artificial finger using the actual finger, March 18.)

The slight difference between the moisture levels of the real and gelatin made fingerprints and the capacity to add moisture to a fake fingerprint, make this method not feasible to use as liveness detection option on mobile devices.

9.5 CONCLUSION

Spoofing is a real concern with regard to the security of biometric system in the mobile industry. In this chapter, we explained various approaches to prevent the attacker from fooling the biometric system with fake fingerprints and we also discussed some of the challenges of each method.

Software methods, image-based, have more popularity due to the diversity of algorithms that can be used to analyze the obtained fingerprints. A promising liveness detection approach, from among the many possible techniques, is the profiling and wavelet procedure presented in this chapter. This scheme has an advantage over other methods for liveness detection on fingerprints since only one image is used to detect spoof attacks [10]. Profiling and wavelet process only requires 1 s for liveness detection thus making this approach suitable for real time applications such as mobile phone biometric user authentication.

Another optimistic answer to liveness detection on fingerprints is FPCLiveTouch(TM)'s commercially available solution introduced before. Although is new in the market, the sales and popularity have already surpassed the expectations within months of its release. The sophisticated design includes swipe, touch, and optical properties with a 95%–99% accuracy of fingerprint spoof detection. The liveness detection can be applied in tablets, cellphones, and biometric cards.

Conversely, approaches that did not meet the criteria to be suitable for fingerprint liveness detection are, among several others, the pore detection and temperature-based methods. The pore detection method achieved good results, but it works best in the presence of more active pores. This method seems a good fit for mobile devices although it needs further development to become more practical. The temperature-based liveness detection is not a feasible method to detect fingerprint liveness since the scanner can be easily deceived using a thin silicone fingerprint over a live finger. In addition, some fake fingers moisturized or warmed up were recognized by the system as live fingers. The pulse oximetry approach presented in the beginning of this chapter was also easily fooled. The same applied for the skin resistance-based approach.

The amount of spoofing attempts is continuously increasing and new methods are emerging. Both industry and academic circles are working on creating more robust biometric devices. Still every counterstep can sooner or later be bypassed. Thus, research and development efforts must be continuous. The solutions should be precise, fast, and easy to use. The technology for mobile fingerprint authentication is evolving rapidly and it is just a matter of including liveness detection for better authentication.

Single modal biometric techniques for liveness fingerprint recognition are under continuous research and have achieved very good results. However, the integration of multimodal biometric systems for fingerprint authentication is under initial development. Further research is needed to integrate the liveness detection method into multimodal biometric systems. The challenge would be to choose a property or multiple properties in the fingerprints that are very difficult or impossible to imitate.

REFERENCES

1. Memon, S., Manivannan, N., and Balachandran, W. 2011. Active pore detection for liveness in fingerprint identification system. In *2011 19th Telecommunications Forum (TELFOR)*, Belgrade, Serbia. IEEE, pp. 619–622, November.
2. Shinde, M. K. and Annadate, S. A. 2015. Analysis of fingerprint image for gender classification or identification: Using wavelet transform and singular value decomposition. In *2015 International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India. IEEE, pp. 650–654, February.
3. What's So Special about Your Fingerprints? n.d. http://wonderopolis.org/wonder/what-s-so-special-about-your-fingerprints (retrieved March 8, 2016).
4. Hoover, J. E. n.d. Fingerprint. http://www.britannica.com/topic/fingerprint (retrieved March 2, 2016).
5. Understanding Fingerprints. n.d. http://www.viewzone.com/fingerprintsx.html (retrieved February 25, 2016).
6. Advantages and Disadvantages of Technology. PB Works. http://biometrics.pbworks.com/ (retrieved March 1, 2016).
7. Gottschlich, C., Marasco, E., Yang, A. Y., and Cukic, B. 2014. Fingerprint liveness detection based on histograms of invariant gradients. In *2014 IEEE International Joint Conference on Biometrics (IJCB)*, Clearwater, Florida. IEEE, pp. 1–7, September.
8. Abhyankar, A. and Schuckers, S. 2006. Fingerprint liveness detection using local ridge frequencies and multiresolution analysis techniques. In *International Conference on Image Processing*, Atlanta, Georgia, pp. 321–324.

9. LivDet—Liveness Detection Competitions. n.d. http://livdet.org/ (retrieved February 25, 2016).

10. Akhtar, Z., Michelon, C., and Foresti, G. L. 2014. Liveness detection for biometric authentication in mobile applications. In *2014 International Carnahan Conference on Security Technology (ICCST)*, Rome, Italy. IEEE, pp. 1–6, October.

11. Kent, J. Malaysia car thieves steal finger. *BBC News*, Kuala Lumpur, http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

12. Institute of Automation, Chinese Academy of Sciences (CASIA). Biometrics Ideal Test. http://biometrics.idealtest.org/ (retrieved March 1, 2016).

13. Reddy, P., Kumar, A., Rahman, S., and Mundra, T. 2007. A new method for fingerprint antispoofing using pulse oximetry. In *IEEE Biometrics: Theory, Applications and Systems (BTAS)*, Washington, DC, pp. 1–6.

14. FCW: The Business of Federal Technology. https://fcw.com/articles/2011/08/25/fbi-fingerprint-check-system-national-database-mobile.aspx

15. The FBI's big, bad identification system. By Michael Cooney, Network World |Sep 25, 2014 8:31 AM PT. http://www.networkworld.com/article/2687913/security/164703-The-FBI-s-big-bad-identification-system.html#slide9

16. Aggarwal, T. 2014. *CS Journals*, May 1. http://www.csjournals.com/ (retrieved March 1, 2016).

17. Sandström, M. 2004. Liveness detection in fingerprint recognition systems, Master thesis, http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf

18. Drahansky, M. 2008. Experiments with skin resistance and temperature for liveness detection. In *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Harbin, China. IEEE, pp. 1075–1079, August.

19. Image of Pore. https://handfacts.files.wordpress.com/2011/04/sweat-pores-skin-ridges.jpg

20. Ray, M., Meenen, P., and Adhami, R. 2005. A novel approach to fingerprint pore extraction. In *Proceedings of the Thirty-Seventh Southeastern Symposium on System Theory, SSST '05*. IEEE, pp. 282–286.

21. Watson, C. and Wilson, C. L. 2008. *NIST Special Database 4, Fingerprint Database*. National Institute of Standards and Technology. http://www.nist.gov/srd/nistsd4.cfm

22. Parthasaradhi, S.T.V., Derakhshani, R., Hornak, L.A., and Schuckers, S.A.C. 2005. Time-series detection of perspiration as a liveness test in fingerprint devices. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 35, 335–343.

23. Zhang, Y., Tian, X., Chen, X., Yang, X., and Shi, P. 2007. Fake finger detection based on thin-plate spline distortion model. *Advances in Biometrics Lecture Notes in Computer Science*, 4642, 742–749.

24. Jia, J., Cai, L., Zhang, K., and Chen, D. 2007. A new approach to fake finger detection based on skin elasticity analysis. In *Proceedings of the 2007 International Conference on Advances in Biometrics (ICB'07)*, S.-W. Lee and S. Z. Li (Eds.). Springer-Verlag, Berlin, Heidelberg, pp. 309–318.

25. Bhanarkar, A., Doshi, P., Abhyankar, A., and Bang, A. 2013. Joint time frequency analysis based liveness fingerprint detection. In *2013 IEEE Second International Conference on Image Information Processing (ICIIP)*, Shimla, India. IEEE, pp. 166–169, December.
26. Fingerprint cards extends security for fingerprint sensors. 2016, February 17. http://www.fingerprints.com/corporate/en/fingerprint-cards-extends-security-for-fingerprint-sensors/ (retrieved February 28, 2016).
27. Kaseva, A. and Stén, A. 2003. Creating an artificial finger using the actual finger, March 18. http://biometrics.mainguet.org/ (retrieved March 9, 2016).