

Overview on Fingerprinting Authentication Technology



N. Sulaiman and Q. A. Tajul Ariffin

Abstract This paper addresses the characteristics, technology, and possible future of fingerprints authentication method. Fingerprint physiology makes it an ideal for biometrics authentication, primarily the tiny details located on its surface called minutiae. Fingerprint scanning systems are designed to detect minutiae. Images of detected minutiae are processed through matching algorithms in order to verify a query fingerprint that is identical to a stored fingerprint. However, fingerprint authentication based on minutiae can be easily bypassed and the need for a more secure method is required. With respect to the issue, this work explores the possibility of detecting the thickness of the skin layer within a fingerprint as a method of biometrics authentication. Current thickness measuring methods that are non-invasive for that task are identified as Laser Scanning Microscopy (LSM), Optical Coherence Tomography (OCT) and Near Infrared Spectroscopy (NIR). Of the three listed, only OCT and NIR methodology seems viable for simple yet reliable use and can become as promising methods for authentication based on skin layer thickness.

Keywords Fingerprint · Biometrics · Skin thickness · Authentication · Security

1 Introduction

Fingerprints are the most established form of authentication. Historically, fingerprinting had been near exclusively used in forensics, but over the years, it has grown in popularity where it is now a common method used in various day-to-day services [1, 2]. As such, the need for a better technology to secure a person's fingerprint identity has also increased [3]. This paper aims to go over the characteristics of a fingerprint that allows for its use in authentication, the technology currently utilized in that endeavor and explore future methods that can be developed for this task.

N. Sulaiman (✉) · Q. A. Tajul Ariffin
Faculty of Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia
e-mail: nadzril@iium.edu.my

© Springer Nature Singapore Pte Ltd. 2020
A. N. Kasruddin Nasir et al. (eds.), *InECCE2019*, Lecture Notes in Electrical Engineering 632, https://doi.org/10.1007/978-981-15-2317-5_38

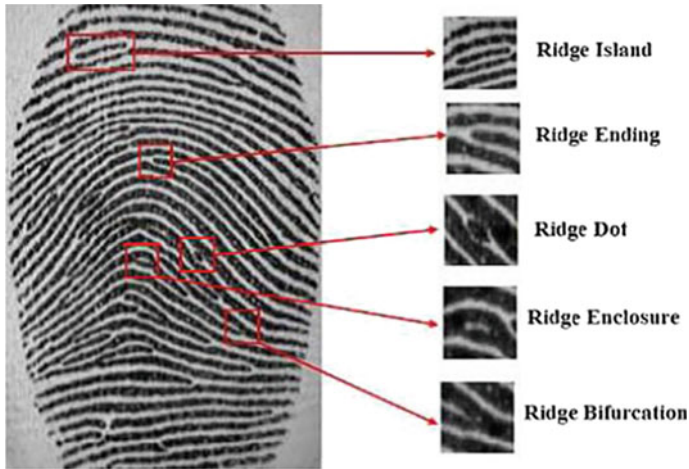


Fig. 1 A fingerprint with multiple kinds of minutiae highlighted [4]

2 Fingerprint Characteristics

The human fingerprint has two characteristics that makes it ideal for biometric use. The fingerprint is able to generate unique details that enable it for use in identification. The structure of how a fingerprint forms allows for its pattern to remain permanent.

2.1 Identification

Fingerprints are unique due to the shapes and patterns that are formed by ridges. Called minutiae [1], the location of these patterns within the surface of the fingerprints are used to identify a person. It is unlikely for another person to have the exact same kind of minutiae in the exact same location, and this unlikeliness grows exponentially greater with each minutia added for comparison (Fig. 1).

In addition, the ridges of a fingerprint often follow a specific overall structure. As seen in Fig. 2, these structures, called types, are useful in categorizing fingerprints. An identification system is able to narrow down the number of images that they need to process in order to identify who the print belongs to.

2.2 Permanence

The human skin is made up of multiple layers but can be simplified to 3 main layers. The epidermis is the outermost layer and acts as a waterproof barrier. The dermis is

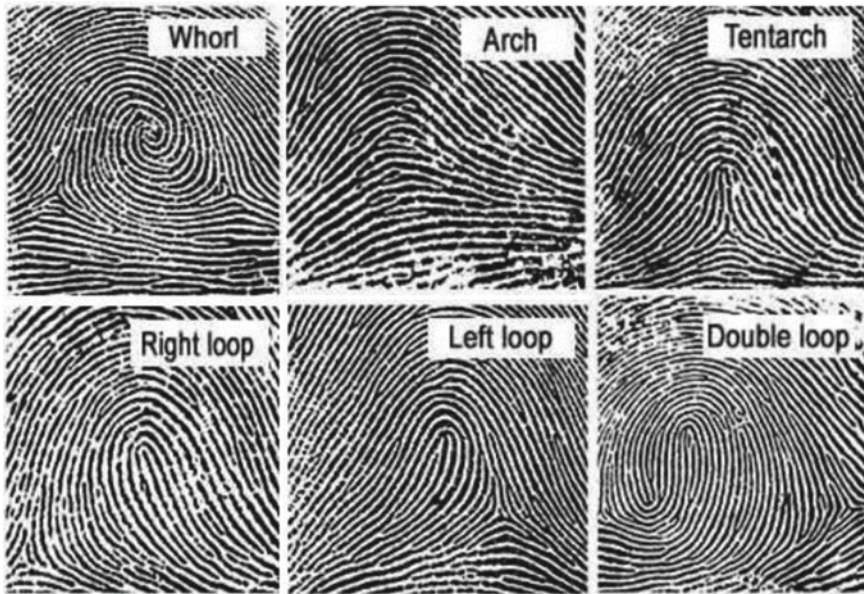


Fig. 2 A showcase of the how various types of fingerprints may appear as [5]

the middle layer that is mainly composed of hair follicles, sweat glands, and tough connective tissue. The innermost layer is the hypodermis, which is composed of fat and connective tissue.

The fingerprint is formed in the dermis, specifically in the papillary layer that is right beneath the epidermis. This layer anchors to the epidermis using a “double row of peg like protuberances” [6] known as papillae, which forms the layout of the fingerprint. The ridges appear on the epidermis layer are determined by the position of the papillae in the epidermis layer.

This arrangement is what allows fingerprint to remain permanent throughout a person’s life. The papillae act as a “blueprint” that exists under the regenerative layer of the skin. Thus, whenever the epidermal layer restores itself, it will grow following the layout set by the papillae. As long as the papillae remain undamaged, a person’s fingerprint will repair itself to its original design.

3 Authentication System

Fingerprint authentication systems function on three fundamental stages: data acquisition, feature extraction, matching [7]. Data acquisition focuses on the method used by the system in order to extract fingerprint data. Feature extraction is the step where the system identifies unique features of the fingerprint data and stores it within the

database. Matching describes the step where a system is required to compare a read fingerprint to those within its database in order to authenticate a person's identity.

3.1 Data Acquisition

Currently, there are three main types of fingerprint authentication system, defined by their data acquisition methods, optical, capacitive, and ultrasonic fingerprinting. This section will go over their method of acquiring data.

Optical Fingerprinting. Is one of the oldest, cheapest and most common forms of biometric identification [8]. The scanner functions by creating a digital photo of the fingerprint (Fig. 3).

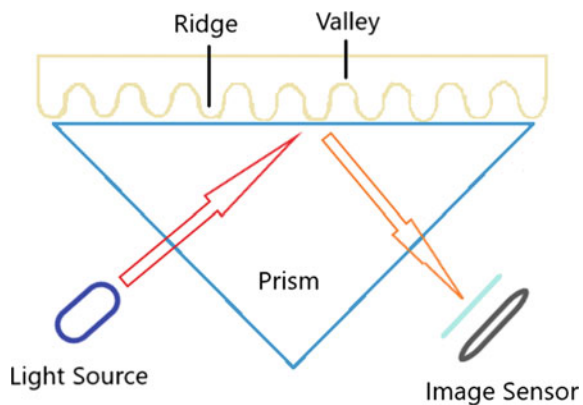
When a fingerprint is placed on the scanning surface, a light source is beamed towards print. An image is generated based on the difference in reflected light levels between ridges and valleys of a fingerprint. The reflected light travels to a light sensor that converts the image into a digital signal. The system performs a few checks to ensure that the generated image is at sufficient brightness before processing the image to be compared to a database of registered fingerprints.

Optical scanners are considered the easiest biometric systems to fool. Its method of simply detecting the changes in reflected light levels means that it can easily be spoofed by simply printing the fingerprint pattern onto a material, such as transparency paper and having the ink produce the ridges and valleys of the fingerprint [8].

Capacitive Fingerprinting. As its name suggest, uses capacitors to “read”s the electrical charges created by the ridges and air pockets of the fingerprint. It is currently the most popular form of fingerprint-based authentication in smartphones [1] (Fig. 4).

A capacitive scanner scanning surface is made up of an array of cells that are composed of conductive plates covered in a protective layer [9]. When the ridge of a fingerprint comes in contact with the surface, it acts as another conductive plate,

Fig. 3 Model of how an optical scanner functions [8]



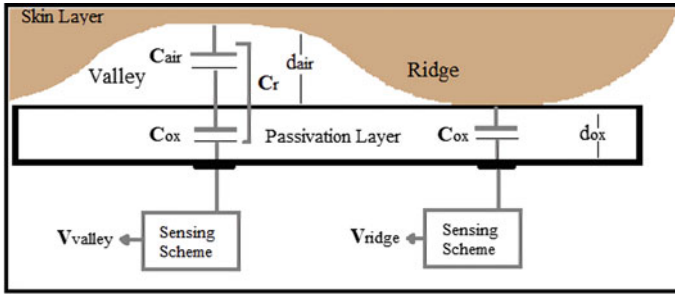


Fig. 4 Model of how a capacitive scanner functions [8]

which in turn charges that cell's conductor plate. The air pockets formed form the valleys however have minimal effect on the charge held by cell. An op-amp integrator is used to detect the changes and the output is recorded by an analog-to-digital converter.

Capacitive scanners, while more secure than optical scanners, have also fallen victim to being spoofed. Simple, 3d molds layered with conductive materials such as gold [10] has been used to successfully bypass most conventional capacitive sensors and complex molds, such as those casted in polydimethylsiloxane, are able to replicate fingerprints at the nanoscale [11].

Ultrasonic Fingerprinting. Is the newest entry in commercial fingerprint detection. They function by generating an ultrasonic pulse onto a finger that is in contact with the scanner. Depending on the details on the fingerprint, some of the pulses are absorbed while others are reflected back to a sensor that is able to detect mechanical stress. The varying intensity of the returned ultrasonic pulse throughout the sensor's surface creates a detailed 3D reproduction of the scanned fingerprint [9].

Ultrasonic scanners are currently considered of the most secure methods of fingerprint identification, but it has also been spoofed. A researcher was able to create a 3D printed, highly detailed model of a fingerprint to bypass a commercial ultrasonic sensor [12].

3.2 Feature Extraction

After acquiring data through one of the various methods mentioned, the system processes the image to help detect specific features on the fingerprint such as the overall pattern of the ridges or the various minutiae on its surface. The first layer of feature extraction revolves around whether the image remains gray-scale or goes through binarization (Fig. 5).

Binarization is a process where the gray-scale fingerprint scan is converted to 1's and 0's for their respective dark and light areas. This generates a much clearer image of the scan.

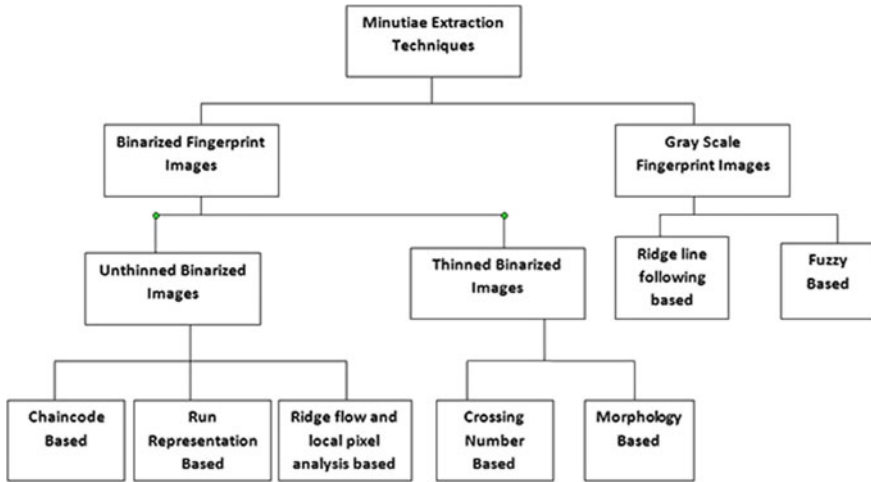


Fig. 5 Classification of minutiae extraction technique [4]

Ridge Extraction is a secondary process that can be applied to images that has gone through binarization. The binary image is filtered through a morphological filter that causes the ridges to be thinned [13] to one-pixel thickness. Techniques that utilizes binarization are as follows.

Chaincode processing is a method that traces a ridge along its boundary in a counter-clockwise direction. Ridge endings are detected when the trace makes a significant left turn, while bifurcations are detected when the trace makes a right turn.

Run representation based is a method that performs a vertical and horizontal scan on to the image while applying run-length encoding to the pixels passed. Base on the adjacency of the runs, minutiae are able to be identified [14].

Ridge flow and local pixel analysis process the image through a 3×3 mask that calculates the average of each pixel. Pixels that average less than 0.25 denotes a ridge ending while those greater than 0.75 denotes a bifurcation.

Crossing-number based processes the image through a 3×3 window that detects the neighboring pixel. Each neighboring pixel adds to the “crossing number” which is a value used to determine the properties of the ridge at that pixel [14] (Fig. 6).

Morphology based processes the image through multiple filters that detect a specific shape. An output only appears if the scanned image is able to fully complete the desired shape.

Gray-scale images do have their own advantages over binarization. First of all, it’s able to function with low quality images. Second, binarization and ridge extraction is a time-consuming process, hence gray-scale based processing will often time perform much faster than their processed image counterpart [14]. Techniques based on gray-scale are as follows.

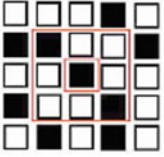
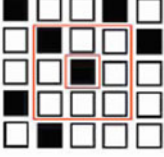
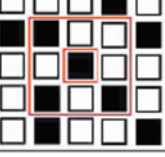
| | |
|---|--|
|  | <p>Crossing Number =2. Normal ridge pixel.</p> |
|  | <p>Crossing Number =1. Termination point.</p> |
|  | <p>Crossing Number =3. Bifurcation point.</p> |

Fig. 6 A breakdown of the crossing number method. Each “pattern” within the 3 × 3 window helps the system identify the minutiae [15]

Ridge line following based process functions by following the ridge flow lines set by the fingerprint type. By simply following the lines, the system can detect minutiae it passes through.

Fuzzy based technique uses fuzzy logic model to process the varying gray levels in order to detect minutiae.

3.3 Matching

In order to authenticate a user, the scanned image will be processed by a matching algorithm. This section will briefly describe some of the algorithms used in fingerprint authentication.

Direct matching is the most basic algorithm used for authentication. It functions simply by comparing the pixels of the input image against a template image stored within the database. This method however, requires the system to align the scanned image with the template. This uses a lot of computational power and requires samples to be very large to ensure that the image is aligned properly [16].

Minutiae based matching authentication is performed by detecting minutiae and classifying it based on its surrounding neighbors. The algorithm detects the location,

orientation, type and quality of the minutiae [17] and then compares it to ones detected in the print from the database.

Euclidian distance authentication involves identifying 2 minutiae and calculating the distance and angle they are from one another. This process may be repeated for multiple “minutiae pairs”. The system then compares the Euclidian distances of the print and those within its database to find a match [18].

4 System Security

Fingerprint authentication increased use in protecting private information has made the security of the system crucial. A compromised fingerprint has much bigger impact to a person than getting their password stolen since you can't just change the former as you could the latter.

Threats to the authentication system can be categorized into passive and active attacks. Passive attacks refer to methods that steal information from an authentication system, while active attacks are those that attempt to thwart the authentication service [19, 20]. An example of a passive attack would be a backdoor program that sends a copy of the scanned fingerprint to the attacker, while an example of an active attack would be using the scanned fingerprint to fool a biometric system (Fig. 7).

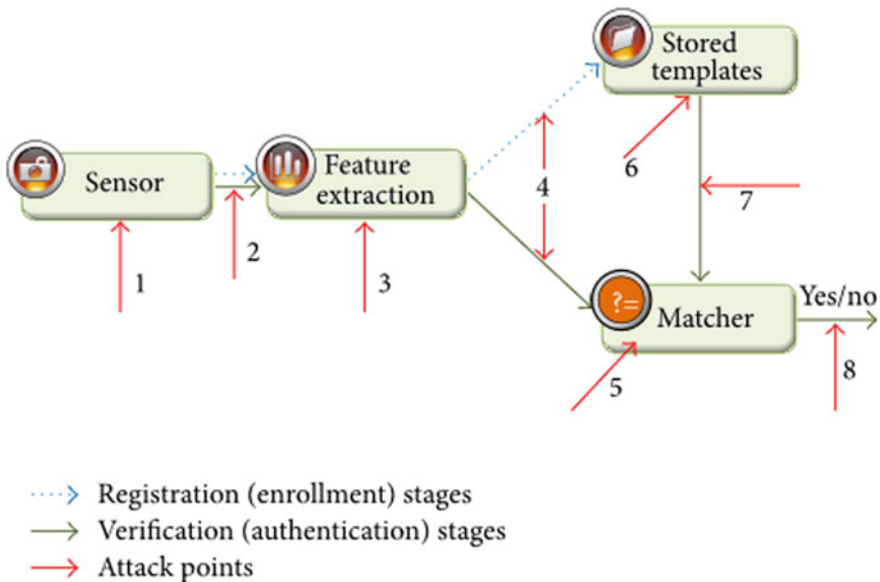


Fig. 7 Flowchart of fingerprint authentication system for both enrollment and authentication function and the various points of attack that can occur [21]

5 Future Technology

New methods of fingerprint base authentication are necessary. Currently, there is a research on utilizing thickness of the skin within a fingerprint as a method of biometric identification. While there is no commercial method of thickness-based fingerprinting, there are currently multiple non-invasive methods to measure the thickness of the skin layer. This section aims to describe how these methods work and their potential application into fingerprinting authentication.

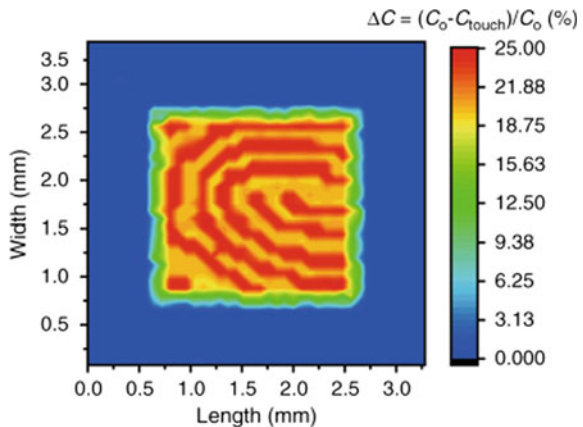
Pyroelectric Sensor are passive electronic component that is sensitive to infrared radiation. Changes in temperature causes a change in charge within the pyroelectric crystals within the component, which in turn will generate an electrical signal.

Similar to how a capacitive sensor works, a pyroelectric sensor is able to generate an image based on the location where the ridges of a fingerprint come in contact with the sensor’s surface. The heat generated by the ridges, will be higher than the air pockets within its valleys, which results in differences in the electrical signals generated at those location.

Pyroelectric sensor is potentially a viable method of fingerprinting authentication. The image it generates can easily be implemented into already established extraction and matching processes. A recent research [22] have managed to design a transparent thermal sensor, which increases the ability for its use in commercial smartphones. As seen in Fig. 8, the sensor is able to generate an accurate image of the fingerprint pattern.

Laser Scanning Microscopy (LSM) is an imaging technique that is able to capture multiple micrographs at different depths. It functions by transmitting a filtered, colored light through a pinhole onto the surface of the subject. The subject material is infused with fluorescent chemical that will react with the filtered light. The fluorescent chemical will emit its own filtered light, which will then pass through a dichroic to reach the camera. An image is generated by moving the subject along the x–y axis. The pinhole ensures that the filtered light only activates within a set depth,

Fig. 8 Captured fingerprint pattern using pyroelectric sensor [22]



thus, only an image of that layer. By moving the subject along the z-axis, images for different depths can also be obtained [23, 24].

LSM is deemed a high-resolution technique with a resolution of less than 1 μm , it does have a major drawback. In order for accurate detection to occur, a fluorescent agent must be properly injected into the subject. This results in an increased cost as the fluorescent agent must be resupplied for continuous use.

While it would be extremely difficult for someone to spoof the detection system, as they would have to make a multi-layered model that's able to replicate each layer exactly, the increased cost and requirement for proper fluorescent agent injection makes it not very viable for authentication use.

Optical Coherence Tomography (OCT) is another non-invasive imaging technique that functions similarly to echo-location. The OCT directs low-coherence light into a tissue. As the light travels throughout the tissue, some of it will scatter when it comes in contact with certain features and materials within the tissue. The OCT then detects the scattered light and utilizes interferometry to filter out photons that have scattered multiple times. This allows for the OCT to create a complete 3D image of the tissue (Fig. 9).

OCT is highly suggested for use in fingerprint authentication, with multiple research [25–27] have suggested methods of implementation. OCT's ability of producing an image of the dermis and epidermis layer of the fingerprint makes it extremely difficult to spoof. Furthermore, the ability for OCT to model individual layers of the skin [28] allows fingerprint thickness to be used as an additional metric for identification.

Near Infrared Spectroscopy (NIRS) is an imaging technique similar to OCT. It functions by beaming near infrared into a tissue sample. The NIRS light will be absorbed differently by different parts of the tissue. A detector is used to measure the change in the reflected light. Information on the thickness of the tissue can be determined by the change in transmittance of the infrared light [29–31].

Like OCT, NIRS is able to produce high information scans and is very easy to use. While not as popular as OCT methods of determining fingerprint biometrics, there have been successful research showing its viability to function in authentication [32,

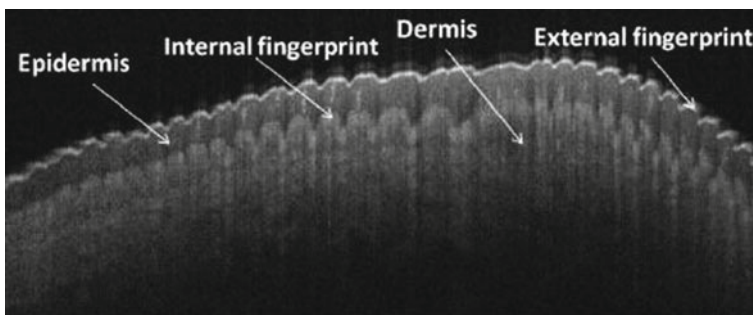


Fig. 9 Cross-section of a fingerprint generated through OCT [23]

33]. However, in both methods, further testing into its consistency and reaction to various factors, such as skin color, before it can be proven truly viable for commercial use.

6 Conclusion

Fingerprints are essential in the use of biometric based authentication. Its physiology makes it a convenient and ideal tool for that purpose. The number of methodology and techniques used in fingerprint identification is vast, but not without weakness. Thus, alternative methods, such as fingerprint thickness and thermal based detection would be a welcome addition to further improving security.

Of the methods proposed in thickness-based fingerprinting, Optical Coherence Tomography and Near Infrared Spectroscopy are better candidates for further research for authentication application. Their ability to model high detail images of the layers under the epidermis greatly increases the difficulty of being spoofed.

Acknowledgements It is acknowledged that this work is supported by the Ministry of Education of Malaysia and the International Islamic University Malaysia under grant FRGS/1/2018/TK04/UIAM/02/24 (FRGS19-003-0611).

References

1. Bhagavatula R, Ur B, Iancovino K, Kywe SM, Cranor LF (2015) Biometric authentication on iPhone and Android: usability, perceptions, and influences on adoption. In: USEC'15, San Diego, CA (2015)
2. Kumar Sharma A, Raghuwanshi A, Kumar Sharma V (2015) Biometric system—a review. *Int J Comput Sci Inf Technol* 6(5):4616–4619
3. InAuth (2017) Fingerprints: the most popular biometric. <https://www.inauth.com/blog/fingerprints-popular-biometric/>. Last accessed 28 March 2019
4. Thakkar D (2016) Minutiae based extraction in fingerprint recognition. *Bayometric*. <https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/>. Last accessed 26 April 2019
5. Topaloglu N (2013) Revised: fingerprint classification based on gray-level fuzzy clustering co-occurrence matrix. *Energy Educ Sci Technol Part A: Energy Sci Res* 31(3):1307–1316
6. Hoover, J. E.: Finger. *Encyclopaedia Britannica* (2016), <https://www.britannica.com/topic/fingerprint>, last accessed 2019/3/28
7. Faridah Y, Nasir H, Kushairy AK, Safie SI, Khan S, Gunawan TS (2016) Fingerprint biometric systems. *Trends Bioinf* 9(2):52–58
8. Triggs R (2018) How fingerprint scanners work: optical, capacitive, and ultrasonic variants explained. *Android Authority*. <https://www.androidauthority.com/how-fingerprint-scanners-work-670934/>. Last accessed 29 March 2019
9. Tang K, Liu A, Wang W, Li P, Chen X (2018) A novel fingerprint sensing technology Based on electrostatic imaging. *Sensors* 19(9)
10. Arora SS, Jain AK, Paulter NG Jr (2017) Gold Fingers: 3D targets for evaluating capacitive readers. *IEEE Trans Inf Forensics Secur* 12(9):2067–2077

11. Schultz CW, Wong JXH, Yu H-Z (2018) Fabrication of 3D fingerprint phantoms via unconventional polycarbonate molding. *Sci Rep* 8(1)
12. Katz E, Halámek J (2016) Fingerprint spoofing and liveness detection. *Forensic science: a multidisciplinary approach*. Wiley
13. Abel R (2019) Researchers claim to trick Samsung Galaxy S10 fingerprint scanner using a 3D printed image. *SC Magazine*. <https://www.scmagazine.com/home/security-news/mobile-security/a-reddit-user-claims-to-have-fooled-the-ultrasonic-fingerprint-scanner-on-the-samsung-galaxy-s10-using-a-3d-printed-image/>. Last accessed 10 April 2019
14. KivutiNjeru S, Oboko DR (2016) Comparative analysis of minutiae based fingerprint matching algorithms. *Int J Comput Sci Inf Technol* 8(6):59–71
15. Guruprakash G, Vasanth AV (2014) Combined fingerprint minutiae template generation. *Int J Innov Res Comput Commun Eng* 2(1)
16. Mathur A, Gupta R (2016) Analysis of algorithms used in biometric. *Int Conf Adv Computing*, 398–403
17. Sahu D, Shrivastava R (2016) Minutiae based fingerprint matching for identification and verification. *Int J Sci Res* 5(3):2103–2106
18. Bhargava N, Kumawat A, Bhargava R (2015) Fingerprint matching of normalized image based on Euclidean distance. *Int J Comput Appl* 120(24):20–23
19. Joshi M, Mazumdar B, Dey S (2018) Security vulnerabilities against fingerprint biometric system
20. Hosseini S (2018) Fingerprint vulnerability: a survey. In: 4th international conference on web research (ICRW)
21. Jo Y-H, Jeon S-Y, Im J-H, Lee M-K (2016) Security Analysis and Improvement of Fingerprint Authentication for Smartphones. *Mobile Information Systems* 2016:1–11
22. An BW, Heo S, Ji S, Bien F, Park J-U (2018) Transparent and flexible fingerprint sensor array with multiplexed detection of tactile pressure and skin temperature. *Nat Commun* 9(1)
23. Bellinger R (2018) Principles of laser scanning confocal microscopes. *Tech Briefs*. <https://www.techbriefs.com/component/content/article/tb/supplements/pit/features/29736>. Last accessed 14 June 2019
24. Kamweru P, Diekmann S, Hoischen C (2015) Elucidation of the kinetochore structure using quantitative confocal laser Scanning microscopy based technique. In: *IONS/FOCUS Tunis 2015*, Carthage Tunis
25. Vyas S, Meyerle J, Burlina P (2015) Non-invasive estimation of skin thickness from hyperspectral imaging and validation using echography. *Comput Biol Med* 57:173–181
26. Wang H, Ma L, Chen P (2018) External and internal fingerprint extraction based on optical coherence tomography. In: *Sixth International conference on optical and photonic engineering*
27. Liu F, Liu G, Wang X (2019) High-accurate and robust fingerprint anti-spoofing system using optical coherence tomography. *Expert Syst Appl*
28. Li A, Cheng J, Yow AP, Wall C, Wong DWK, Tey HL, Liu J (2015) Epidermal segmentation in high-definition optical coherence tomography. In: *37th annual international conference of the IEEE engineering in medicine and biology society (EMBC)*
29. Ozaki Y, Genkawa T, Futami Y (2017) Near-infrared spectroscopy. In: *Encyclopedia of spectroscopy and spectrometry*, 3rd edn, pp 40–49
30. *Near Infrared Spectroscopy*, L-A Write Now (2019). <https://lawrittenow.com/consulting/near-infrared-spectroscopy-nirs/>. Last accessed 18 June 2019
31. Miyamae Y, Kawabata M, Yamakawa Y, Tsuchiya J, Ozaki Y (2012) Non-invasive estimation of skin thickness by near infrared diffuse reflection spectroscopy—separate determination of epidermis and dermis thickness. *J Near Infrared Spectrosc* 20(6):617–622
32. Pena A, García M, Posada E, Ponce L, Reyes T (2014) Non-invasive optical method for epidermal thickness estimation. *OnLine J Biol Sci* 14:163–166
33. Souza-Barros L, Dhaidah G, Maunula M, Solomon V, Gabison S, Lilje L, Nussbaum EL (2017) Skin color and tissue thickness effects on transmittance, reflectance, and skin temperature when using 635 and 808 nm lasers in low intensity therapeutics. *Lasers Surg Med* 50(4):291–301