Chapter 1
Introduction to Selfie Biometrics

Ajita Rattani, Reza Derakhshani and Arun Ross

Abstract Traditional password-based solutions are being predominantly replaced by biometric technology for mobile user authentication. Since the inception of smartphones, smartphone cameras have made substantial progress in image resolution, aperture size, and sensor size. These advances facilitate the use of selfie biometrics such as the self-acquired face, fingerphoto, and ocular region for mobile user authentication. This chapter introduces the topic of selfie biometrics to the readers. Overview of the methods for different selfie biometrics modalities is provided. Liveness detection, soft-biometrics prediction, and cloud-based infrastructure for selfie biometrics are also discussed. Open issues and research directions are included to provide the path forward. The overall aim is to improve the understanding and advance the state-of-the-art in this field.

1.1 Mobile Biometrics

Biometrics is the science of recognizing an individual based on the inherent physical (fingerprints, iris, face, hand geometry, and palmprint) or behavioral traits (gait, voice, and signature) associated with the person [1]. A conventional biometric system operates by capturing the biometric trait of a person and comparing the acquired sample with the biometric template(s) in a database to determine the identity or to validate a claimed identity.

With the unprecedented mobile technology revolution, mobile devices have transcended from their primary communication role to all-in-one platforms for

A. Rattani (✉)
Wichita State University, Wichita, KS, USA
e-mail: ajita.rattani@wichita.edu

R. Derakhshani
University of Missouri—Kansas City, Kansas City, MO, USA
e-mail: derakhshanir@umkc.edu

A. Ross
Michigan State University, East Lansing, MI, USA
e-mail: rossarun@cse.msu.edu

A. Rattani et al. (eds.), *Selfie Biometrics*, Advances in Computer Vision and Pattern Recognition, https://doi.org/10.1007/978-3-030-26972-2_1

shopping, entertainment, productivity, and social networking. An increasing number of individuals are accessing the internet and online services, such as e-commerce and banking, using their smartphones instead of traditional desktop computers. Although individuals are using their smartphones for sensitive applications and transactions, these devices can be easily misplaced, lost, or stolen more often than other computing devices, thereby demanding the use of effective user authentication mechanisms. Traditional methods for mobile security include the use of passwords, PINs, and screen lock patterns to restrict access to authorized users. However, these methods have many security drawbacks: They can be guessed, forgotten, stolen, or eavesdropped.

Password replacement solutions are now predominantly based on biometrics. In some cases, passcodes are used in conjunction with biometrics in a multifactor configuration. The use of biometric technology in mobile devices has been referred to as *mobile biometrics*, encompassing the sensors that acquire biometric samples as well as the associated algorithms for preprocessing, and matching the biometric samples to verify the claimed identity [2–4].

Since the inception of smartphones, smartphone *cameras* have made substantial progress. Image resolution, aperture size, and a sensor size of smartphone cameras have all improved tremendously over time. Since 2008, the megapixel count of these images has gone up from 2 to 20+; apertures have become brighter, with f/1.4 camera modules being considered; and sensor diagonal has increased from 0.25 inches to approximately 0.45 inches.[1] These advances in smartphone cameras facilitate the acquisition and integration of biometric modalities such as the face and ocular region for mobile user authentication [5–8]. Figure 1.1 shows an example of face-based mobile user authentication. This figure was taken from https://www.scnsoft.com/blog/3d-face-recognition-to-join-a-list-of-mobile-enabled-biometrics.

Other popular modalities such as fingerprint and iris that are used for mobile user authentication warrant the use of additional hardware for data acquisition. Further, behavioral biometrics such as gait/motion, keystroke, and touch/swipe analysis have also been used for user authentication in mobile devices [9, 10].

Mobile biometrics is, ubiquitously, installed in 100 percent of mobile devices, fueled by advances in mobile biometrics and rapid expansion of smartphones' market share. Figure 1.2 is a chart from Statista showing biometrics to be installed on 100% of wearables and tablets by 2020. In fact, the latest smartphones provide a range of biometric capabilities, with the most common OEM-provided modalities being the face, fingerprint, and at times iris recognition. Mobile device applications include online banking, password vaults, signing documents univocally, secure access to Web sites, and execution of administration procedures. E-commerce giant Alibaba is using facial recognition service in their mega-app Alipay Wallet.[2] MasterCard[3] has introduced user authentication based on face biometrics, and many more followed suit. Some versions of the Android mobile operating system have also used face

[1] https://petapixel.com/2017/06/16/smartphone-cameras-improved-time/.

[2] https://www.computerworld.com/article/2897117/alibaba-uses-facial-recognition-tech-for-online-payments.html.

[3] http://www.bbc.com/news/technology-35631456.

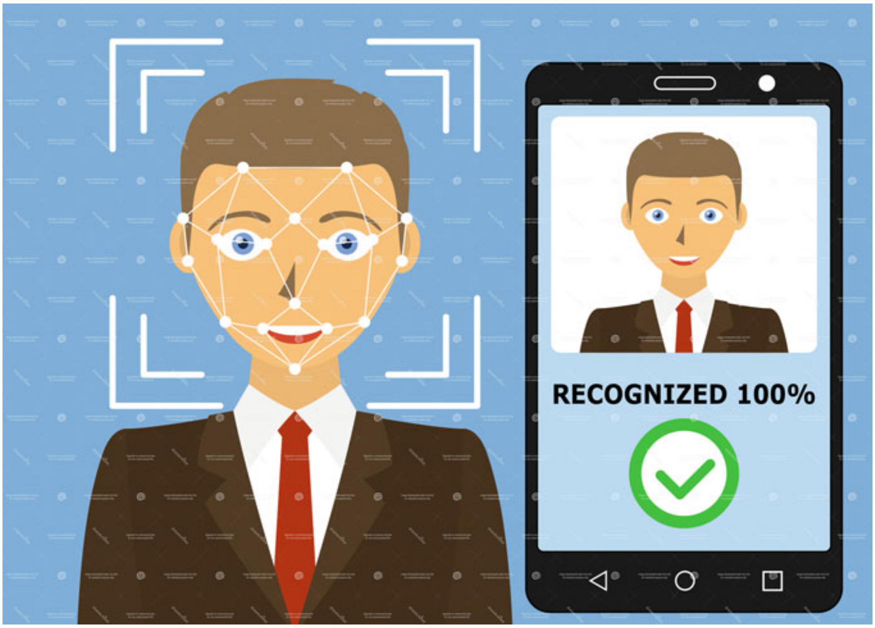

Fig. 1.1 Face biometrics for mobile user authentication

biometrics to log in users (Google has developed “Face Unlock” for Android 4.0).[4] It is reported that future versions of Android will be shipped with native support for more advanced and secure $3D$ face recognition algorithms,[5] similar to what Apple introduced under their “Face ID” moniker with iPhone X.

The applications of mobile biometrics are in border control, financial transactions, and physical and logical access control.

- **Border Control**: Passenger-friendly security is one of the primary concerns at high-volume border checkpoints such as airports. Mobile devices are exceedingly being utilized to facilitate customs and border crossings[6] to address such needs. As such, deployment of mobile devices is poised to automate the process of traveler identification and border security at checkpoints like airports and seaports in a secure yet user-friendly and private manner. Mobile passport apps are already taking advantage of modalities such as face to authenticate and process international travelers using their smartphones.[7]
- **Financial Market**: The democratization of financial services has gone hand-in-hand with the spread of mobile technologies, enabling consumers to have access

[4] https://www.technologyreview.com/s/425805/new-google-smart-phone-recognizes-your-face/.

[5] http://www.planetbiometrics.com/article-details/i/9918/desc/google-developing-3d-face-authentication/.

[6] https://www.airsidemobile.com.

[7] https://mobilepassport.us/faq.php.

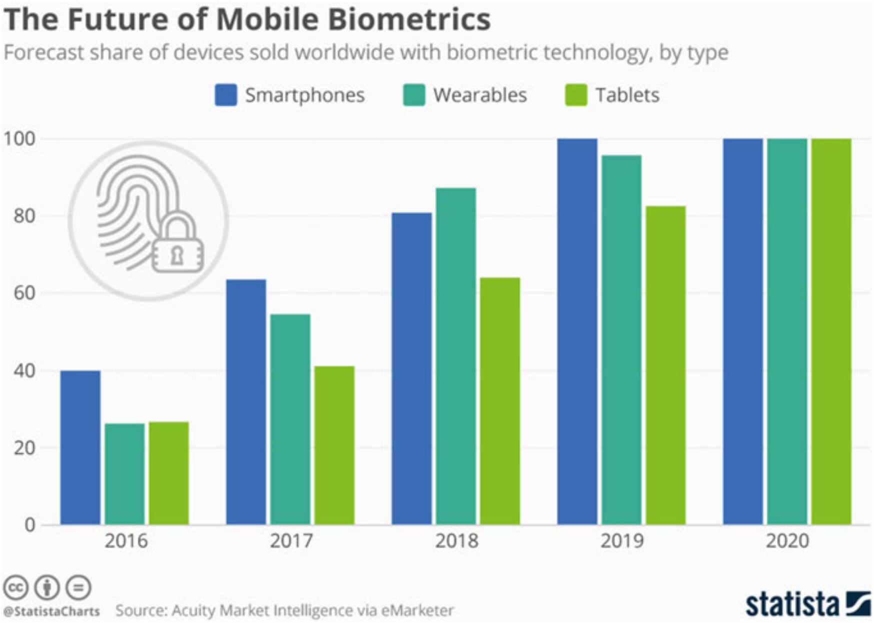

Fig. 1.2 Chart from Statista, biometrics to be installed on 100% of wearables and tablets by 2020. *Source* https://www.statista.com/chart/11122/the-future-of-mobile-biometrics/

to a wide swath of financial services without needing the traditional brick-and-mortar institutions, especially in developing markets. Examples include online shopping, micro-lending, immediate transfer of funds, or paying bills via mobile apps. Biometrics is increasingly being used to authenticate the involved parties in such transactions. Mobile wallets and other payment systems such as Apple Pay and Android Pay, along with major players like MasterCard[8] are utilizing smartphone-based biometric authentication for financial transactions.

- **Physical and Logical Access Control**: Access control is used to regulate restricted access to resources or a place. Physical and logical are the two main types of access control. While physical access control limits access to buildings, rooms, areas, and IT assets, logical access control limits connection to computer networks, system files, and data. The role of biometrics in physical and logical access control is to avoid illegal access by validating the identity of a user through biometric traits. These biometric-based access control solutions are better authentication methods compared to physical keys, key cards, and PINs because they cannot be lost, stolen, and easily compromised. Out of band authentication is one popular method where a mobile device is used to transmit the user's identity from his or her phone to a nearby logical or physical asset in need of user authentication, such as a personal computer or a smart lock.

[8] http://newsroom.mastercard.com/eu/press-releases/mastercard-makes-fingerprint-and-selfie-paymenttechnology-a-reality/.

Mobile biometrics aims to achieve conventional functionality and robustness while supporting portability, mobility, and user experience; bringing greater convenience and opportunity for deployment in a wide range of operational environments. The technology is expected to continue experiencing exponential growth due to increased consumer demand for convenient security. The Global Biometrics and Mobility Report in 2017 by Acuity Market Intelligence projected that global mobile biometric market revenues will reach 50.6 billion annually by 2022. This includes 2.7 billion biometrically enabled smart mobile devices generating 3.1 billion in biometric sensor revenue annually, 16.7 billion biometric app downloads generating 29.2 billion in annual revenues from direct purchase and software development fees, and 1.37 trillion biometrically secured payment and non-payment transactions generating 18.3 billion in annual authentication fees: http://www.acuity-mi.com/GBMR_Report.php/.

However, it is worth mentioning that classical methods for biometric recognition may not be readily adaptable to a mobile environment because of the following factors:

- Due to device mobility and operation in an uncontrolled environment, biometric samples acquired using a mobile phone's front-facing cameras are usually degraded due to factors such as specular reflection, motion blur, illumination variation, and background lighting, not to mention the inherent lower quality of front-facing cameras compared to the main back-facing modules used in smartphones. Therefore, more efficient and robust methods may be required for biometric integration in mobile devices.
- Although the computational power of mobile devices is proliferating, it still may not be sufficient for real-time operation of highly accurate and computationally costly methods for biometric authentication.

  Given that about 0.5 seconds is spent by the camera module to initialize, meter, and capture an image, an ideal biometric recognition module should take less than half a second for the whole process not to make more than a second, an essential factor in user experience.

Therefore, most of the proposed studies on mobile biometric methods have emphasized on developing computationally efficient methods (low memory and CPU impact) for accurate recognition of mobile use cases [11–13].

1.2 Selfie Biometrics

The storage and computational capability of smartphones have improved substantially over time. Figure 1.3 shows the enhancement in the storage capabilities of different models of flagship smartphones.

Chipsets from four leading vendors that power the handsets are as follows: Apple's 4-core A10 Fusion (iPhone 7/7 plus) and 6-core AI- and AR-optimized A11 Bionic

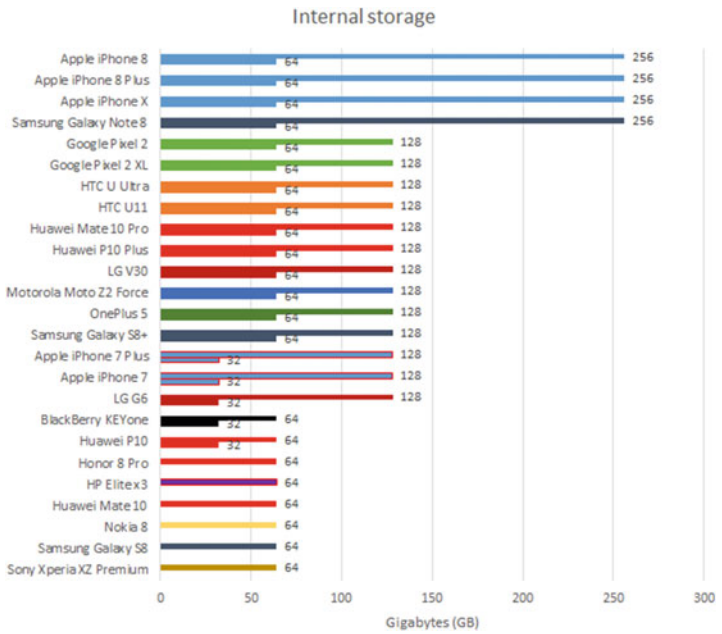

Fig. 1.3 Charts from ZDNet shows substantial improvement in storage capability of flagship smartphones. *Source* https://www.zdnet.com/article/flagship-smartphones-specs-benchmarks-and-prices-for-iphone-samsung-huawei-and-more//

(iPhone 8/8Plus/X). Samsung's 8-core Exynos 8995 in the Galaxy S8/S8+/Note 8 (worldwide versions). Qualcomm's mid-range 8-core Snapdragon 625 (BlackBerry KEYone and Motion); 4-core 820 (HP Elite x3) and 821 (HTC U Ultra, LG G6); and top-end 8-core 835 (Google Pixel 2/2XL, HTC U11+, LG V30, Moto Z2 Force, OnePlus 5T, Galaxy S8/S8+/Note 8 [US/China versions], Sony Xperia XZ Premium). HiSilicon's Kirin 960 in the Huawei P-series and Honor handsets, and the AI-optimized 8-core Kirin 970 in the new Huawei Mate 10 and 10 Pro.[9] Chart in Fig. 1.4 shows how these platforms measure up in terms of processor and graphics performance, as assessed by Primate Labs' multi-core Geekbench 4 (Gb4) and Futuremark's 3DMark Ice Storm Unlimited (ISU) benchmarks, respectively. This chart shows continuous improvement in the CPU and GPU performance over time.

The advancement in storage and computational performance, to a great extent, facilitate the use of *Selfie biometrics*. *In the context of mobile device, a selfie, by definition, is a self-portrait photograph, typically taken with a smartphone's camera while being held in hand or supported by a selfie stick. Selfie biometrics is, therefore, an authentication mechanism where a user captures images of her biometric traits (such as the face or ocular region) by using the imaging sensors available in the device itself.*

[9] https://www.zdnet.com/article/flagship-smartphones-specs-benchmarks-and-prices-for-iphone-samsung-huawei-and-more/.

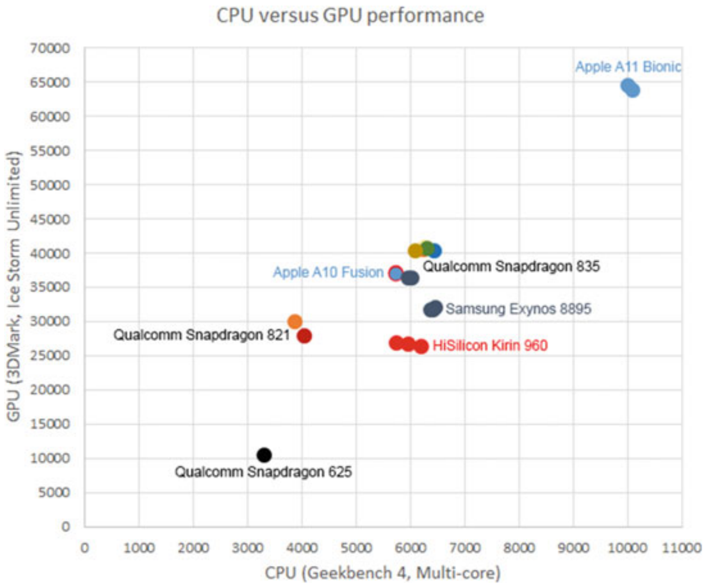

Fig. 1.4 Charts from ZDNet shows substantial improvement in computational capability of flagship smartphones. *Source* https://www.zdnet.com/article/flagship-smartphones-specs-benchmarks-and-prices-for-iphone-samsung-huawei-and-more//

The advantages of selfie biometrics include:

- **No Additional Hardware Needed**: As the mobile camera is used for selfie image acquisition, no additional hardware is needed for personal authentication in mobile devices.
- **High Acceptability and Usability**: Over 1 million selfies are taken each day globally (https://infogram.com/selfie-statistics-1g8djp917wqo2yw). Given the popularity of selfies, it is widely accepted as a means of mobile user authentication.

Challenges of selfie biometrics include intra-class variations such as poses, occlusion, low lighting, spectral reflection, and motion blur due to operation in a free mobile environment.

1.2.1 Types of Selfie Biometrics

1.2.1.1 Face

Figure 1.5 shows sample face images acquired using the front-facing camera of an iPhone 5*s*. The complete face recognition pipeline consists of selfie face acquisition, face detection, possibly normalization, and finally matching with one or more

Fig. 1.5 Example face images acquired using the front-facing camera of iPhone 5s

stored templates. Face normalization reduces the effect of intra-class variations such as lighting and poses variations through preprocessing, geometric frontalization, and registration routines. Most of the proposed studies on mobile face biometrics have emphasized developing computationally efficient methods (low memory and CPU impact) for face detection (such as optimized Viola–Jones) and recognition [5, 14–21]. Mobile face recognition methods can be broadly categorized into (a) client–server based and (b) device based [21]. In the client–server approach, face acquisition, face detection, and sometimes feature extraction routines are performed on the device side. The remaining computationally intensive tasks, such as classifier training and recognition, are performed on the server. In the device-based approach, all of the operations are performed within the device and exceedingly using secure hardware pipelines. The templates themselves are usually stored on the device, especially with native OEM implementations. However, third-party apps may store templates on secure servers via their cloud services. Of late, deep learning such as CNN solutions have been successfully ported into mobile phones, and they are working with very high accuracy and speed both on the device- and server-side [22] applications. One widely deployed commercial example is Face++ (https://www.faceplusplus.com/)).

1.2.1.2 Ocular

Ocular biometrics encompasses the imaging and use of characteristic features extracted from the eyes for personal recognition. Ocular biometric modalities in visible light have mainly focused on iris, blood vessel structures over the white of the eye (mostly due to conjunctival and episcleral layers), and the periocular region around the eye. Figure 1.7 shows an example of an eye image labeled with iris, conjunctival vasculature, and periocular region. Textural descriptors (such as LBP,

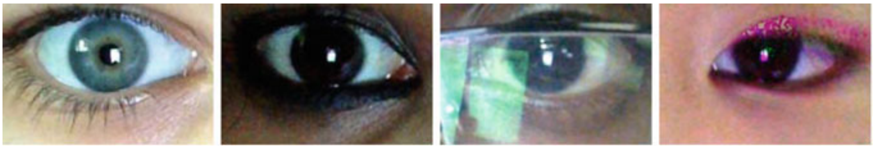

Fig. 1.6 Sample eye images acquired using iPhone 5s containing variations such as **a** light and **b** dark irides, **c** reflection, and **d** imaging artifact

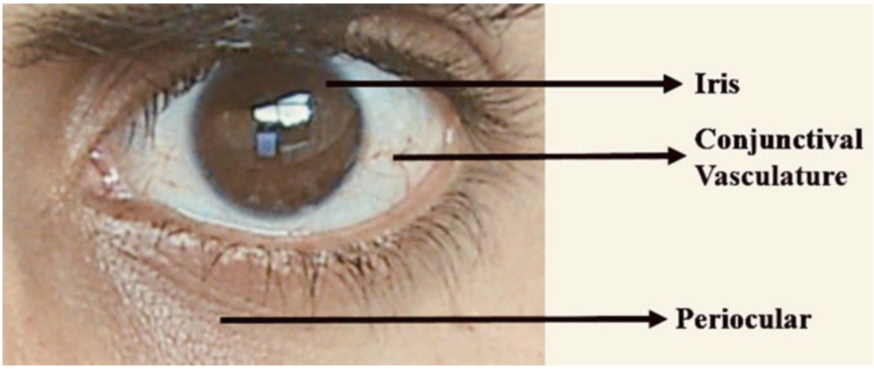

Fig. 1.7 Example eye image labeled with iris, conjunctival vasculature, and periocular region

LQP, and BSIF) and deep learning-based CNNs have been mostly used for identity verification in mobile ocular biometrics [23–26]. In 2016, a large-scale competition was conducted on Mobile Ocular Biometric Recognition on VISOB dataset [27]. Figure 1.6 shows substantial variations in the ocular images captured using the front-facing camera of iPhone 5s from publicly available VISOB mobile ocular biometrics dataset [27].

1.2.1.3 Fingerphoto

There has been a recent trend in touchless fingerprint recognition technology, where the back-facing smartphone cameras acquire high-resolution photographs of finger ridge patterns. This mobile modality is henceforth referred to as fingerphotos[10] [8, 28]. Fingerphoto authentication methods may offer an economical alternative to traditional fingerprint systems for mobile use cases as they avoid the need for extra hardware [29]. The further advantages of the touchless finger photo authentication methods over traditional touch-based fingerprint include being hygienic and removing the risk of leaving latent prints on the sensor. Furthermore, there are no finger impression deformations in the acquired images that could be caused by pressing the

[10] Though not a traditional selfie capture per se, and given its commonalities with selfie mobile biometrics, we have included it among other selfie modalities.

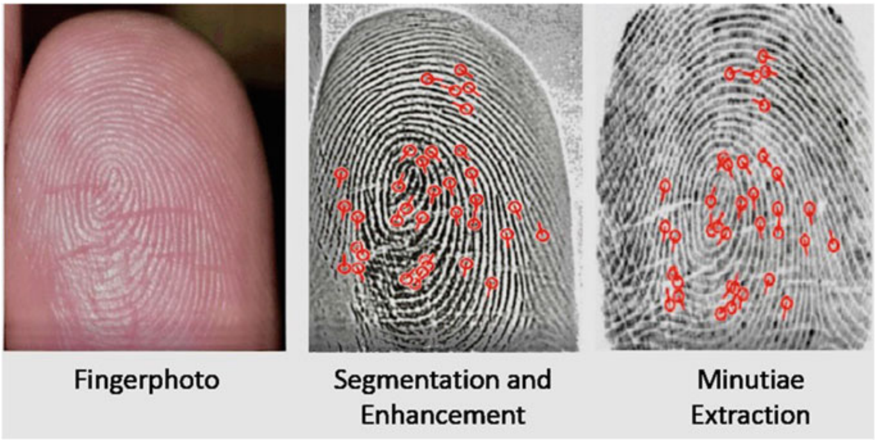

Fig. 1.8 Complete pipeline of fingerphoto-based system in mobile devices

finger on a touch-based sensor. Low-quality fingerprints due to low pressure or dry skin may also be mitigated by such touchless photographic fingerprint acquisition.

A typical pipeline for finger photo authentication system consists of imaging one or more fingers (with or without flash) with a high-quality back-facing mobile camera from a short distance. This is followed by image segmentation, enhancement, and minutiae extraction. The extracted minutiae form the template that is subsequently matched with an enrolled reference to establish the identity of the mobile user (see Fig. 1.8). Some of the finger photo challenges include the improper focus of the camera due to which ridge patterns of the finger may not be captured. Further, various potential poses of the finger must be considered: the orientation angle, pitch angle, and position of the finger, as well as the distance of the finger to the camera and the background.

1.2.2 Selfie Biometrics and Spoof Attacks

As the use of biometrics for smartphone user authentication continues to increase, capabilities to detect spoof attacks are needed to alleviate user concerns. A spoof attack occurs when an adversary mimics the biometric trait of another individual to circumvent the system for illegitimate access and advantages [30]. These attacks may pose a serious threat because they can be executed at the sensor (camera) level without requiring any technical knowledge of the functioning of the biometric system. Lack of efficient anti-spoofing and liveness detection methods may create a formidable psychological barrier in the mass adoption of biometrics in mobile applications. Therefore, there is a pressing need for the development of robust countermeasures against spoof attacks for mobile biometrics.

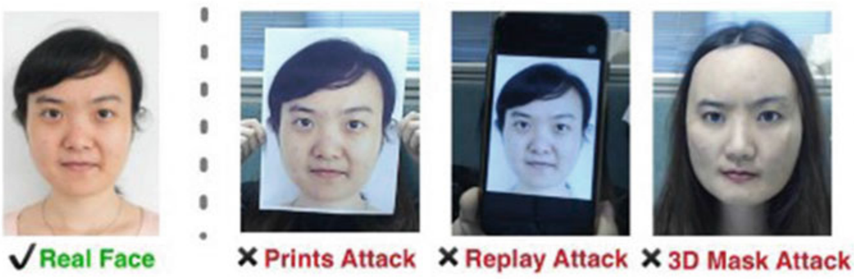

Fig. 1.9 Example of print, replay, and 3D mask attacks for face biometrics in mobile device [31]

In context of selfie biometrics, spoof attacks mainly consist of (i) *print attacks*, (ii) *photograph attacks*, and (iii) *replay attacks*. Print and photograph attacks can be executed using a selfie photograph of the enrolled user, which may be displayed in hard copy (2D or 3D) or on a screen to the mobile device. The video replay attacks are performed by displaying a video on a mobile screen. Anti-spoofing countermeasures aim to disambiguate live, and real face captures from spoof counterparts to avoid spoof attacks in mobile devices.

Face: Figure 1.9 shows example of print and replay attacks for face biometrics in the mobile device. Apart from print and photograph attacks, face recognition is also subject to 3D face mask attacks which require high-resolution fabrication system capturing the 3D shape and texture information of the target subject's face. However, print and replay attacks can be launched more easily by malicious users than 3D mask attacks.

The existing countermeasures can be coarsely classified into motion analysis-based [32–35], texture-based [36–44], image-quality based [39, 45–47], and deep learning-based (which can be considered as an end-to-end data-driven spoofing artifact feature extractor and classifier) [48]. Motion analysis-based methods can be considered as liveness detection, and texture, image quality and deep learning-based methods can be considered as spoof detection methods (since they mostly detect artifacts and distortions arising from spoofing methods).

Fingerphoto: The types of spoof attacks for finger photo can be photograph, print, and spoofs fabricated using material such as gelatin and latex. Countermeasures include use of textural descriptors such as local binary patterns, dense scale invariant feature transform, and locally uniform comparison image descriptor features combined with with classifiers such as support vector machine (SVM) [49], use of challenge response [50] and deep convolutional neural networks (which combines feature extraction and classification steps of the earlier mentioned methods) [51].

Ocular: Apart from photograph and print attacks, spoof attacks for ocular or iris biometrics may include the use of artificial eyes and patterned lenses. Common countermeasures include use of local and global textural descriptors such as LBP and GLCM [52], eye motion analysis, and convolutional neural networks, similar to face anti-spoofing [53].

1.2.3 Selfie and Cloud-Based Services

The significant challenge associated with selfie biometrics is the limited availability of resources—within the smartphone—for storage and computation. Therefore, it may be necessary in some cases to outsource the computing and storage demands to a more powerful server outside the smartphone. In this regard, cloud computing may be harnessed as a viable option [54, 55]. Cloud computing facilitates the outsourcing of computing and storage tasks to infrastructures managed by dedicated providers a potential approach to surpassing mobile resource limits. For instance, the feature extraction, data storage, and matching components of a biometric system can be moved to a cloud infrastructure, while leaving only the sensing task in the smartphone. There is an increased interest in performing biometric recognition in mobile devices and as a cloud-based service [54, 56, 57]. If the biometrics-in-the-cloud architecture is offered by a service provider, then it is referred to as Biometrics-as-a-Service (BaaS). If the infrastructure allows for component developers to develop and incorporate custom components in the cloud (e.g., feature extraction or matcher modules), then it is referred to as Platform-as-a-Service (PaaS). This paper in [54] presents a framework for Biometrics-as-a-Service (BaaS) that performs biometric matching operations in the cloud while relying on simple and ubiquitous consumer devices such as a smartphone.

1.2.4 Selfie and Soft Biometrics

Apart from biometric authentication using selfie images, several soft-biometric attributes can also be extracted from selfie captures. These soft-biometric attributes may include eyeglasses, gender, age, and clothing, which can be used in the absence of primary biometric trait, or conjunction with a primary biometric trait for performance enhancement. Also, these soft-biometric traits can also be used for continuous user authentication to verify that the user initially authenticated is still the user in control of the device [58]. Selfie soft biometrics including gender [59–61], age [62], eyeglasses [63], eyebrows [64], and clothing information [65] have been studied for use with mobile face and ocular modalities for performance enhancement and continuous user authentication (see Fig. 1.10). Further study in [66] proposed a combination of soft-biometric attributes such as face shape, skin tone, hair color, eyeglasses, ethnicity, and gender for continuous user authentication in mobile devices.

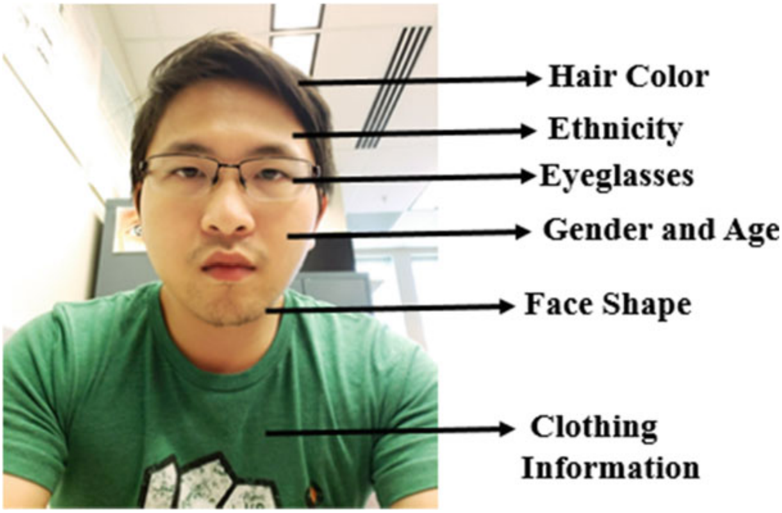

Fig. 1.10 Example of soft-biometric attributes from selfie images

1.3 Challenges and Future Directions

One of the main challenges in selfie biometrics involves developing accurate and computationally efficient methods for the mobile environment. Due to data acquisition in a mobile and uncontrolled environment, the acquired samples may exhibit substantial intra-class variations. This can lower the accuracy of the system and may even frustrate users of the devices.

A recent survey [21] suggests an average reported face recognition accuracy of 92.3% in a mobile environment. However, most of the existing methods are evaluated on in-house mobile datasets of limited size. Therefore, the relevance of the reported results cannot be established.

Reported error rates regarding the performance of proposed countermeasures against spoof attacks [21] in mobile devices are usually high, especially for replay attacks. This suggests the need for advanced and accurate methods for liveness and spoof detection for selfie biometrics. Continuous advancement in spoofing techniques will lead to novel methods for spoof attacks. There is an immediate need for designing a liveness detection/ anti-spoof method that is robust across new spoof attacks [67]. Therefore, the development of advanced and open-set liveness/ anti-spoof detection methods for known and novel spoof attacks should be the path forward.

With the advancement in mobile technology, deep learning-based solutions became viable for client-oriented and cloud-based mobile biometrics applications. Consequently, deep learning-based solutions for accurate recognition and anti-spoofing should be developed. Advanced loss functions such as triplet- [68] and center-loss [69] should be utilized for the task. There is a room for the development of a framework for Biometrics-as-a-Service that performs selfie matching operations in the cloud. Dynamic fusion framework needs to be developed for combining available soft-biometric attributes from selfie images for performance enhancement. Efforts should also be directed toward large-scale database collection for selfie face images to evaluate and compare deep learning solutions on a common test set.

1.4 Conclusion

Recently, several papers have been published on the topic of selfie biometrics. This book describes the state-of-the-art in selfie biometrics with a focus on the face, ocular, and finger modalities. This introductory chapter has described the notion of selfie biometrics and summarized the notable state of the art on this topic. This chapter will be followed by individual chapters covering: various selfie modalities, the methods of selfie-based mobile user authentication, predicting soft biometrics for performance enhancement and continuous authentication, anti-spoofing (measures and robustness), quality, privacy, security, and usability of selfie biometrics.

References

1. Jain A, Ross A, Nandakumar A (2011) Introduction to biometrics. Springer Publishers
2. Han S, Park H, Cho D, Park D, Lee S (2007) Face recognition based on near-infrared light using mobile phone. In: Beliczynski B, Dzielinski A, Iwanowski M, Ribeiro B (eds) Adaptive and natural computing algorithms, vol 4432. Lecture Notes in Computer Science. Springer, Heidelberg, pp 440–448
3. Jung S, Chung Y, Yoo J, Moon K (2008) Real-time face verification for mobile platforms. In: Bebis G, Boyle R, Parvin B, Koracin D, Remagnino P, Porikli F, Peters J, Klosowski J, Arns L, Chun Y, Rhyne T, Monroe L (eds) Advances in visual computing, vol 5359. Lecture Notes in Computer Science. Springer, Heidelberg, pp 823–832
4. Tao Q, Veldhuis R (2006) Biometric authentication for a mobile personal device. In: Third annual international conference on mobile and ubiquitous systems: networking services, San Jose, CA, pp 1–3
5. Walgamage T, Farook C (2014) A real-time hybrid approach for mobile face recognition. In: International conference on intelligent systems, modelling and simulation, pp 1–6
6. Rattani A, Derakhshani R (2017) Ocular biometrics in the visible spectrum: a survey. Image Vis Comput 59:1–16
7. Rattani A, Derakhshani R (2017) On fine-tuning convolutional neural networks for smartphone based ocular recognition. In: IEEE international joint conference on biometrics (IJCB), pp 762–767
8. Sankaran A, Malhotra A, Mittal A, Vatsa M, Singh R (2015) On smartphone camera based fingerphoto authentication. In: IEEE 7th international conference on biometrics theory, applications and systems, pp 1–7
9. Maiorana E, Campisi P, González-Carballo N, Neri A (2011) Keystroke dynamics authentication for mobile phones. In: ACM symposium on applied computing, New York, NY, USA, pp 21–26

10. Derawi MO, Nickel C, Bours P, Busch C (2010) Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: Sixth international conference on intelligent information hiding and multimedia signal processing, pp 306–311
11. Tao Q, Veldhuis R (2010) Biometric authentication system on mobile personal devices. IEEE Trans Instrum Measur 59(4):763–773
12. Chen B, Shen J, Sun H (2012) A fast face recognition system on mobile phone. In: International conference on systems and informatics, Yantai, pp 1783–1786
13. Yang J, Chen X, Kunz W (2002) A PDA-based face recognition system. In: Sixth IEEE workshop on applications of computer vision, pp 19–23
14. Doukas C, Maglogiannis I (2010) A fast mobile face recognition system for android os based on eigenfaces decomposition. In: Papadopoulos H, Andreou A, Bramer M (eds) Artificial intelligence applications and innovations, vol 339. IFIP Advances in Information and Communication Technology. Springer, Heidelberg, pp 295–302
15. Kumar S, Singh P, Kumar V (2010) Architecture for mobile based face detection/recognition. Int J Comput Sci Eng 2(3):889–894
16. Yu H (2010) Face recognition for mobile phone using eigenfaces. University of Michigan, Tech. rep
17. Findling RD, Mayrhofer R (2012) Towards face unlock: on the difficulty of reliably detecting faces on mobile phones. In: International conference on advances in mobile computing and multimedia, Bali, Indonesia, pp 275–280
18. Kremic E, Subasi A, Hajdarevic K (2012) Face recognition implementation for client server mobile architecture. In: International conference on information technology interfaces, Dubrovnik, Croatia, pp 435–440
19. Mukherjee S, Chen Z, Gangopadhyay A, Russell A (2008) A secure face recognition system for mobile-devices without the need of decryption. In: Workshop on secure knowledge management, pp 11–16
20. Schneider C, Esau N, Kleinjohann L, Kleinjohann B (2006) Feature based face localization and recognition on mobile devices. In: International conference on control, automation, robotics and vision, Singapore, pp 1–6
21. Rattani A, Derakhshani R (2018) A survey of mobile face biometrics. Comput Electr Eng 72:39–52. https://doi.org/10.1016/j.compeleceng.2018.09.005, http://www.sciencedirect.com/science/article/pii/S004579061730650X
22. Gnther M, Costa-Pazo A, Ding C, Boutellaa E, Chiachia G, Zhang H, de Assis Angeloni M, Truc V, Khoury E, Vazquez-Fernandez E, Tao D, Bengherabi M, Cox D, Kiranyaz S, de Freitas Pereira T, Ganec Gros J, Argones-Ra E, Pinto N, Gabbouj M, Simes F, Dobriek S, Gonzlez-Jimnez D, Rocha A, Neto MU, Pavei N, Falco A, Violato R, Marcel S (2013) The 2013 face recognition evaluation in mobile environment. In: International conference on biometrics, Madrid, pp 1–7
23. Das A, Pal U, Ballester M, Blumenstein M (2014) A new efficient and adaptive sclera recognition system. In: IEEE symposium on computational intelligence in biometrics and identity management (CIBIM), pp 1–8
24. Park U, Ross A, Jain A (2009) Periocular biometrics in the visible spectrum: a feasibility study. In: IEEE 3rd international conference on biometrics: theory applications and systems, pp 1–6
25. Marsico MD, Nappi M, Proena H (2017) Results from miche ii mobile iris challenge evaluation ii, Pattern Recogn Lett 91(C):3–10
26. Reddy N, Rattani A, Derakhshani R (2018) Ocularnet: deep patch-based ocular biometric recognition. In: 2018 IEEE international symposium on technologies for homeland security (HST), pp 1–6. https://doi.org/10.1109/THS.2018.8574156
27. Rattani A, Derakhshani R, Saripalle SK, Gottemukkula V (2016) ICIP 2016 competition on mobile ocular biometric recognition. In: IEEE International Conference on image processing, challenge session on mobile ocular biometric recognition, Phoenix, AZ, pp 320–324
28. Stein C, Nickel C, Busch C (2012) Fingerphoto recognition with smartphone cameras. In: BIOSIG—Proceedings of the international conference of biometrics special interest group, pp 1–12

29. Carney LA, Kane J, Mather JF, Othman A, Simpson AG, Tavanai A, Tyson RA, Xue Y (2017) A multi-finger touchless fingerprinting system: mobile fingerphoto and legacy database interoperability. In: Proceedings of the 2017 4th international conference on biomedical and bioinformatics engineering, ICBBE 2017, New York, NY, USA, pp 139–147
30. Chingovska I, dos Anjos AR, Marcel S (2014) Biometrics evaluation under spoofing attacks. IEEE Trans Inf Forensics Secur 9(12):2264–2276
31. Liu S, Yang B, Yuen P, Zhao G (2016) A 3D mask face anti-spoofing database with real world variations. In: The IEEE conference on computer vision and pattern recognition (CVPR) workshops, pp 1551–1557
32. Patel K, Han H, Jain AK (2016) Cross-database face antispoofing with robust feature representation. In: You Z, Zhou J, Wang Y, Sun Z, Shan S, Zheng W, Feng J, Zhao Q (eds) Biometric recognition. Springer International Publishing, Cham, pp 611–619
33. Siddiqui IA, Bharadwaj S, Dhamecha TI, Agarwal A, Vatsa M, Singh R, Ratha N (2016) Face anti-spoofing with multifeature videolet aggregation. In: International conference on pattern recognition, Cancun, pp 1035–1040
34. Tirunagari S, Poh N, Windridge D, Iorliam A, Suki N, Ho ATS (2015) Detection of face spoofing using visual dynamics. IEEE Trans Inf Forensics Secur 10(4):762–777
35. Pinto A, Pedrini H, Schwartz WR, Rocha A (2015) Face spoofing detection through visual codebooks of spectral temporal cubes. IEEE Trans Image Process 24(12):4726–4740
36. Akhtar Z, Michelon C, Foresti GL (2014) Liveness detection for biometric authentication in mobile applications. In: 2014 international Carnahan conference on security technology, Rome, pp 1–6
37. Chingovska I, Anjos A, Marcel S (2012) On the effectiveness of local binary patterns in face anti-spoofing. In: International conference of biometrics special interest group (BIOSIG), Germany, pp 1–7
38. Boulkenafet Z, Komulainen J, Li L, Feng X, Hadid A (2017) OULU-NPU: a mobile face presentation attack database with real-world variations. In: IEEE international conference on automatic face gesture recognition, Washington, DC, pp 612–618
39. Costa-Pazo A, Bhattacharjee S, Vazquez-Fernandez E, Marcel S (2016) The replay-mobile face presentation-attack database. In: International conference of the biometrics special interest group, Germany, pp 1–7
40. Boulkenafet Z, Komulainen J, Hadid A (2016) Face spoofing detection using colour texture analysis. IEEE Trans Inf Forensics Secur 11(8):1818–1830
41. Arashloo SR, Kittler J, Christmas W (2015) Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features. IEEE Trans Inf Forensics Secur 10(11):2396–2407
42. Gan J, Li S, Zhai Y, Liu C (2017) 3D convolutional neural network based on face anti-spoofing. In: International conference on multimedia and image processing, Wuhan, pp 1–5
43. Atoum Y, Liu Y, Jourabloo A, Liu X (2017) Face anti-spoofing using patch and depth-based CNNs. In: IEEE international joint conference on biometrics, Denver, CO, pp 319–328
44. Pereira F, Komulainen J, Anjos A, Martino MD, Hadid A, Pietikäinen M, Marcel S (2014) Face liveness detection using dynamic texture. EURASIP J Image Video Process 2014(1):2
45. Patel K, Han H, Jain AK, Ott G (2015) Live face video vs. spoof face video: use of moire patterns to detect replay video attacks. In: International conference on biometrics, Phuket, pp 98–105
46. Wen D, Han H, Jain AK (2015) Face spoof detection with image distortion analysis. IEEE Trans Inf Forensics Secur 10(4):746–761
47. Galbally J, Marcel S (2014) Face anti-spoofing based on general image quality assessment. In: International conference on pattern recognition, Stockholm, pp 1173–1178
48. Boulkenafet Z, Komulainen J, Akhtar Z, Benlamoudi A, Samai D, Bekhouche SE, Ouafi A, Dornaika F, Taleb-Ahmed A, Qin L, Peng F, Zhang LB, Long M, Bhilare S, Kanhangad V, Costa-Pazo A, Vazquez-Fernandez E, Perez-Cabo D, Moreira-Perez JJ, Gonzalez-Jimenez D, Mohammadi A, Bhattacharjee S, Marcel S, Volkova S, Tang Y, Abe N, Li L, Feng X, Xia Z, Jiang X, Liu S, Shao R, Yuen PC, Almeida WR, Andalo F, Padilha R, Bertocco G, Dias W,

Wainer J, Torres R, Rocha A, Angeloni MA, Folego G, Godoy A, Hadid A (2017) A competition on generalized software-based face presentation attack detection in mobile scenarios. In: IEEE international joint conference on biometrics, Denver, CO, pp 688–696

49. Taneja A, Tayal A, Malhorta A, Sankaran A, Vatsa M, Singh R (2016) Fingerphoto spoofing in mobile devices: a preliminary study. In: IEEE international conference on biometrics theory, applications and systems, pp 1–7
50. Stein C, Bouatou V, Busch C (2013) Video-based fingerphoto recognition with anti-spoofing techniques with smartphone cameras. In: International conference of the BIOSIG Special Interest Group (BIOSIG), pp 1–12
51. Fujio M, Kaga Y, MurakamiT, Ohki T, Takahashi K (2018) Face/fingerphoto spoof detection under noisy conditions by using deep convolutional neural network. In: International joint conference on biomedical engineering systems and technologies, pp 54–62
52. Sequeira AF, Murari J, Cardoso JS (2014) Iris liveness detection methods in the mobile biometrics scenario. In: International joint conference on neural networks (IJCNN), pp 3002–3008
53. Sequeira AF, Oliveira HP, Monteiro JC, Monteiro JP, Cardoso JS (2014) Mobilive 2014 mobile iris liveness detection competition. In: IEEE international joint conference on biometrics, pp 1–6
54. Talreja V, Ferrett T, Valenti MC, Ross A (2018) Biometrics-as-a-service: a framework to promote innovative biometric recognition in the cloud. In: IEEE international conference on consumer electronics (ICCE), pp 1–6
55. Mell P, Granc T (2011) The nist definition of cloud computing. Tech. rep, Recommendations of the National Institute of Standards and Technology
56. Chow R, Jakobsson M, Masuoka R, Molina J, Niu Y, Shi E, Song Z (2010) Authentication in the clouds: a framework and its application to mobile users. In: ACM cloud computing security workshop (CCSW), New York, NY, USA, pp 1–6
57. Barra S, Casanova A, Narducci F, Ricciardi S (2015) Ubiquitous iris recognition by means of mobile devices. Pattern Recogn Lett 57:66–73
58. Patel VM, Chellappa R, Chandra D, Barbello B (2016) Continuous user authentication on mobile devices: recent progress and remaining challenges. IEEE Signal Process Mag 33(4):49–61
59. Rattani A, Reddy N, Derakhshani R (2017) Gender prediction from mobile ocular images: a feasibility study. In: IEEE international symposium on technologies for homeland security, pp 1–6
60. Buriro A, Akhtar Z, Crispo B, Frari FD (2016) Age, gender and operating-hand estimation on smart mobile devices. In: International conference of the biometrics special interest group, pp 1–5
61. Rattani A, Reddy N, Derakhshani R (2018) Convolutional neural networks for gender prediction from smartphone-based ocular images. IET Biometrics 7:423–430
62. Rattani A, Reddy N, Derakhshani R (2017) Convolutional neural network for age classification from smart-phone based ocular images. In: 2017 IEEE international joint conference on biometrics (IJCB), pp 756–761. https://doi.org/10.1109/BTAS.2017.8272766
63. Mohammad AS, Rattani A, Derahkshani R (2017) Eyeglasses detection based on learning and non-learning based classification schemes. In: IEEE international symposium on technologies for homeland security (HST), pp 1–5. https://doi.org/10.1109/THS.2017.7943484
64. Mohammad AS, Rattani A, Derakhshani R (2018) Short-term user authentication using eyebrows biometric for smartphone devices. In: IEEE computer science and electronic engineering conference, pp 1 – 6
65. Nguyen H, Sai R, Li Z, Derakhshan R (2018) User re-identification using clothing information for smartphones. In: IEEE international symposium on technologies for homeland security (HST), pp 1–5
66. Samangouei P, Patel VM, Chellappa R (2015) Attribute-based continuous user authentication on mobile devices. In: IEEE 7th international conference on biometrics theory, applications and systems (BTAS), pp 1–8

67. Rattani A, Scheirer WJ, Ross A (2015) Open set fingerprint spoof detection across novel fabrication materials. IEEE Trans Inf Forensics Secur 10(11):2447–2460
68. Schroff F, Kalenichenko D, Philbin J. FaceNet: a unified embedding for face recognition and clustering, CoRR abs/1503.03832
69. Wen Y, Zhang K, Li Z, Qiao Y (2016) A discriminative feature learning approach for deep face recognition. In: Leibe B, Matas J, Sebe N, Welling M (eds) European conference on computer vision. Cham, pp 499–515