Chapter 12
Active Authentication on Mobile Devices

Pramuditha Perera and Vishal M. Patel

Abstract In recent years, we have witnessed a significant growth in the use of mobile devices such as smartphones and tablets. In this context, security and privacy in mobile devices becomes vital as the loss of a mobile device could compromise personal information of the user. To deal with this problem, Active Authentication (AA) systems have been proposed in the literature where users are continuously monitored after the initial access to the mobile device. In this chapter, we provide a survey of recent face-based AA methods.

12.1 Introduction

Traditional methods for authenticating users on mobile devices are based on explicit authentication mechanisms such as passwords/ pin numbers or secret patterns. Studies have shown that users often choose a simple, easily guessable password like "12345," "abc1234," or even "password" to protect their data [1, 2]. As a result, hackers could easily break into many accounts just by trying most commonly used passwords. On the other hand, when a secret pattern is used to gain initial access to the mobile device, the user would draw the same pattern multiple times on the screen over the time. It has been shown that with special lighting and high-resolution photograph, one can easily deduce the secret pattern (see Fig. 12.1) [3] using the oily residues or smudges left on the screen.

Furthermore, recent studies have shown that about 34% or more users did not use any form authentication mechanism on their devices [4–7]. In these studies, inconvenience was cited to be one of the main reasons why users did not use any authentication mechanism on their devices [6, 7]. Moreover, [7] demonstrated that mobile device users considered unlock screens unnecessary in 24% of the situations and they spent up to 9% of time they use their smartphone to deal with unlock screens.

P. Perera · V. M. Patel (✉)
Johns Hopkins University, Baltimore, MD, USA
e-mail: vpatel36@jhu.edu

P. Perera
e-mail: pperera3@jhu.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_12

Fig. 12.1 Smudge attack [3]. Secret pattern can be determined with special lighting and high-resolution camera

Furthermore, as long as the mobile phone remains active, typical devices incorporate no mechanisms to verify whether the user originally authenticated is still the user in control of the device. Thus, unauthorized individuals could potentially obtain access to personal information of the user if a password is compromised or if the user does not exercise adequate vigilance after initial authentication on a device.

In order to overcome these issues, both biometrics and security research communities have developed techniques for continuous authentication on mobile devices. These methods essentially make use of the physiological and behavioral biometrics using the built-in sensors and accessories such as gyroscope, touchscreen, accelerometer, orientation sensor, and pressure sensor to continuously monitor the user identity. For instance, physiological biometrics such as face can be captured using the front-facing camera of a mobile device and can be used to continuously authenticate a mobile device user. On the other hand, sensors such as gyroscope, touchscreen, and accelerometer can be used to measure behavioral biometric traits such as gait, touch gestures, and hand movement transparently. Figure 12.2 highlights some of the sensors and accessories available in a modern mobile device. These sensors are capable of providing raw data with high precision and accuracy. Therefore, they can be used to monitor three-dimensional device movement, device positioning, and changes in ambient environment near the device. Note that the terms continuous authentication, Active Authentication [8], implicit authentication [9, 10], and transparent authentication [11] have been used interchangeably in the literature.

12.2 Common AA Approaches

Figure 12.3 shows the typical setup of a biometrics-based mobile device continuous authentication system [12]. Biometric modalities such as gait, face, keystroke, or voice are measured by the sensors and accessories that are available in the mobile device. Then, the biometric system determines whether these biometric traits correspond to a legitimate user or not. If the features do correspond to the legitimate user, the biometric system will continue to process new incoming data. However, if the biometric system produces a negative response then the system will prompt the

Fig. 12.2 Sensors and accessories available in a mobile device. Raw information collected by these sensors can be used to continuously authenticate a mobile device user

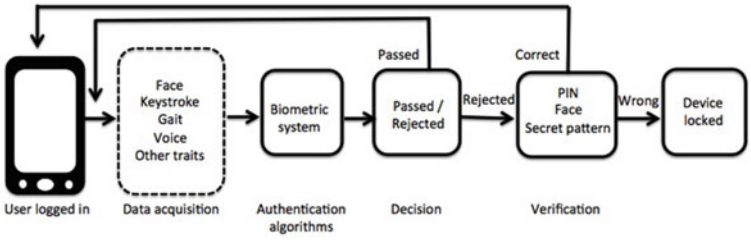

Fig. 12.3 A biometrics-based mobile continuous authentication framework [12]

user to verify his or her identity by using a traditional explicit authentication method. If the user is able to verify his identity, then he will be allowed to use the mobile device. Otherwise, the device will be locked. In a practical continuous authentication system, this entire process happens in real time.

A plethora of mobile continuous authentication methods have been proposed in the literature. Screen-touch gestures are one of the earliest modalities proposed for Active Authentication. Screen-touch gestures are basically the way users swipe their fingers on the screen of mobile devices. They have been used to continuously authenticate users while users perform basic operations on the phone [13–18]. In these methods, a behavioral feature vector is extracted from the recorded screen-touch data and a discriminative classifier is trained on these features for authentication. Touch gestures along with the micro-movement of the device caused by user's screen-touch actions have also been used for authentication in [19]. Stylometry, GPS location, Web browsing behavior, and application usage patterns were used in [20] for continuous

authentication. Face-based continuous user authentication has also been proposed in [21–24]. Gait as well as device movement patterns measured by the smartphone accelerometer were used in [25, 26] for continuous authentication. Fusion of speech and face was proposed in [21] while [27] proposed to fuse face images with the inertial measurement unit data to continuously authenticate the users. A low-rank representation-based method was proposed in [28] for fusing touch gestures with faces for continuous authentication. A domain adaptation method was proposed in [29] for dealing with data mismatch problem in continuous authentication. Some of the other continuous authentication methods are based on Web browsing behavior [30], behavior profiling [31], text-based [32, 33], and body prints [34].

12.3 Face-Based AA Methods

The face modality is one of the widely used biometric modalities in Active Authentication. Such systems typically consist of three main stages. In the first stage, faces are detected from the images or videos captured by the front-facing cameras of smartphones. Then, holistic or local features are extracted from the detected faces. Finally, these features are passed on to a classifier for authentication. A number of different methods have been proposed in the literature for detecting and recognizing faces on mobile devices. In what follows, we provide a brief overview of recent face-based AA methods that have been proposed recently in the literature [23, 35–41].

In [24], the feasibility of face and eye detection on mobile phones was evaluated using AdaBoost cascade classifiers with Haar-like and LBP features as well as a skin color-based detector. On a Nokia N90 mobile phone that has an ARM9 220 MHz processor and a built-in memory of 31 MB, their work reported that the Haar + AdaBoost method can detect faces in 0.5 s from 320 $\times$ 240 images. This approach, however, is not effective when wide variations in pose and illumination are present or the images contain partial or clipped images. To deal with these issues, a deep convolutional neural network (DCNN)-based method was recently developed in [42] for detecting faces on mobile platforms. In this method, deep features are first extracted using the first five layers of AlexNet [43]. Different-sized sliding windows are considered, to account for faces of different sizes, and an SVM is trained for each window size to detect faces of that particular size. Then, detections from all the SVMs are pooled together and some candidates are suppressed based on overlap criteria. Finally, a single bounding box is generated as the output by the detector. It was shown that this detector is quite robust to illumination change and is able to detect partial or extremely profile faces. A few sample positive detections from the UMDAA dataset [22] are shown in Fig. 12.4. The DCNN-based detections are marked in red, while the ground truth is in shown yellow. Another part-based method for detecting partial and occluded faces on mobile devices was developed in [44]. This method is based on detecting facial segments in the given frame and clustering them to obtain the region that is most likely to be a face.

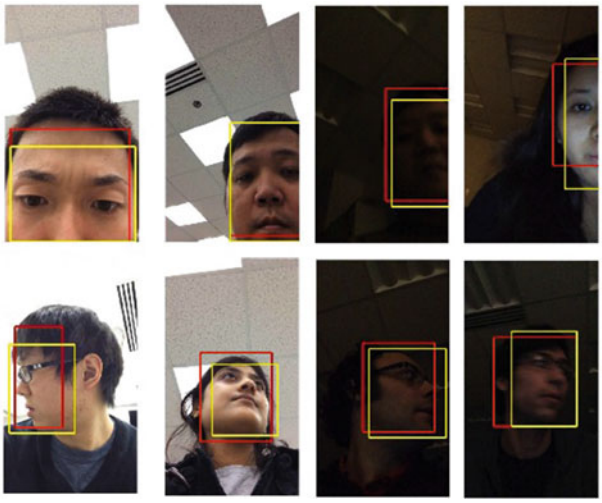

Fig. 12.4 Examples of positive detections with pose variations and occlusion on the UMDAA dataset. The detector's output is in red, while ground truth is in yellow [42]

Several works in the literature have used face recognition-based algorithms to perform Active Authentication. In [45], a AA method was proposed based on one-class SVM. In their approach, faces are detected using the Viola–Jones detector [46]. Histogram equalization is then applied on the detected images to normalize the effect of illumination. Finally, two-dimensional Fourier transform features are extracted from the normalized images and fed into one-class SVM for authentication. In [24], a face and eye detection scheme has been introduced along with a LBP feature-based face recognition method designed for mobile devices. It was shown that their proposed continuous face authentication system can process about 2 frames per second on a Nokia N90 mobile phone with an ARM9 processor with 220 MHz. Average authentication rates of 82 and 96% for images of size 40×40 and 80×80, respectively, were reported in [24]. In [22], a number of different face recognition methods were evaluated on a dataset of 750 videos from 50 users collected over three sessions with different illumination conditions.

12.3.1 Attribute-Based AA

Visual attributes are essentially labels that can be given to an image to describe its appearance [47]. A facial attribute-based continuous authentication method was recently proposed in [23, 38]. Figure 12.5 gives an overview of this method. Given a face image sensed by the front-facing camera, pre-trained attribute classifiers are used to extract a 44-dimensional attribute feature. The binary attribute classifiers

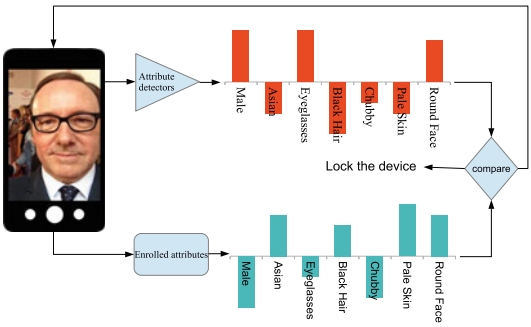

Fig. 12.5 Overview of the attribute-based authentication method proposed in [23]

are trained using the PubFig dataset [47] and provide compact visual descriptions of faces. The score is determined by comparing extracted attribute features with the features corresponding to the enrolled user. These score values are essentially used to continuously authenticate a mobile device user. Furthermore, it was shown that the attribute-based method can be fused LBP features [24] to obtain an improved performance.

This method was later extended in [39] where DCNNs were used to predict attributes for AA. In particular, a multi-task, part-based DCNN architecture was proposed for attribute detection. It was shown in [39] that this method can outperform the previously presented attribute-based methods as well as baseline LBP method for face-based mobile AA. Furthermore, effectiveness of this architecture was also demonstrated in terms of speed and power consumption by deploying it on an actual mobile device.

12.3.2 Extreme Value Analysis for Mobile AA

In principle, the primary goal of an authentication system is to ensure information security through intruder prevention. In order to prevent intrusions, an authentication mechanism should operate with a very low degree of false alarms. In [35], a special emphasis was given to the AA systems at the low false alarm region (from 0.001 to 0.1) and a new performance enhancement mechanism in this region for unimodal mobile AA systems was presented based on the statistical Extreme Value Theory (EVT).

Figure 12.6 gives an overview of this EVT-based AA system. A typical AA system extracts features of a probe and compares them against the enrolled features. In this system, distribution of the probability scores is also obtained in the enrollment phase. Tail of the probability score distribution is modeled using the EVT and is used together with the similarity score generated in the standard AA system to enhance the performance of the standard system. It is interesting to note that this EVT-based mechanism is independent of sensors and features used in the

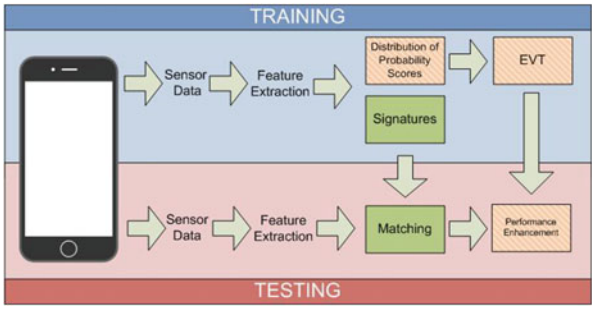

Fig. 12.6 Overview of the EVT-based AA system. Non-shaded blocks represent typical components of an AA system. Shaded components are the additions for performance enhancement [35]

underline AA system. Therefore, any existing AA system can be extended by incorporating this performance enhancement scheme. Experiments were conducted on three publicly available AA datasets, and it was shown that the new method can improve performance of the existing face and touch gesture-based AA systems.

12.3.3 One-Class Classification

Due to unavailability of training samples from negative classes, AA can be viewed as an one-class classification problem. To this end, a Single-class Minimax Probability Machine (1-MPM)-based solution called Dual Minimax Probability Machines (DMPM) for AA applications was recently introduced in [48]. In contrast to 1-MPM, this method has two notable differences.

(1) An additional hyper-plane is learned to separate training data from the origin by taking into account maximum data covariance.
(2) The possibility of modeling the underline distribution of training data is considered as a collection of sub-distributions.

Intersection of negative half-spaces defined by the two learned hyper-planes is considered to be the negative space during inference. The effectiveness of this mechanism was demonstrated by performing evaluations on three publicly available face-based AA datasets. In particular, it was shown that the decision boundary found by this method was indeed better than the decision boundary produced by 1-MPM. In all datasets, DMPM method demonstrated an improvement of 4–6% compared to 1-MPM.

In another work [49], a new DCNN-based one-class classification algorithm was recently introduced and was evaluated on AA application. Figure 12.7 gives an overview of the proposed CNN-based approach for one-class classification. The overall network consists of a feature extractor network and a classifier network. The feature extractor network essentially embeds the input target class images into a feature space. The extracted features are then appended with the pseudo-negative class data and generated from a zero-centered Gaussian in the feature space. The appended

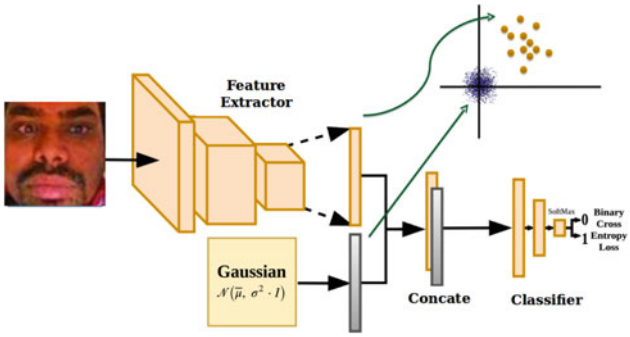

Fig. 12.7 Block diagram of the DCNN-based one-class classification approach proposed in [49]. Here, $\bar{\mu}$ and σ are mean and standard deviation parameters of a Gaussian, respectively, and **I** is the identity matrix

features are then fed into a classification network which is characterized by a fully connected neural network. The classification network assigns a confidence score for each feature representation. The output of the classification network is either 1 or 0. Here, 1 corresponds to the data sample belonging to the target class and 0 corresponds to the data sample belonging to the negative class. The entire network is trained end-to-end using binary cross-entropy loss. Extensive experiments were conducted, and it was demonstrated that this new DCNN-based one-class classification method achieved significant improvements over the recent state-of-the-art methods including one-class SVM, 1-MPM and support vector data description (SVDD) [49].

12.3.4 Quickest Intrusion Detection in Mobile AA

It is well known that a balance needs to be made between security and usability of a biometrics-based AA system [5, 50, 51]. In order to strike this balance in an AA scheme, following fundamental challenges should be factored.

1. Accuracy: How accurately does a mobile AA system detect an attacker or an intruder? Due to limitations of representation and classification models on mobile devices, behavioral and physiological biometrics-based methods do not provide good accuracy in practice [12, 52]. The AA system will be of little use in terms of security if it produces a high degree of false positives. On the other hand, a higher false negative rate would severely degrade the usability of the technology. Many recent approaches in the literature have attempted to address this factor by proposing better features and classifiers [12].

2. Latency: How long does it take to detect an attacker? If an AA system takes too long (e.g., 1–3 min) to detect an intrusion, it would grant an intruder plenty of time to extract sensitive information prior to the lock down. Hence, unless intruder

Fig. 12.8 Problem of quick intrusion detection in face-based AA systems. (A–I) show the genuine user with varying facial expressions. An intrusion occurs starting from (J). Active authentication systems should be able to detect intrusions as quickly as possible without causing too many false detections [41]

detection is sufficiently fast, the AA system would hold a little value in practice no matter how high its detection accuracy is.

Consider a series of observations captured from a front-facing camera of an Android device shown in Fig. 12.8. Frames (A–I) belong to the genuine user of the device. From frame J onward, an attacker starts to operate the device. In this scenario, frame J signifies a change point (i.e., an intrusion). The AA system should be able to detect intrusions with a minimal delay while maintaining a low rate of false detections. For instance, note the changes in genuine user's images in frames (D-F) due to camera orientation and facial expressions. While having a fast response, an AA system ideally should not falsely interpret these variations as intrusions.

3. Efficiency: How much resource does the system use? By definition, mobile AA systems are continuous processes that run as background applications. If they consume considerable amount of resources, memory, and processing power, it could slow down other applications and cause the battery to drain quickly. Despite the improvements in mobile memory and processors, battery capacity remains to be a constraint due to limitations in heat transfer and space [53]. Therefore, it can be expected to be the bottleneck in terms of efficiency in years to come. If an AA application causes battery to drain too quickly, then it is unrealistic to expect the users to use AA technology as they would typically opt out from using such applications [54]. Therefore, efficiency has a huge impact over the usability of AA as a technology. Recently, [38] studied the efficiency of a mobile AA system based on face biometric. Experiments were conducted on a Google Nexus 5 device with 2 GB of RAM and a quad-core 2.2 GHz CPU. It was shown that the normal usage of the device consumes about 520 mW of power and the facial attribute-based AA framework running at 4 frames per second consumes about 160.8 mW additional power. It is needless to say that nearly 30% increase in power consumption would take a toll on battery life. A trivial solution for this problem would be to decrease the sampling rate of data acquisition. However, the effects of such a measure on the detection performance have not been studied in the literature.

Many existing AA systems attempt to improve the accuracy of the system by proposing sophisticated features and classifiers. However, how fast an AA system could detect an intruder has not been widely studied in the literature. Yet, it remains to be an important feature of an AA system. In a recent paper [37, 41], authors addressed the problem of quickly detecting intrusions with lower false detection rates

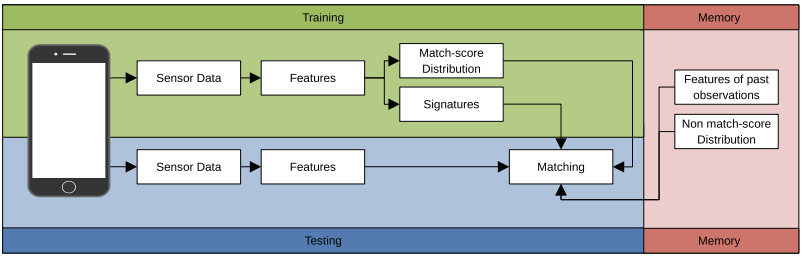

Fig. 12.9 An overview of the QCD-based AA method proposed in [41]

in mobile AA systems. They proposed Quickest Change Detection (QCD), which is a well-studied problem in statistical signal processing and information theory, for the purpose of intrusion detection in mobile AA systems. Figure 12.9 gives an overview of the proposed method. As opposed to a conventional AA system, this system utilizes all past observations along with distributions of match and non-match data of the genuine user to arrive at a decision. This proposed method does not require a specific feature nor a specific classifier; therefor, it can be built upon any existing AA system to enhance its performance. In particular, the introduced algorithms not only reduced the number of observations taken, but also improved the performance of the system in terms of latency and false detections. The validity of this result was demonstrated using various AA datasets.

12.3.5 Multi-user AA

Multiple-user active authentication [36, 40], in contrast with single-user active authentication, requires verification of identity of multiple subjects. Both traditional verification- and identification-based solutions fail to address the specific challenges presented in this problem. In a recent work [40], introduced Extremal Openset Rejection (EOR), a twofold mechanism with a sparse representation-based identification step and a verification step for this purpose. In the verification step, concentration of the sparsity vector and the overlap between matched and non-matched distributions are considered for decision making. Furthermore, a semi-parametric model based on EVT for modeling the distributions and an algorithm to estimate the parameters of extreme value distributions were also introduced in [40].

The EOR method essentially utilizes matched and non-matched distribution information on top of the identification criterion to make a better decision. It was shown that this additional processing has a significant gain particularly when identification criterion is poor (i.e., when a low number of users are enrolled). If a large number of classes are present, the additional verification step does not introduce a significant improvement. It was shown that EOR performs on par with the identification

method in such scenarios. As a result, the EOR framework is particularly suited for multiple-user authentication problems.

Effectiveness of this method was demonstrated using three publicly available face-based mobile active authentication datasets. It was observed that verification-based algorithms generally performed well when low number of users were enrolled. On the one hand, identification-based algorithms required larger number of users to obtain good performance. However, good performance of both of these cases was confined to extremes with respect to number of users. On the other hand, the new EOR method yielded superior performance consistently as the number of users was varied. Hence, it was shown that EOR is suited for multiple AA in mobile devices where the number of users may vary.

12.4 AA Datasets

Data collection is one of the biggest challenges in mobile AA research. Several small-scale datasets are publicly available to the research community [12]. In particular, UMDAA-01 [22], MOBIO [21], and UMDAA-02 [55] are the three most commonly used face-based AA datasets. Sample images from these datasets are shown in Fig. 12.10. In what follows, we give a brief overview of these datasets.

The UMDAA-01 dataset [22] contains images captured using the front-facing camera of a iPhone 5S mobile device of 50 different individuals captured across three sessions with varying illumination conditions. Images of this dataset contain pose variations, occlusions, partial clippings as well as natural facial expressions as evident from the sample images shown in Fig. 12.10a.

The MOBIO dataset [21] contains videos of 152 subjects taken across two phases where each phase consists of six sessions. Videos in this dataset are acquired using a standard 2008 MacBook laptop computer and a NOKIA N93i mobile phone. Sample images from this dataset are shown in Fig. 12.10b.

The UMDAA-02 Dataset [55] is an unconstrained multimodal dataset where 18 sensor observations were recorded across a two-month period using a Nexus 5 mobile

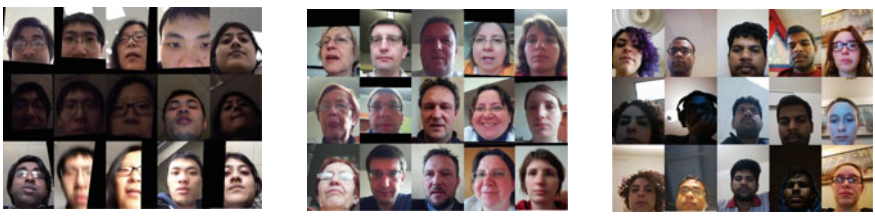

Fig. 12.10 Sample images from three face-based AA datasets. **a** UMDAA-01 [22], **b** MOBIO [21], **c** UMDAA-02 [55]. Each column represents sample images obtained for the same user

device. Unlike the earlier datasets, there exists a huge intra-class variation in this dataset in terms of poses, partial faces, illumination as well as appearances of the users as evident from the sample images shown in Fig. 12.10c.

12.5 Discussion

In this chapter, we provided a brief overview of recent advances in mobile-based active authentication methods. In particular, a special emphasis was given to the face-based methods. Continuous authentication on mobile devices promises to be an active area of research especially as more and more sensors are being added to the smartphone device and computation power of mobile devices has increased tremendously. There are, however, several challenges to be overcome before successfully designing a biometric-based continuous authentication system. Below, we list a few.

- A number of continuous authentication methods have been proposed in the literature that evaluate the performance of their proposed method on a variety of different datasets using different performance measures. However, there is no clear standard for evaluating the performance of different methods in the literature. Guidelines on an acceptable benchmark are needed.
- As discussed earlier, one of the major challenges in mobile-based AA is the datasets. Most mobile-based AA techniques discussed earlier have been evaluated on small- and mid-sized datasets consisting of hundreds of samples. However, in order to really see the significance and impact of various continuous authentication schemes in terms of usability and security, they need to be evaluated on large-scale datasets containing thousands and millions of samples.
- More usability and acceptability studies need to be conducted to really see the significance of AA in practice.

Acknowledgements This work was supported by US Office of Naval Research (ONR) Grant YIP N00014-16-1-3134.

References

1. Clarke N, Furnell S (2005) Authentication of users on mobile telephones: a survey of attitudes and practices. Comput Secur 24(7):519–527
2. Vance A (2010) If your password is 123456, just make it hackme (online; posted 20 Jan 2010). Available http://www.nytimes.com (online)
3. Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM (2010) Smudge attacks on smartphone touch screens. In: Proceedings of the 4th USENIX conference on offensive technologies, pp 1–7
4. Tapellini D (2014) Smart phone thefts rose to 3.1 million in 2013: industry solution falls short, while legislative efforts to curb theft continue (online; posted 28 May 2014). Available http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm (online)

5. Khan H, Hengartner U, Vogel D (2015) Usability and security perceptions of implicit authentication: convenient, secure, sometimes annoying. In: Eleventh symposium on usable privacy and security (SOUPS 2015), pp 225–239
6. Egelman S, Jain S, Portnoff RS, Liao K, Consolvo S, Wagner D (2014) Are you ready to lock? In: Proceedings of the 2014 ACM SIGSAC conference on computer and communications security, pp 750–761
7. Harbach M, von Zezschwitz E, Fichtner A, Luca AD, Smith M (2014) It's a hard lock life: a field study of smartphone (un)locking behavior and risk perception. In: Symposium on usable privacy and security (SOUPS 2014), pp 213–230
8. Guidorizzi RP (2013) Security: active authentication. IT Prof 15(4):4–7
9. Jakobsson M, Shi E, Golle P, Chow R (2009) Implicit authentication for mobile devices. In: Proceedings of USENIX
10. Shi E, Niu Y, Jakobsson M, Chow R (2011) Implicit authentication through learning user behavior. In: Proceedings of the 13th international conference on information security, pp 99–113
11. Clarke NL (2011) Transparent user authentication—biometrics. Springer, RFID and Behavioural Profiling
12. Patel VM, Chellappa R, Chandra D, Barbello B (2016) Continuous user authentication on mobile devices: recent progress and remaining challenges. IEEE Sig Process Mag 33(4):49–61
13. Frank M, Biedert R, Ma E, Martinovic I, Song D (2013) Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans Inf Forensics Secur 8(1):136–148
14. Serwadda A, Phoha V, Wang Z (2013) Which verifiers work?: a benchmark evaluation of touch-based authentication algorithms. In: IEEE international conference on biometrics: theory. Sept, applications and systems, pp 1–8
15. Feng T, Liu Z, Kwon KA, Shi W, Carbunar B, Jiang Y, Nguyen N (2012) Continuous mobile authentication using touchscreen gestures. In: IEEE conference on technologies for homeland security, pp 451–456
16. Sherman M, Clark G, Yang Y, Sugrim S, Modig A, Lindqvist J, Oulasvirta A, Roos T (2014) User-generated free-form gestures for authentication: security and memorability. In: Proceedings of the 12th annual international conference on mobile systems, applications, and services, pp 176–189
17. Zhao X, Feng T, Shi W, Kakadiaris I (2014) Mobile user authentication using statistical touch dynamics images. IEEE Trans Inf Forensics Secur 9(11):1780–1789
18. Zhang H, Patel VM, Fathy ME, Chellappa R (2015) Touch gesture-based active user authentication using dictionaries. In: IEEE winter conference on applications of computer vision
19. Bo C, Zhang L, Li XY, Huang Q, Wang Y (2013) Silentsense: silent user identification via touch and movement behavioral biometrics. In: Proceedings of the 19th annual international conference on mobile computing & networking, ser. MobiCom '13. ACM, New York, NY, USA, pp 187–190
20. Fridman L, Weber S, Greenstadt R, Kam M (2015) Active authentication on mobile devices via stylometry, GPS location, web browsing behavior, and application usage patterns. IEEE Syst J
21. McCool C, Marcel S, Hadid A, Pietikainen M, Matejka P, Cernocky J, Poh N, Kittler J, Larcher A, Levy C, Matrouf D, Bonastre JF, Tresadern P, Cootes T (2012) Bi-modal person recognition on a mobile phone: using mobile phone data. In: IEEE international conference on multimedia and expo workshops, pp 635–640
22. Fathy ME, Patel VM, Chellappa R (2015) Face-based active authentication on mobile devices. In: IEEE international conference on acoustics, speech and signal processing
23. Samangouei P, Patel VM, Chellappa R (2015) Attribute-based continuous user authentication on mobile devices. In: IEEE international conference on biometrics: theory, applications and systems
24. Hadid A, Heikkila J, Silven O, Pietikainen M (2007) Face and eye detection for person authentication in mobile phones. In: ACM/IEEE international conference on distributed smart cameras, pp 101–108

25. Derawi M, Nickel C, Bours P, Busch C (2010) Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: International conference on intelligent information hiding and multimedia signal processing, pp 306–311
26. Primo A, Phoha V, Kumar R, Serwadda A (2014) Context-aware active authentication using smartphone accelerometer measurements. In: IEEE conference on computer vision and pattern recognition workshops, pp 98–105
27. Crouse D, Han H, Chandra D, Barbello B, Jain AK (2015) Continuous authentication of mobile user: fusion of face image and inertial measurement unit data. In: International conference on biometrics
28. Zhang H, Patel VM, Chellappa R (2015) Robust multimodal recognition via multitask multivariate low-rank representations. In: IEEE international conference on automatic face and gesture recognition, vol 1, pp 1–8
29. Zhang H, Patel VM, Shekhar S, Chellappa R (2015) Domain adaptive sparse representation-based classification. In IEEE international conference on automatic face and gesture recognition, vol 1, pp 1–8
30. Abramson M, Aha DW (2013) User authentication from web browsing behavior. In: Florida artificial intelligence research society conference. AAAI Press
31. Li F, Clarke N, Papadaki M, Dowland P (2014) Active authentication for mobile devices utilising behaviour profiling. Int J Inf Secur 13(3):229–244
32. Saevanee H, Clarke N, Furnell S, Biscione V (2014) Text-based active authentication for mobile devices. In: Cuppens-Boulahia N, Cuppens F, Jajodia S, Abou El Kalam A, Sans T (eds) ICT systems security and privacy protection, ser. IFIP advances in information and communication technology. Springer, Berlin, Heidelberg, vol 428, pp 99–112
33. Gascon H, Uellenbeck S, Wolf C, Rieck K (2014) Continuous authentication on mobile devices by analysis of typing motion behavior. Sicherheit 2014:1–12
34. Holz C, Buthpitiya S, Knaust M (2015) Bodyprint: biometric user identification on mobile devices using the capacitive touchscreen to scan body parts. In: Proceedings of the 33rd annual ACM conference on human factors in computing systems. ACM, New York, NY, USA, pp 3011–3014
35. Perera P, Patel VM (2017) Extreme value analysis for mobile active user authentication. In: IEEE international conference on automatic face and gesture recognition
36. Perera P, Patel VM (2017) Towards multiple user active authentication in mobile devices. In: IEEE international conference on automatic face and gesture recognition
37. Perera P, Patel VM (2016) Quickest intrusion detection in mobile active user authentication. In: International conference on biometrics theory, applications and systems
38. Samangouei P, Patel VM, Chellappa R (2016) Facial attributes for active authentication on mobile devices. Image Vis Comput 58:181–192
39. Samangouei P, Chellappa R (2016) Convolutional neural networks for attribute-based active authentication on mobile devices. In: IEEE international conference on biometrics: theory, applications, and systems
40. Perera P, Patel VM (2018) Facebased multiple user active authentication on mobile devices. IEEE Trans Inf Forensics Secur 14:1240–1250
41. Perera P, Patel VM (2018) Efficient and low latency detection of intruders in mobile active authentication. IEEE Trans Inf Forensics Secur 13(6):1392–1405
42. Sarkar S, Patel VM, Chellappa R (2016) Deep feature-based face detection on mobile devices. In: IEEE international conference on identity, security and behavior analysis
43. Krizhevsky A, Sutskever I, Hinton GE (2012) Imagenet classification with deep convolutional neural networks. In: Advances in neural information processing systems, p 2012
44. Mahbub U, Patel VM, Chandra D, Barbello B, Chellappa R (2016) Partial face detection for continuous authentication. In: IEEE international conference on image processing
45. Abeni P, Baltatu M, D'Alessandro R (2006) Nis03-4: implementing biometrics-based authentication for mobile devices. In: IEEE global telecommunications conference, pp 1–5
46. Viola PA, Jones MJ (2004) Robust real-time face detection. Int J Comput Vis 57(2):137–154

47. Kumar N, Berg A, Belhumeur P, Nayar S (2011) Describable visual attributes for face verification and image search. IEEE Trans Pattern Anal Mach Intell 33(10):1962–1977
48. Perera P, Patel VM (2018) Dual-minimax probability machines for one-class mobile active authentication. In: IEEE international conference on biometrics: theory, applications, and systems
49. Oza PB, Patel VM (2018) One-class convolutional neural network. IEEE Sig Process Lett 26:277–281
50. Clarke N, Karatzouni S, Furnell S (2009) Flexible and Transparent User Authentication for Mobile Devices. In: Emerging challenges for security, privacy and trust: 24th IFIP TC 11 international information security conference, SEC 2009, Pafos, Cyprus, 18–20 May 2009. Proceedings. Springer, Berlin, Heidelberg, pp 1–12
51. Crawford H, Renaud K (2014) Understanding user perceptions of transparent authentication on a mobile device. J Trust Manag 1(7):1–28
52. Meng W, Wong DS, Furnell S, Zhou J (2015) Surveying the development of biometric user authentication on mobile phones. IEEE Commun Surv Tutorials 17(3):1268–1293
53. Li JGWD, Hao S, Halfond GJ (2014) An empirical study of the energy consumption of android applications. In: IEEE international conference on software maintenance and evolution (ICSME)
54. Lee W (2013) Mobile apps and power consumption—basics, part 1. Available https://developer.qualcomm.com/blog/mobile-apps-and-power-consumption-basics-part-1 (online)
55. Mahbub U, Sakar S, Patel V, Chellappa R (2016) Active authentication for smartphones: a challenge data set and benchmark results. In: IEEE international conference on biometrics: theory applications and systems