Vishal M. Patel, Rama Chellappa,
Deepak Chandra, and Brandon Barbello

Continuous User Authentication on Mobile Devices

Recent Progress and Remaining Challenges

Recent developments in sensing and communication technologies have led to an explosion in the use of mobile devices such as smartphones and tablets. With the increase in the use of mobile devices, users must constantly worry about security and privacy, as the loss of a mobile device could compromise personal information. To deal with this problem, continuous authentication systems (also known as *active authentication systems*) have been proposed, in which users are continuously monitored after initial access to the mobile device. In this article, we provide an overview of different continuous authentication methods on mobile devices. We discuss the merits and drawbacks of the available approaches and identify promising avenues of research in this rapidly evolving field.

IMAGE LICENSED BY INGRAM PUBLISHING

Introduction

Traditional methods for authenticating users on mobile devices are based on explicit authentication mechanisms such as a password, a personal identification number (PIN), or a secret pattern. Studies have shown that users often choose a simple, easily guessed 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 the most commonly used passwords. Also, when secret patterns are used for gaining initial access on the mobile devices, users tend to use the same pattern over and over again. As a result, they leave oily residues or smudges on the screen of the mobile device. It has been shown that with special lighting and high-resolution photography, one can easily deduce the secret pattern (see Figure 1) [3].

Digital Object Identifier 10.1109/MSP.2016.2555335
Date of publication: 1 July 2016

1053-5888/16©2016IEEE

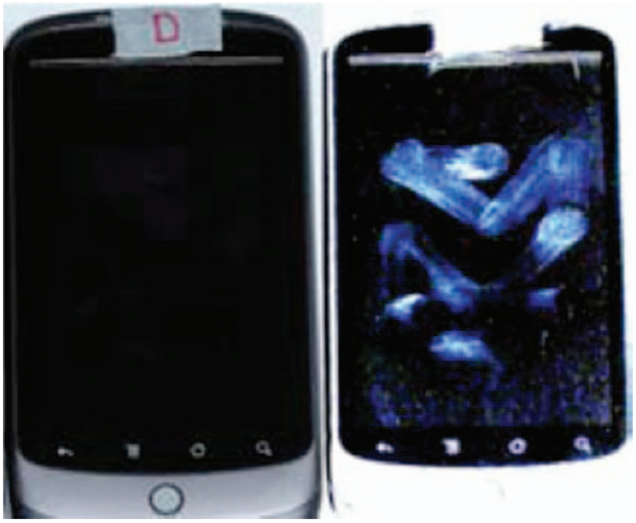

FIGURE 1. A smudge attack [3]. A user's secret pattern can be determined with special lighting and high-resolution camera.

Furthermore, recent studies have shown that about 34% of users did not use any form of authentication mechanism on their devices [4]–[7]. In these studies, inconvenience was cited as one of the main reasons that users did not employ any authentication mechanism on their devices [6], [7]. The authors of [7] demonstrated that mobile-device users considered unlock screens unnecessary in 24% of situations and that they spent up to 9% of their smartphone use time unlocking the screen. Furthermore, as long as the mobile phone remains active, typical devices incorporate no mechanisms to verify that the user originally authenticated is still the user in control of the device. Thus, unauthorized individuals may improperly obtain access to a user's personal information if a password is compromised or if the user does not exercise adequate vigilance after initial authentication.

To overcome these issues, both the biometrics and security research communities have developed techniques for continuous authentication on mobile devices. These methods essentially make use of physiological and behavioral biometrics, using built-in sensors and accessories such as the gyroscope, touch screen, accelerometer, orientation sensor, and pressure sensor, to continuously monitor user identity. For instance, physiological biometrics such as those of the face can be captured using the front-facing camera of a mobile device and used to continuously authenticate a mobile-device user. On the other hand, sensors such as the gyroscope, touch screen, and accelerometer can be used to measure behavioral biometric traits such as gait, touch gestures, and hand movement. Figure 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, and are useful in monitoring three-dimensional (3-D) device movement or positioning or to monitor changes in the ambient environment near a mobile 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.

Our goal in this article is to survey recent developments in continuous authentication, discuss their advantages and limitations, and identify areas still open for exploration. Development of feasible and robust continuous authentication systems for

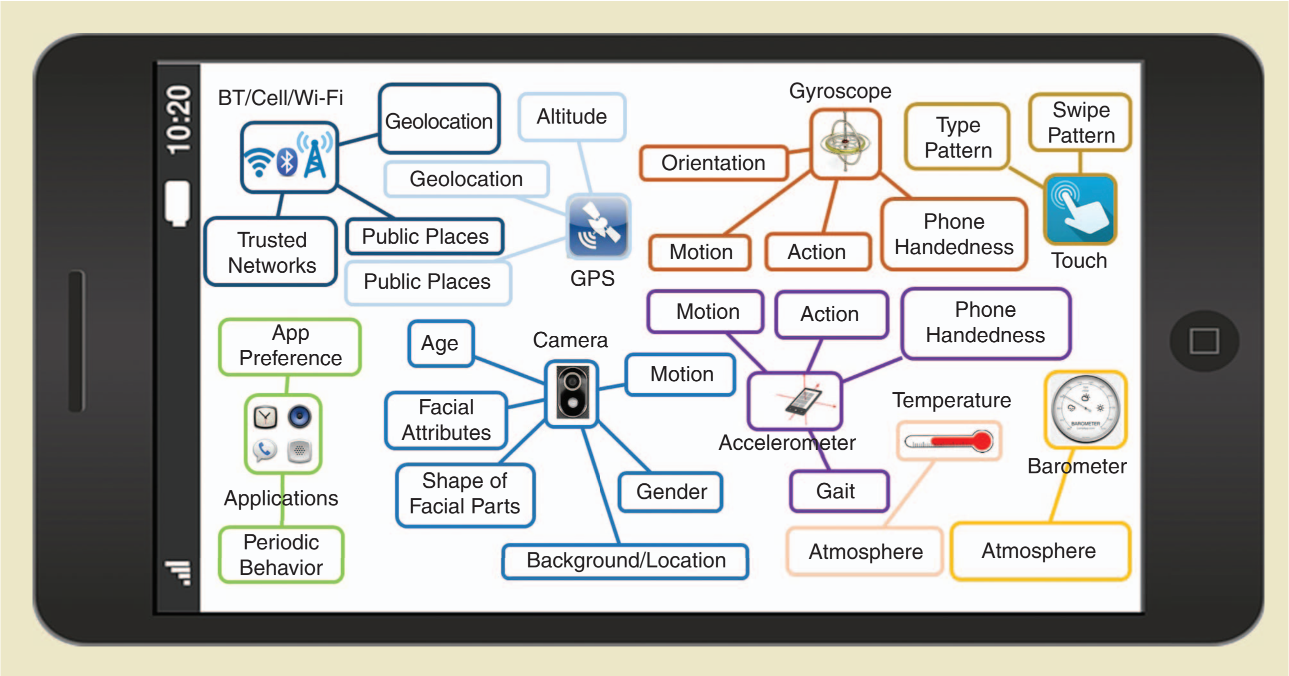

FIGURE 2. Sensors and accessories available in a mobile device. Raw information collected by these sensors can be used to continuously authenticate a mobile-device user. GPS: global positioning system.

mobile devices is important, as we are becoming increasingly dependent on mobile devices.

Continuous authentication approaches

Figure 3 shows the basic concept 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 in a mobile device. Then, the biometric system will determine whether these biometric traits correspond to a legitimate user or not. If the features do correspond to a legitimate user, the biometric system will continue processing the new incoming data. However, if the biometric system produces a negative response, the system will ask the user to verify his or her identity by using the traditional explicit authentication methods based on PIN, face, or secret pattern. If the user is able to provide identity verification, the mobile device will continue in service; otherwise, it will be locked.

In a practical continuous authentication system, the entire process happens in real time. A plethora of mobile continuous authentication methods have been proposed in the literature. In what follows, we review a few recent methods based on physiological as well as behavioral biometrics for continuous authentication.

Touch dynamics

Touch dynamics is one of the most commonly used continuous authentication methods for mobile devices. In touch dynamics, touch screen input is used as a data source. In particular, screen touch gestures—the way users swipe their fingers on the touch screen of their mobile devices—are used as a behavioral biometric to continuously authenticate users while they perform basic smartphone operations. In these methods, a behavioral feature vector is extracted from the recorded screen touch data, and a discriminative classifier is trained on these extracted features for authentication. Figure 4 shows some swipes performed by eight different users while reading text on an Android device [13]. It is interesting to see that even for the same task, touch data of different users show significant differences. In addition to the x and y coordinates of each swipe, information such as finger pressure, the screen area covered by each finger, and time information can be used to extract useful features.

A swipe or a stroke on the touch screen is a sequence of touch data when the finger is in touch with the screen of the mobile device. Every swipe $\mathbf{s}$ can be encoded as a sequence of vectors

$$\mathbf{s}_i = (x_i, y_i, t_i, p_i, A_i, O_i^f, O_i^{ph}), \quad i = \{1, 2, L, N\}, \qquad (1)$$

where xi, yi are the location points, and t_i, p_i, A_i, O_i^f, and O_i^{ph} are the time stamp, the pressure on screen, the area occluded by the finger, the orientation of the finger, and the orientation of the phone (landscape or portrait), respectively. Here, N is the total number of swipes. Based on these measurements, a 30-dimensional feature vector was proposed in [13] for each swipe: midstroke area covered; 20% pairwise velocity; midstroke pressure; direction of end-to-end line; stop x; start x; average direction; start y; average velocity; stop y; stroke duration; direct end-to-end distance; length of trajectory; 80% pairwise velocity; median velocity at last three points; 50% pairwise velocity; 20% pairwise acceleration; ratio of end-to-end distance and length of trajectory; largest deviation from end-to-end line; 80% pairwise acceleration; mean resultant length; median acceleration at first five points; 50% deviation from end-to-end line; interstroke time; 80% deviation from end-to-end line; 20% deviation from end-to-end line; 50% pairwise acceleration; phone orientation; midstroke finger orientation; and up/down/left/right flag. After feature analysis, three of these features were discarded and the remaining 27 were evaluated using a kernel support vector machine (SVM) and k-nearest-neighbors (kNNs) classifiers on a data set consisting of 41 users' touch gestures. It was shown that these classifiers can achieve equal error rates (EERs) between 0% and 4%, depending on the application scenario [13]. Similar features have been used in [14]–[16] for touch gesture-based continuous authentication. For classification, nonlinear sparse representation-based classifiers were used in [16], while ten different classification algorithms were evaluated in [15].

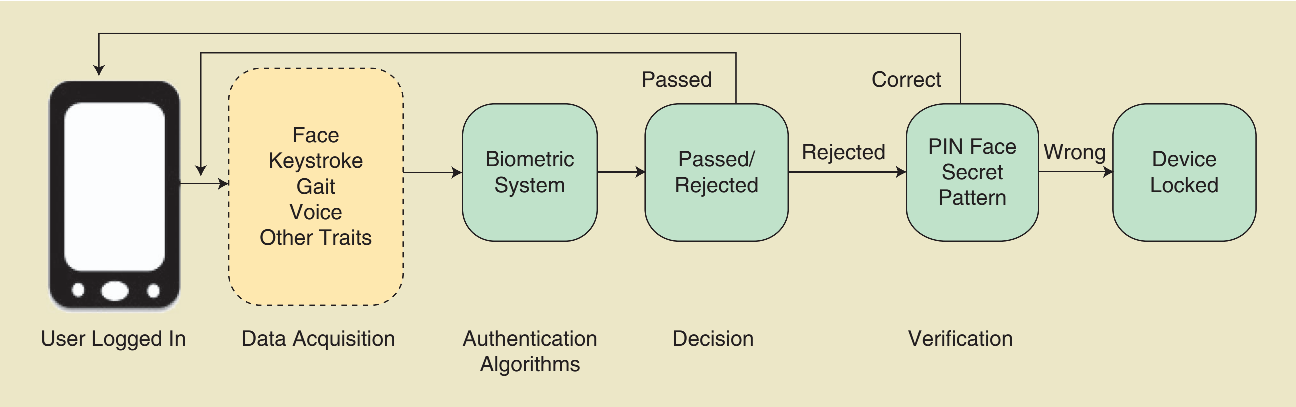

FIGURE 3. A biometrics-based mobile continuous authentication framework [12].

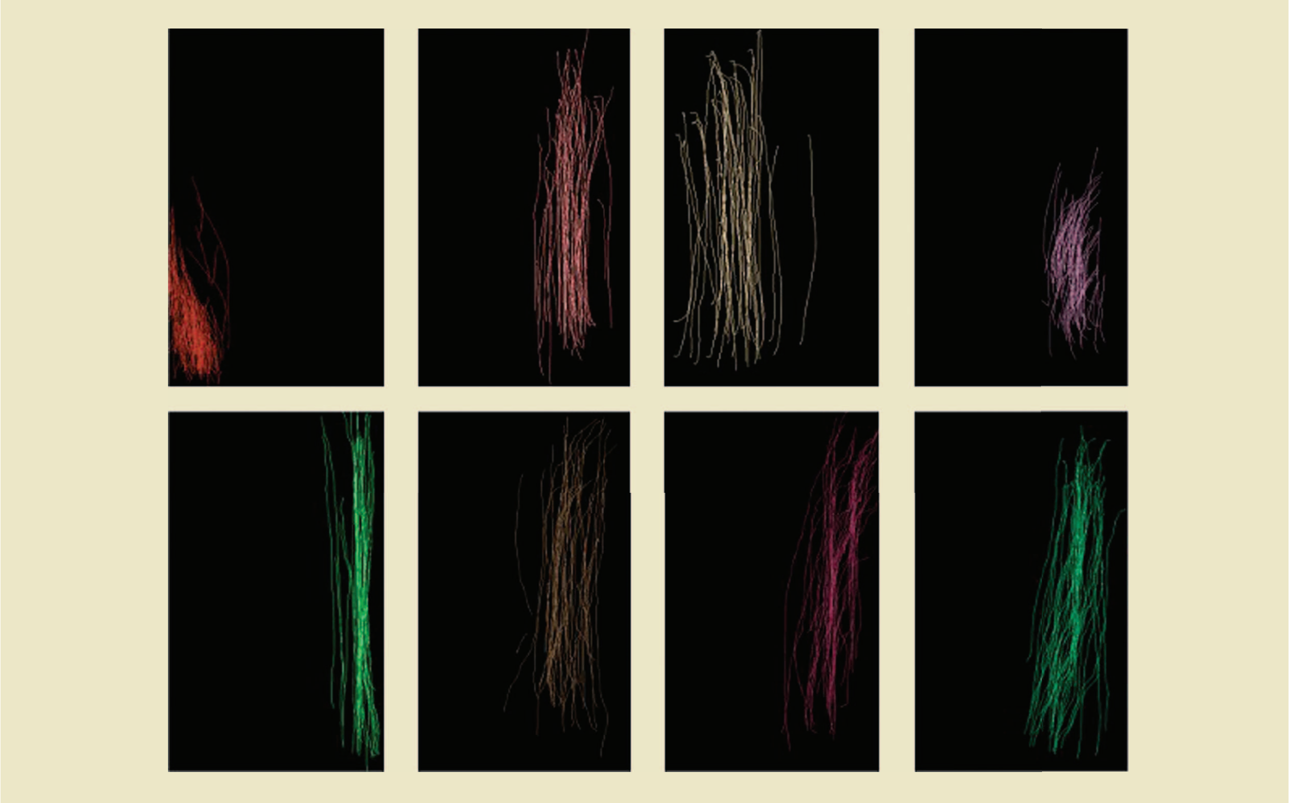

FIGURE 4. Swipes of eight different users while reading text [13]. Different colors are used to show different users' swipes.

The methods presented in [13]–[16] are essentially based on the fact that only a single finger is in contact with the touch screen while users are performing basic operations. In practice, many applications require users to employ two or more fingers to perform a particular task, such as zooming in and zooming out by pinching and spreading two fingers. More general multitouch, gesture-based continuous authentication systems have also been proposed in the literature [17], [18]. Similar to single-finger gestures, in [17] x and y coordinates, direction of finger motion, finger motion speed, pressure at each sampled touch point, and the distance between multitouch points are used to extract multitouch gesture features. On the other hand, in [18] a second-order autoregressive model is used for modeling multitouch sequences, and a mutual information-based metric is used for multitouch gesture recognition.

Different from the touch gesture features discussed above, an image-based feature called graphic touch gesture feature (GTGF) was proposed in [19] for modeling touch dynamics. In this approach, swipe geometry traits are converted to the image space so the dynamics of swipes can be explicitly modeled. Furthermore, the pressure dynamics are emphasized by fusing them with the movement dynamics. This method was later extended in [20] by building a touch gesture appearance model from the GTGF. The model learns the intraperson variations of the GTGF in the image domain by statistical analysis and is capable of synthesizing new instances according to a new probe swipe. Furthermore, these methods are applicable to both single-finger and multifinger swipes. Figure 5 shows the GTGF features extracted from two users.

Table 1 compares all the aforementioned touch dynamics-based continuous authentication methods. Here, the false accept rate (FAR) and the false reject rate (FRR) are presented for one of the studies. As can be seen from this table, some methods achieve very low EER values on certain data sets. These studies have demonstrated that touch gestures can be used as a promising behavioral biometric for continuous user authentication of mobile devices.

Face recognition

Another continuous authentication system that is widely used for continuously monitoring a user's identity on a mobile device is based on face recognition. A generic face recognition system consists of three main stages. In the first, faces are detected from the images or videos captured by smartphones' front-facing cameras. 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 briefly review some of these methods.

In [21], the feasibility of face and eye detection on cell phones was evaluated using the Adaboost cascade classifiers with Haar-like and local binary pattern (LBP) features [22], [23] as well as a skin color-based detector. On a Nokia N90 mobile phone that has an ARM9 220-MHz processor

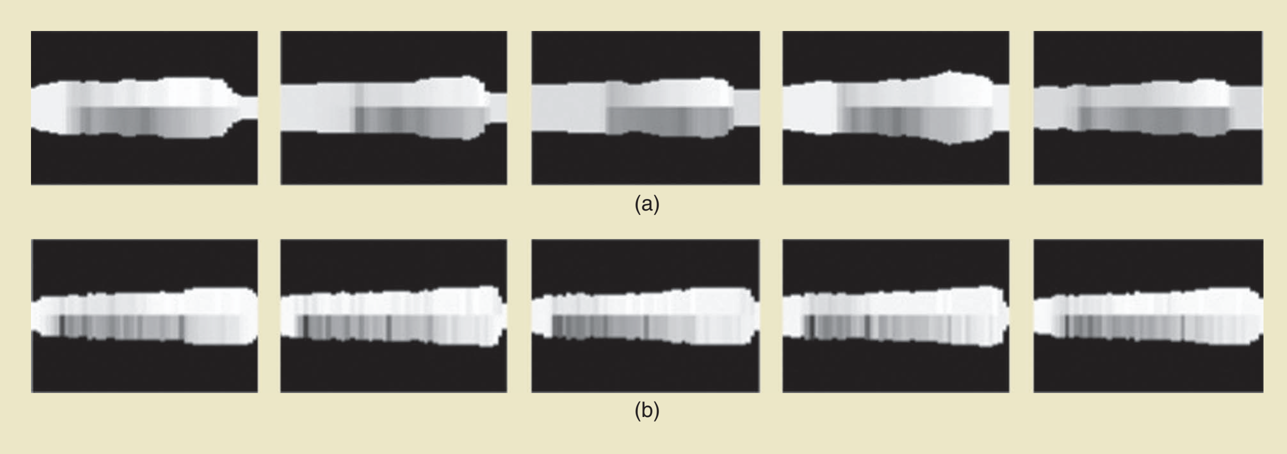

FIGURE 5. The GTGF features corresponding to two different users [19]: (a) shows the GTGF features corresponding to five touch gestures of a single user, while (b) shows the GTGF features extracted from five swipes of a different user.

and a built-in memory of 31 MB, the researchers reported that the Haar + Adaboost method can detect faces in 0.5 seconds from 320 × 240 images. This approach, however, is not effective when wide variations in pose and illumination are present or when the images contain partial or clipped images. To deal with these issues, a deep convolutional neural network (DCNN)-based method was recently developed in [24] for detecting faces on mobile platforms. In this method, deep features are first extracted using the first five layers of Alexnet [25]. Different-size 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 an overlap criterion. Finally, a single bounding box is output by the detector. It was shown that this detector is quite robust to illumination change and is able to detect partial or extremely posed faces. A few sample positive detections from the University of Maryland–Active Authentication (UMD-AA) data set [26] are shown in Figure 6. The DCNN-based detections are marked in red, while the ground truth is in yellow. Another part-based method for detecting partial and occluded faces on mobile devices was developed in [27]. 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.

In terms of face recognition on mobile devices, a method based on a one-class SVM was proposed in [28]. In this approach, faces are detected using the Viola–Jones detector [22]. Histogram equalization is then applied on the detected images to normalize the effect of illumination. Finally, bidimensional Fourier transform features are extracted from the normalized images and fed into a one-class SVM for authentication. In addition to developing face- and eye-detection methods on mobile devices, [21] also developed a method for face recognition based on LBP features. It was shown that their proposed continuous face authentication system, including face detection and recognition, can process about two 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 [21]. In [26], several face recognition methods were evaluated on a data set of 750 videos from 50 users collected over three sessions with different illumination conditions. A face-based continuous authentication method was recently developed in [12] that uses gyroscope, accelerometer, and magnetometer data to correct for camera orientation and the orientation of the face image. In [29], a sensor-assisted mobile face recognition system was proposed that utilizes motion and light sensors to defend against media and virtual camera attacks.

Visual attributes are essentially labels that can be given to an image to describe its appearance [30]. A facial attribute-based continuous authentication method was recently proposed in [31]. Figure 7 gives an overview of this method. Given

Table 1. Key touch dynamics-based continuous authentication methods. The best results from the corresponding papers are reported.

Study	Number of Users	Classifiers	Feature Dimension	Performance (%)
Frank et al. [13]	41	SVM, *k*NN	27	EER: 0.00–4.00
Zhang et al. [16]	50	Sparsity-based classifiers	27	EER: 0.77
Li et al. [14]	75	SVM	10	EER: ~ 3.0
Feng et al. [17]	40	Random forest, J48 tree, Bayes' net	53	FAR: ~ 7.50, FRR: ~8.00
Serwadda et al. [15]	138	Ten different classifiers	28	EER: 10.50
Zhao et al. [20]	78	L_1 distance	100 × 150 image	EER: 6.33–15.40

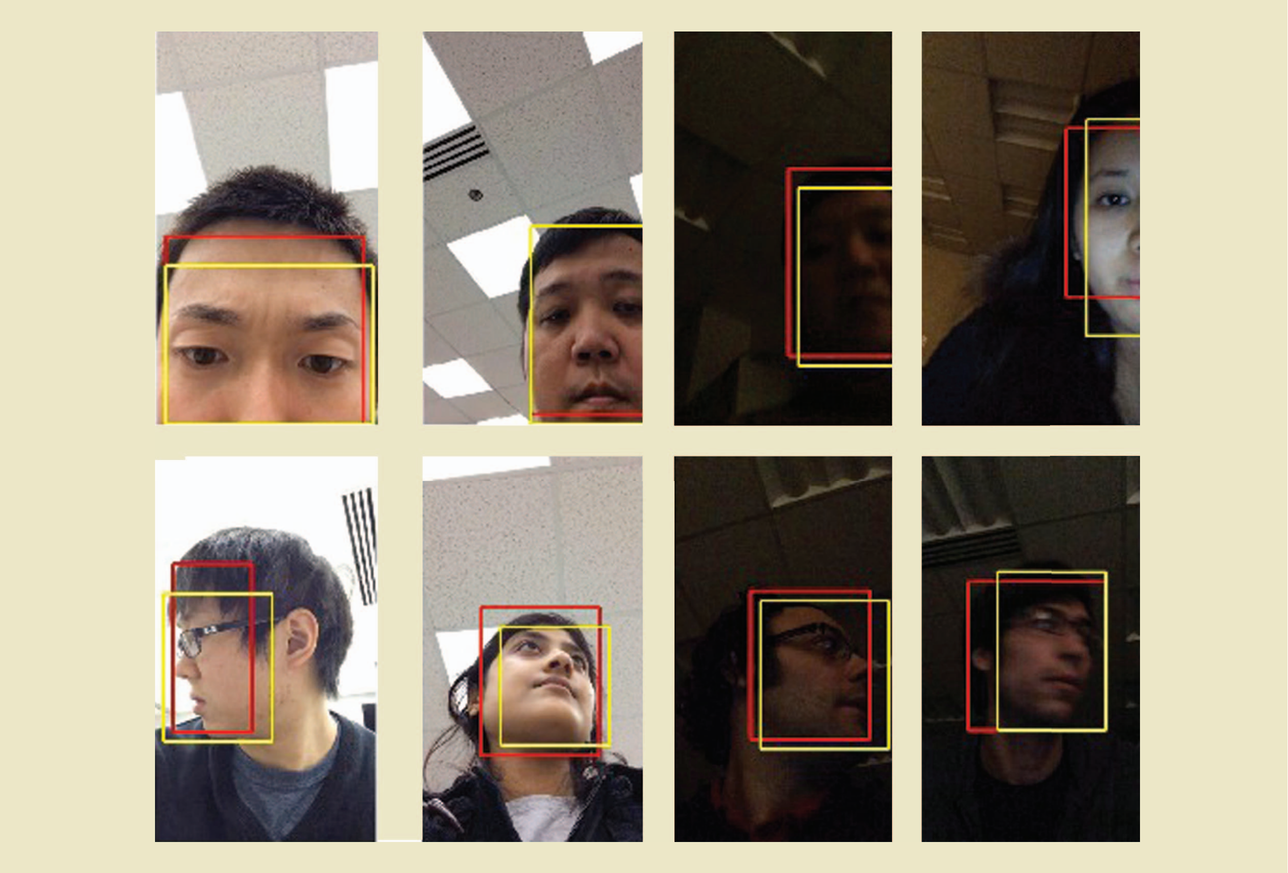

FIGURE 6. Examples of positive detections with pose variations and occlusion on the UMD-AA data set. The detector's output is in red, while ground truth is in yellow [24].

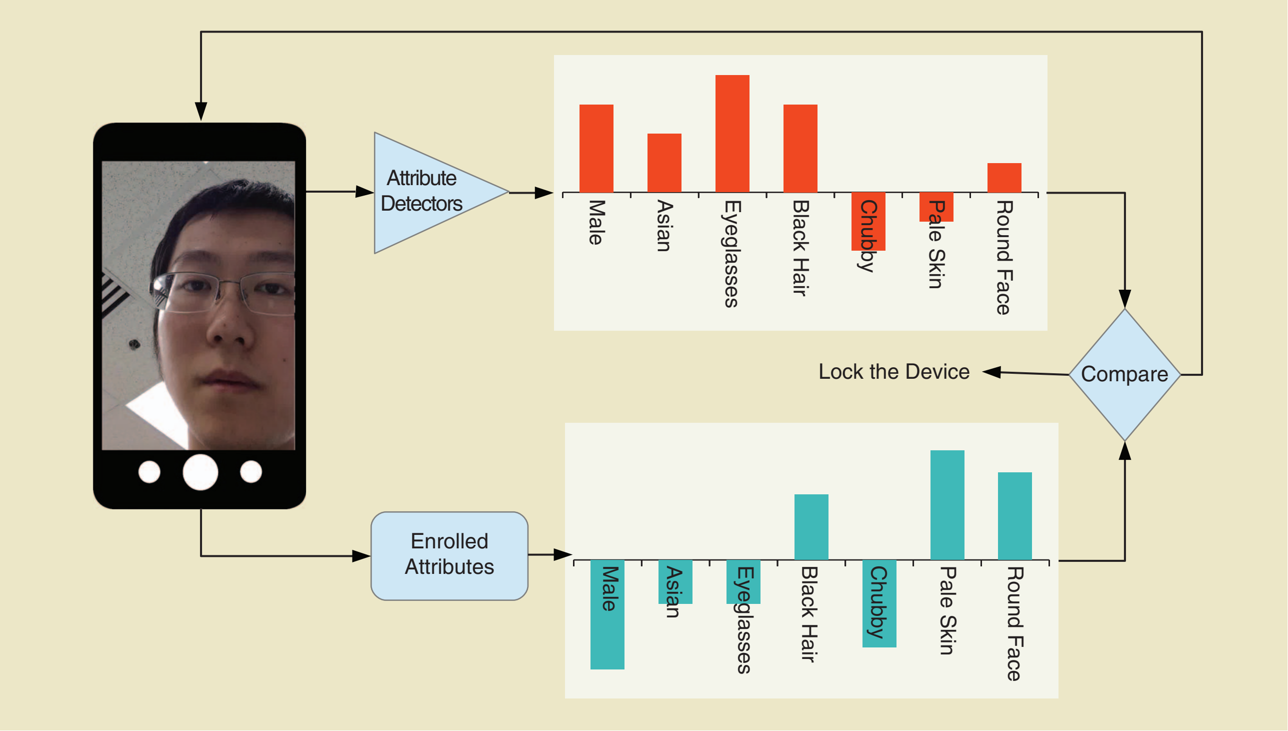

FIGURE 7. An overview of the attribute-based authentication method proposed in [31].

a face image sensed by the front-facing camera, pretrained attribute classifiers are used to extract a 44-dimensional attribute feature. The binary attribute classifiers are trained using the PubFig data set [30] and provide compact visual descriptions of faces. The score is determined by comparing the 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 with an LBP-based method such as in [21] to obtain improved matching performance.

Table 2 summarizes key face-based continuous authentication methods. Here, the recognition rate (RR), true accept rate (TAR), and average authentication rate (AAR) are noted for some of the studies.

Table 2. A summary of key face-based continuous authentication methods.

Study	Number of Users	Method/Features	Performance (%)
Abeni et al. [28]	32	1-class SVM/Fourier transform	EER: 3.95–7.92
Hadid et al. [21]	12	Histogram intersection distance/LBP	AAR: 82–96
Fathy et al. [26]	50	Nine different classifiers/MEEN	RR: ~95
Crouse et al. [12]	10	SVM/biologically inspired model	TAR: ~40–50 @FAR 0.1
Samangouei et al. [31]	50	Attributes	EER: 13–30

MEEN: mouth, left eye, right eye, nose.

Gait dynamics

Gait dynamics-based continuous authentication systems identify users based on how they walk. The data needed for gait-based authentication are often measured by the built-in accelerometer and gyroscope sensors. Once the raw data are measured, discriminative features are extracted, which are then fed into a classifier to distinguish users. In recent years, several methods have been developed for gait-based recognition on mobile devices [32]–[38]. These methods differ essentially in the types of features extracted from the raw data for classification or the types of classification methods used for authentication. For instance, methods based on correlation, frequency domain analysis, and data distribution statics are used in [32], while methods based on dynamic time warping are used in [36] and [37]. Rather than using the gait cycles for extracting features, [35] proposes an application of hidden Markov models (HMMs) for gait recognition. In particular, a sensor orientation invariant gait representation called *gait dynamic images* (*GDIs*) was proposed in [39]. Given a 3-D time series captured by a three-axis accelerometer, its GDI is calculated by the cosine similarity of the motion measurement at time *t* with the time-lagged signal of lag *l*. Figure 8 shows an example of raw three-axis accelerometer data and their corresponding GDI. As can be seen from this figure, since GDI is invariant in regard to sensor orientation, it shows much better consistency before and after sensor rotation. Also, pace-independent gait recognition approaches have been proposed in [34] and [38]. In [38], GDIs are used, while in [34] cyclostationarity and continuous wavelet transform spectrogram analysis are used for gait-based recognition. Table 3 summarizes key gait dynamics-based continuous authentication methods in terms of their performance on various data sets. In this table, the verification rate (VR), false nonmatch rate (FNMR), and false match rate (FMR) are noted in two of the studies.

Behavior-based profiling

Behavior profiling techniques verify the user's identity based on the applications and services they use. The research into mobile behavior profiling started in late 1990s, focusing mainly on developing intrusion detection systems (IDSs) to detect telephony service fraud by monitoring user calling and migration behavior [40]–[42]. In these systems, user profiles are created by monitoring user activities for a period of time and are compared against the current activity profiles of the user. If a significant deviation is observed, a possible intrusion is detected.

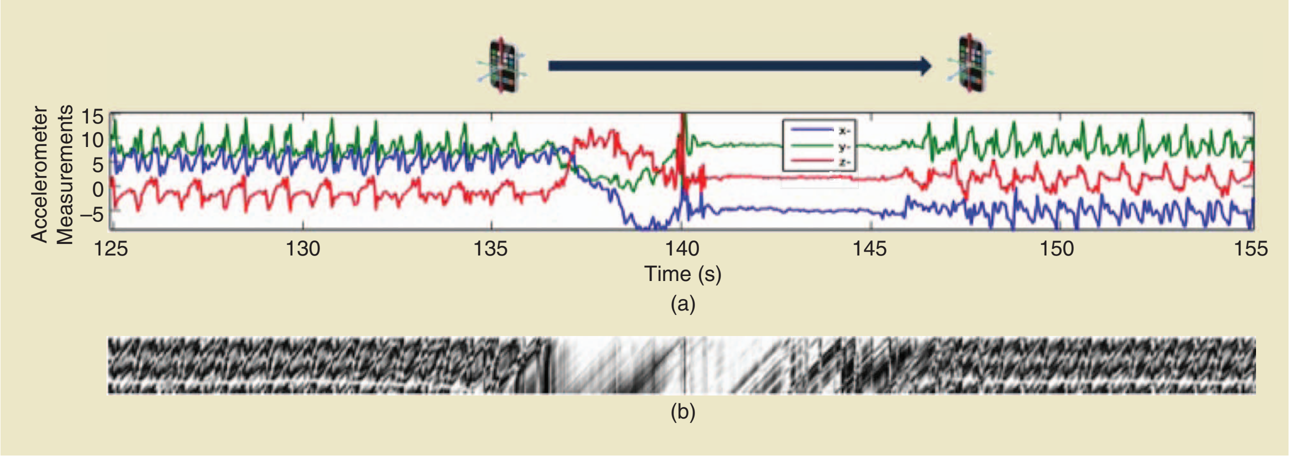

FIGURE 8. (a) Data measurements from a three-axis accelerometer embedded in a mobile phone carried by a walking user. (b) The corresponding GDI.

Table 3. Key gait-based continuous authentication methods for mobile devices.

Study	Number of Users	Feature	Classifier	Performance (%)
Mantyjarvi et al. [32]	36	Raw data	Correlation coefficients	EER: 7
Thang et al. [36]	11	FFT	SVM	Accuracy: 92.7
Muaaz et al. [37]	51	Raw data	SVM	EER: 22.49–33.30
Nickel et al. [35]	48	Raw data	HMM	FNMR: 10.42 @ FMR10.29
Zhong et al. [38]	51	GDI	Nearest neighbor	EER: 3.88–7.22
Juefei-Xu et al. [34]	36	Wavelets	SVM	61.1–99.4 VR @ 0.1 FAR

Recently, a number of different techniques have been developed in the literature that focus on the use of such methods for continuous authentication [43]–[45]. In these methods, application-level as well as application-specific features such as cell ID, date, time and number of caller, duration of call, application time, and name and time of application usage are used to continuously monitor the user identity. For instance, EERs of 5.4%, 2.2%, and 13.5% have been reported in [43] for telephony, text messaging, and general application usage, respectively, on the MIT Reality data set [46]. Historical application usage data have also been utilized to verify mobile users in a continuous manner. [44] developed a technique based on historical usage data using a combination of a rule-based classifier, a dynamic profiling technique, and a smoothing function. They reported an EER of 9.8%. Recently, a behavior profiling method that focuses on what, where, when, and how the mobile devices were used was developed in [45]. A privacy-preserving implicit authentication system based on behavior profiling has also been proposed in [47]. In [48], a data-driven approach was proposed for continuous authentication based on incremental training. The researchers argued that a few weeks of data may not be sufficient for training but that training must be set automatically on a per-use basis.

Furthermore, a behavior profiling method based on application usage, Bluetooth sightings, and Wi-Fi access point sightings was recently presented in [49]. Discriminative features from these modalities were extracted, and a categorical nearest-neighbor classifier was used to produce matching scores. The authors reported average identification rates of 80%, 77%, 93%, and 85% when using application, Bluetooth, Wi-Fi, and the combination of these three types of behavioral features, respectively. Table 4 summarizes the results for all the behavior-based profiling methods discussed above.

Other approaches

Keystroke dynamics is another behavioral biometric that is widely used to continuously authenticate mobile-device users. In keystroke dynamics, users are identified based on their typing patterns. In this method, two types of features, interkey time (the time between two successive key presses) and hold time (the time between pressing and releasing a single key), are commonly used. In particular, [50] proposed the use of keystroke dynamics based on the way users type graphical-based passwords to authenticate the mobile-device users. Some of the other keystroke dynamics-based methods can be found in [51]–[53].

In keystroke dynamics, users are identified based on their typing patterns.

Mobile-device movement and the ambient noise measured by smartphone microphones were used in [54] to implicitly authenticate mobile-device users. Based on the data captured from nine subjects, the authors reported recognition accuracy of 88.3%, 47.8%, and 90.1% for movement, audio, and the combination of these two features, respectively. Furthermore, [55] studied the feasibility of voice biometrics on mobile devices. It was shown that a mobile user's identity could be verified by his or her voice with an EER of 7.77%. In [56], linguistic profiling was used to authenticate users based on their writing vocabulary and style of short-message-service message. Experimental results based on 30 participants showed that linguistic profiling can be successfully used to authenticate users, with low error rates.

Several studies have used contextual information to enhance the performance of continuous authentication. For example, [57] investigates how the position in which the smartphone is held affects user authentication. Another

Table 4. Key behavior profiling-based continuous authentication methods for mobile devices.

Study	Behavior	Data Set (Users)	Classifier	Performance (%)
Li et al. [43]	Application usage	MIT Reality	Neural net	EER: 13.5
Li et al. [43]	Text message	MIT Reality	Neural net	EER: 2.2
Li et al. [43]	Calls	MIT Reality	Neural net	EER: 5.4
Li et al. [44]	Historical usage data	MIT Reality	Neural net	EER: 9.8
Neal et al. [49]	Application usage, Bluetooth, and Wi-Fi	UND data set (200)	Nearest neighbor	RR: 80-93

context-aware continuous authentication method [58] proposes to use passive as well as active factors to continuously authenticate users. The authors argue that digital sensors, combined with models of people and places, can give some information about user identity. In [59], contextual application information is used to improve user authentication based on touch gestures.

Fusion of multiple modalities

Unimodal continuous authentication systems rely on a single source of information, such as touch gestures, faces, or behavior profiling. Such unimodal systems have to deal with some of the following inevitable problems [60]:

- *Noisy data*: Poor lighting on a user's face or occlusion are examples of noisy data.
- *Nonuniversality*: The continuous authentication system based on a single source of evidence may not be able to capture meaningful data from some users. For instance, gait-based systems may extract incorrect patterns for certain users due to leg injuries.
- *Intraclass variations*: These often occur when a user incorrectly interacts with the sensor.
- *Spoof attack*: Using a photograph to gain access to a user's mobile device is an example of this type of attack.

It has been observed that some of the limitations of unimodal continuous authentication systems can be addressed by deploying multimodal systems that essentially integrate the evidence presented by multiple sources of information such as touch gestures and faces. Such systems are less vulnerable to spoof attacks, as it would be difficult for an imposter to simultaneously spoof multiple biometric traits of a genuine user.

Some of the limitations of unimodal continuous authentication systems can be addressed by deploying multimodal systems that essentially integrate the evidence presented by multiple sources of information such as touch gestures and faces.

Classification in multimodal systems is done by fusing information from different modalities. The information fusion can be done at different levels, which can be broadly divided into feature-level, score-level, and rank/decision-level fusion. Several methods have been proposed in the literature that make use of multiple modalities for continuous authentication. For instance, a feature-level fusion method based on multitask multivariate low-rank representations was recently proposed in [61] for fusing touch gestures and faces for continuous authentication. A decision-level fusion method was proposed in [62] for fusing four modalities based on stylometry (text analysis), application usage patterns, web browsing behavior, and physical location of the device for continuous authentication. The analysis performed on a data set of 200 Android mobile-device users whose data were collected for a period of at least 30 days showed that the method can achieve an EER of 0.05 using a one-minute window and an EER below 0.01 using a 30-minute window. Similarly, in [63] a SenGuard system was proposed in which multiple modalities are fused at the decision level for continuous authentication. Data from the accelerometer, touch screen, and microphone as well as location history are used to continuously monitor the user identity on a mobile device. In the authors' approach, they rely on the Jigsaw continuous sensing engine [64] to process the motion and voice data. Furthermore, their touch-based method can handle single as well as multitouch gestures.

A bimodal continuous authentication method based on face and speaker recognition was proposed in [65]. The authors' face detection and recognition approach is based on LBPs [23]. For speaker recognition, voice activity detection is first performed using a Hungarian downscaled phoneme recognizer, which is essentially the cascade of three neural networks. After voice activity detection, all valid frames are passed to the speaker-authentication component, which uses an *i*-vector extractor to obtain features that are then modeled using probabilistic linear discriminant analysis. Finally, similarity scores for face authentication and the log-likelihood scores for speaker authentication are normalized to produce probabilities and fused by taking the product of the two resulting scores.

Recently, a set of behavioral features called hand movement, orientation, and grasp (HMOG) was proposed in [66] to continuously authenticate smartphone users. HMOG is essentially based on the accelerometer, gyroscope, and magnetometer readings and captures subtle hand micromovements and orientation patterns generated when a user taps on the screen. A set of 96 HMOG features was proposed and evaluated on a data set consisting of 100 users' typing data. It was shown that one can achieve authentication EERs as low as 7.16% (walking) and 10.05% (sitting) when the HMOG features are combined with tap and keystroke features using a score-level fusion framework [66]. Table 5 summarizes the key multimodal fusion methods for continuous authentication in terms of their performance on various data sets. In this table, the half total error rate (HTER) is noted for one of the studies.

In [67], three different text-based biometric modalities—linguistic profiling, behavioral profiling, and keystroke dynamics—were fused using a score-level fusion method for continuous authentication. Since there is no multimodal data set that consists of these three text-based biometric modalities for the same individual, these modalities were combined from different data sets to create a virtual data set of 30 users. Based on this data set, the authors reported an average EER of 3.3% when linguistic profiling, behavioral profiling, and keystroke dynamics are fused.

Summary of continuous authentication approaches

As discussed previously, several physiological and behavioral biometrics-based techniques have direct application

Table 5. Key multimodal fusion-based continuous authentication methods for mobile devices.

Study	Modalities	Number of Users	Fusion Method	Performance (%)
Zhang et al. [61]	Face, touch gestures	50	Feature level	RR: 83.75
Fridman et al. [62]	Stylometry, application usage, web browsing, GPS location	200	Decision level	EER: 5 (One minute), 1 (30 minute)
Shi et al. [63]	Accelerometer, touch screen, microphone, location history	Seven	Decision level	EER: -
McCool et al. [65]	Face, voice	152	Score level	HTER: 11.9 (male), 13.3 (female)
Sitova et al. [66]	HMOG, tap, keystroke	100	Score level	EER: 7.16 (walking), 10.05 (sitting)
Saevanee et al. [67]	Linguistic profiling, behavioral profiling, keystroke dynamics	30	Score level	EER: 3.3 (weighting) - 4.4 (sum)

within a continuous authentication framework. Several research studies have specifically focused on the applicability of these biometrics modalities for nonintrusive authentication. It is seen that physiological biometrics such as the face can provide higher authentication accuracy than behavioral biometrics such as gait or touch gestures. Further, as behavioral biometric characteristics tend to change over time and under various environmental conditions, one has to constantly update the templates to maintain the performance of these techniques. The tradeoff among computation, processing speed, and accuracy has to be considered when using these modalities for transparent authentication. For example, the face-based continuous authentication system requires one to detect, align, and recognize faces from the images or videos collected from the front-facing camera. Each of these subalgorithms can be very time consuming, making the overall matching algorithm computationally demanding and not real time. In contrast, touch gesture-based methods often do not require detection or segmentation of data. Hence, they could be more efficient in terms of processing speed. It can be concluded that there is not a single biometric modality that is ideally suited for all scenarios. However, a significant amount of prior research has shown that continuous authentication methods based on multiple biometric traits are often superior to unimodal continuous authentication systems.

Physiological biometrics such as the face can provide higher authentication accuracy than behavioral biometrics such as gait or touch gestures.

Usability and security issues

The usability of transparent continuous authentication systems on mobile devices has become a major issue in research [5], [68], [69]. A balance needs to be struck between security and usability of a biometrics-based continuous authentication system. The design of usable yet secure continuous user authentication systems raises crucial questions concerning how to solve conflicts between mobile security and usability. For instance, in the continuous authentication context, a false rejection is less costly than a false acceptance. This is due to the fact that higher false acceptance rates will lower the security level of the continuous authentication system, while a higher false rejection rate will frustrate a legitimate user, which is less dangerous than a lower security level. It was argued in [70] that to be able to build reliable, effective, and usable systems, one needs specific guidelines that take into account the specific constraints of security mechanisms. Furthermore, security systems should be built so as to be easy to learn and use by users with different backgrounds and skills. It was also argued that human factors should be incorporated into the design of continuous authentication systems, where usability is central during the whole development process.

Several works have discussed the issue of usability of continuous authentication systems. For instance, in [68] a prototype was developed using keystroke, voice, and face biometrics for continuous authentication. The prototype was evaluated using 27 participants, and the study reported that 92% of the participants considered it more secure in comparison to the traditional methods of authentication. Similarly, [69] conducted an in-lab study of security perception of implicit authentication with 30 users based on behavioral biometrics. In their study, the researchers asked users to complete a series of tasks on a smartphone that was ostensibly protected with varying degrees of transparent authentication. They then surveyed the participants regarding their opinion about transparent authentication. They found that 73% of participants felt that implicit authentication based on behavioral biometrics was more secure than traditional methods such as PINs and passwords and 90% indicated that they would consider using a transparent authentication method on their own mobile device.

More recently, a two-part study consisting of a controlled lab experiment and a field study was conducted in [5] on implicit authentication usability and security perceptions with 37 participants. The study indicated that 91% of participants found implicit authentication to be convenient and 81% perceived the provided level of protection to be satisfactory. Furthermore, the authors found that false accepts and detection delay were prime security concerns for 27% and 22% of the participants, respectively. Also, 35% of the participants were annoyed by false rejects. These studies show that users are willing to consider trying mobile transparent and continuous authentication methods based on biometrics, as they see a need for alternatives to secret knowledge techniques such as passwords and PINs.

Discussions and future directions

This article presented an overview of recent advances in mobile-based continuous authentication methods that included behavioral, physiological, and multimodal biometrics-based fusion methods. We hope that the survey has helped to guide an interested reader among the extensive literature to some degree. Obviously, it could not cover all the literature on continuous authentication, so we chose to focus on a representative subset of the latest progress made in biometrics and the security community. 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 the computation power of mobile devices is increasing tremendously. There are, however, several challenges to be overcome before successfully designing a biometrics-based continuous authentication system. These challenges include the following.

1) The biometric data at enrollment time may have different characteristics than those presented during authentication. For example, in the case of the face biometric, the enrolled faces are usually frontal and well illuminated. However, during authentication the mobile device has to process faces that may have very poor illumination, severe pose variations, or missing facial parts. This problem where the training (enrolled) data used to learn a recognition or authentication model have a different distribution from the data on which the model is applied is often known as *domain adaptation* [71]. One such method based on faces and touch gestures for continuous authentication using domain adaptation was recently proposed in [72]. Domain adaptation and transfer learning techniques can be used to deal with the changing distribution problem in continuous authentication. More domain adaptive methods for mobile-based continuous authentication are needed.
2) As more and more continuous authentication systems are becoming available, businesses have started to integrate these technologies into their products. Often, continuous authentication technologies are outsourced to companies that provide authentication and identity assurance as a service, because deploying and maintaining these technologies require specialized expertise and infrastructure. This raises privacy concerns, because biometric information is disclosed to a third party. To deal with this issue, methods for securely outsourcing continuous authentication systems are needed [73].
3) Some of the behavioral biometrics-based continuous authentication methods discussed in this article are based on very simple features. For instance, most touch gesture-based methods make use of very simple features based on the x, y coordinates and time information. However, they usually do not make use of the dynamics present in the touch gestures. We feel that incorporating the dynamics as well as the geometry of touch gestures into a feature extraction algorithm can significantly enhance the performance of a touch based continuous authentication system. Selection of appropriate features is another important problem to be addressed in continuous authentication.
4) Some of the physiological as well as behavioral biometrics-based continuous authentication methods are vulnerable to spoof, mimic, statistic, or digital replay attacks [74], [75]. For example, one can spoof speaker authentication systems by using voice morphing techniques. Some efforts have been made in the literature to address these issues for continuous authentication. However, more is needed. For instance, in the case of face biometrics, making use of additional sensors for liveness detection would counter the problem of spoof attacks.
5) Many continuous authentication methods have been proposed in the literature that evaluate the performance of their proposed method on a variety of different data sets 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.
6) As discussed in the previous section, most continuous authentication methods ignore the usability and acceptability issues. Even though a few recent works have attempted to address these issues, more is needed.
7) Unlike credit cards and passwords, which can be revoked and reissued when compromised, biometrics are permanently associated with a user and cannot be replaced. To prevent the theft of the biometric patterns of mobile-device users, biometric template protection schemes such as cancelable biometrics [76] should be incorporated within the continuous authentication framework.
8) Most mobile-based continuous authentication techniques discussed in this article have been evaluated on small and midsize data sets consisting of hundreds of samples. However, 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 data sets containing thousands and millions of samples.

Authors

Vishal M. Patel (vishal.m.patel@rutgers.edu) is an assistant professor in the Department of Electrical and Computer Engineering at Rutgers University, Piscataway, New Jersey. Prior to joining Rutgers University, he was a member of the research faculty at the University of Maryland Institute for Advanced Computer Studies. His research interests include

signal processing, computer vision, and machine learning, with applications to radar imaging and biometrics. He is a recipient of the 2016 Office of Naval Research Young Investigator Award and the 2010 Oak Ridge Associated Universities postdoctoral fellowship. He is member of Eta Kappa Nu, Pi Mu Epsilon, and Phi Beta Kappa. He is a Senior Member of the IEEE.

Rama Chellappa (rama@umd.edu) is a professor of electrical and computer engineering (ECE) and an affiliate professor of computer science at the University of Maryland, College Park. He is also affiliated with the Center for Automation Research, Institute for Advanced Computer Studies (permanent member), and is the chair of the ECE Department. In 2005, he was named a Minta Martin Professor of Engineering. His current research interests are clustering; three-dimensional modeling from video; image- and video-based recognition of objects, events, and activities; dictionary-based inference; compressive sensing; domain adaptation; and hyperspectral processing. He is a Fellow of the IEEE, the Association for Computing Machines, the International Association of Pattern Recognition, the Optical Society of America, the American Association for the Advancement of Science, and the Association for the Advancement of Artificial Intelligence.

Deepak Chandra (dchandra@google.com) heads authentication in the Machine Intelligence and Research group at Google Inc., Mountain View, California. The project aims to completely redefine authentication for the digital and physical worlds. Prior to this, he was the program lead in Google's Advanced Technology and Projects organization, where he headed all product engineering and design for mobile authentication projects. He defined company-wide authentication strategy for Motorola prior to leading the efforts at Google. He has developed multiple wearable authentication products, including Motorola Skip and Digital Tattoo.

Brandon Barbello (bbarbello@google.com) is a product manager at Google Research and Machine Intelligence, where he works on privacy-sensitive, on-device machine learning. He was previously involved with the Google Advanced Technology and Projects organization on the Project Abacus team, where he managed efforts to develop a multimodal continuous authentication system for smartphones. Prior to his time at Google, he cofounded four companies in electronics, fintech, and private equity.

References

[1] N. Clarke and S. Furnell, "Authentication of users on mobile telephones: A survey of attitudes and practices," *Comput. and Security*, vol. 24, no. 7, pp. 519–527, 2005.

[2] A. Vance. (2010, Jan. 20). If your password is 123456, just make it hackme [Online]. Available: http://www.nytimes.com

[3] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. 4th USENIX Conf. Offensive Technol.*, 2010, pp. 1–7.

[4] D. Tapellini. (2014, May 28). *Smart phone thefts rose to 3.1 million in 2013:* Industry solution falls short, while legislative efforts to curb theft continue [Online]. Available: http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

[5] H. Khan, U. Hengartner, and D. Vogel, "Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying," in *11th Symp. Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 225–239.

[6] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are you ready to lock?" in *Proc. 2014 ACM SIGSAC Conf. Comput. and Commun. Security*, 2014, pp. 750–761.

[7] M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in *Symp. Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 213–230.

[8] R. P. Guidorizzi, "Security: Active authentication," *IT Professional*, vol. 15, no. 4, pp. 4–7, July/Aug. 2013.

[9] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," in *Proc. USENIX*, 2009, pp. 1–9.

[10] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," in *Proc. 13th Int. Conf. Inform. Security*, 2011, pp. 99–113.

[11] N. L. Clarke, *Transparent User Authentication: Biometrics, RFID and Behavioural Profiling*. London: Springer, 2011.

[12] D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain, "Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data," in *Int. Conf. Biometrics*, 2015, pp. 135–142.

[13] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Trans. Inform. Forensics and Security*, vol. 8, no. 1, pp. 136–148, 2013.

[14] L. Li, X. Zhao, and G. Xue, "Unobservable reauthentication for smart phones," in *Proc. 20th Network and Distributed Syst. Security Symp.*, 2014, pp. 1–16.

[15] A. Serwadda, V. Phoha, and Z. Wang, "Which verifiers work? A benchmark evaluation of touch-based authentication algorithms," in *Proc. IEEE Int. Conf. Biometrics: Theory, Applications and Systems*, Sept. 2013, pp. 1–8.

[16] H. Zhang, V. M. Patel, M. E. Fathy, and R. Chellappa, "Touch gesture-based active user authentication using dictionaries," in *Proc. IEEE Winter Conf. Applicat. Comput. Vision*, 2015, pp. 207–214.

[17] T. Feng, Z. Liu, K. A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in *Proc. IEEE Conf. Technol. Homeland Security*, Nov. 2012, pp. 451–456.

[18] M. Sherman, G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvirta, and T. Roos, "User-generated free-form gestures for authentication: Security and memorability," in *Proc. 12th Annu. Int. Conf. Mobile Syst., Applicat., and Services*, 2014, pp. 176–189.

[19] X. Zhao, T. Feng, and W. Shi, "Continuous mobile authentication using a novel graphic touch gesture feature," in *Proc. IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst.*, Sept. 2013, pp. 1–6.

[20] X. Zhao, T. Feng, W. Shi, and I. Kakadiaris, "Mobile user authentication using statistical touch dynamics images," *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 11, pp. 1780–1789, 2014.

[21] A. Hadid, J. Heikkila, O. Silven, and M. Pietikainen, "Face and eye detection for person authentication in mobile phones," in *Proc. ACM/IEEE Int. Conf. Distributed Smart Cameras*, Sept. 2007, pp. 101–108.

[22] P. A. Viola and M. J. Jones, "Robust real-time face detection," *Int. J. Comput, Vision*, vol. 57, no. 2, pp. 137–154, 2004.

[23] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Trans. Pattern Anal. and Mach. Intell.*, vol. 24, no. 7, pp. 971–987, 2002.

[24] S. Sarkar, V. M. Patel, and R. Chellappa, "Deep feature-based face detection on mobile devices," in *Proc. IEEE Int. Conf. Identity, Security and Behavior Anal.*, 2016.

[25] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Advances in Neural Inform. Processing Syst.*, 2012, pp. 1097–1105.

[26] M. E. Fathy, V. M. Patel, and R. Chellappa, "Face-based active authentication on mobile devices," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, 2015, pp. 1687–1691.

[27] U. Mahbub, V. M. Patel, D. Chandra, B. Barbello, and R. Chellappa, "Partial face detection for continuous authentication," in *Proc. IEEE Int. Conf. Image Processing*, 2016.

[28] P. Abeni, M. Baltatu, and R. D'Alessandro, "Nis03-4: Implementing biometrics-based authentication for mobile devices," in *Proc. IEEE Global Telecommun. Conf.*, Nov. 2006, pp. 1–5.

[29] S. Chen, A. Pande, and P. Mohapatra, "Sensor-assisted facial recognition: An enhanced biometric authentication system for smartphones," in *Proc. 12th Annu. Int. Conf. Mobile Syst., Applicat., and Services*, 2014, pp. 109–122.

[30] N. Kumar, A. Berg, P. Belhumeur, and S. Nayar, "Describable visual attributes for face verification and image search," *IEEE Trans. Pattern Anal. and Mach. Intell.*, vol. 33, no. 10, pp. 1962–1977, 2011.

[31] P. Samangouei, V. M. Patel, and R. Chellappa, "Attribute-based continuous user authentication on mobile devices," in *Proc. IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst.*, 2015, pp. 1–8.

[32] J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S. M. Makela, and H. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, March 2005, vol. 2, pp. ii/973–ii/976.

[33] M. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Proc. Int. Conf. Intelligent Inform. Hiding and Multimedia Signal Processing*, Oct. 2010, pp. 306–311.

[34] F. Juefei-Xu, C. Bhagavatula, A. Jaech, U. Prasad, and M. Savvides, "Gait-ID on the move: Pace independent human identification using cell phone accelerometer dynamics," in *Proc. IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst.*, Sept. 2012, pp. 8–15.

[35] C. Nickel, C. Busch, S. Rangarajan, and M. Mobius, "Using Hidden Markov Models for accelerometer-based biometric gait recognition," in *Proc. IEEE Int. Colloq. Signal Processing and Its Applicat.*, March 2011, pp. 58–63.

[36] H. M. Thang, V. Q. Viet, N. D. Thuc, and D. Choi, "Gait identification using accelerometer on mobile phone," in *Proc. Int. Conf. Control, Automation and Inform. Sci.*, Nov. 2012, pp. 344–348.

[37] M. Muaaz and R. Mayrhofer, "An analysis of different approaches to gait recognition using cell phone based accelerometers," in *Proc. Int. Conf. Advances in Mobile Computing and Multimedia*, 2013, pp. 293:293–293:300.

[38] Y. Zhong, Y. Deng, and G. Meltzner, "Pace independent mobile gait biometrics," in *Proc. IEEE Int. Conf. Biometrics Theory, Applicat. and Syst.*, Sept. 2015, pp. 1–8.

[39] Y. Zhong and Y. Deng, "Sensor orientation invariant mobile gait biometrics," in *Proc. IEEE Int. Joint Conf. Biometrics*, Sept. 2014, pp. 1–8.

[40] P. Gosset, "Aspect: Fraud detection concepts: Final report," Tech. Rep. AC095/VOD/W22/DS/P/18/1, Jan. 1998.

[41] Y. Moreau, H. Verrelst, and J. Vandewalle, "Detection of mobile phone fraud using supervised neural networks: A first prototype," in *Proc. Int. Conf. Artificial Neural Networks*, 1997, pp. 1065–1070.

[42] J. Hall, M. Barbeau, and E. Kranakis, "Anomaly-based intrusion detection using mobility profiles of public transportation users," in *Proc. IEEE Int. Conf. Wireless and Mobile Computing, Networking and Commun.*, Aug. 2005, vol. 2, pp. 17–24.

[43] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Behaviour profiling for transparent authentication for mobile devices," in *Proc. Euro. Conf. Inform. Warfare and Security*, 2011, pp. 307–314.

[44] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Active authentication for mobile devices utilising behaviour profiling," *Int. J. Inform. Security*, vol. 13, no. 3, pp. 229–244, June 2014.

[45] D. Bassu, M. Cochinwala, and A. Jain, "A new mobile biometric based upon usage context," in *Proc. IEEE Int. Conf. Technol. for Homeland Security*, Nov. 2013, pp. 441–446.

[46] N. Eagle and A. Pentland, "Reality mining: Sensing complex social systems," *Personal and Ubiquitous Computing*, vol. 10, no. 4, pp. 255–268, May 2006.

[47] N. A. Safa, R. Safavi-Naini, and S. F. Shahandashti, "Privacy-Preserving Implicit Authentication," in *ICT Systems Security and Privacy Protection*, N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 471–484.

[48] H. G. Kayacik, M. Just, L. Baillie, D. Aspinall, and N. Micallef, "Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors," *CoRR*, 2014 vol. abs/1410.7743.

[49] T. Neal, D. Woodard, and A. Striegel, "Mobile device application, Bluetooth, and Wi-Fi usage data as behavioral biometric traits," in *Proc. IEEE Int. Conf. Biometrics Theory, Applicat. and Syst.*, Sept. 2015, pp. 1–6.

[50] T. Y. Chang, C. J. Tsai, and J. H. Lin, "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices," *J. Syst. and Software*, vol. 85, no. 5, pp. 1157–1165, 2012.

[51] N. Clarke and S. Furnell, "Advanced user authentication for mobile devices," *Computers and Security*, vol. 26, no. 2, pp. 109–119, 2007.

[52] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," *Int. J. Inform. Security*, vol. 6, no. 1, pp. 1–14, Dec. 2006.

[53] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous authentication on mobile devices by analysis of typing motion behavior," presented at *Proc. GI Conf. Sicherheit (Sicherheit, Schutz und Verlsslichkeit)*, 2014.

[54] H. Ketabdar, M. Roshandel, and D. Skripko, "Towards implicit enhancement of security and user authentication in mobile devices based on movement and audio analysis," in *Proc. 4th Int. Conf. Advances in Comput.-Human Interactions*, 2011, pp. 188–191.

[55] R. Woo, A. Park, and T. Hazen, "The MIT mobile device speaker verification corpus: Data collection and preliminary experiments," in *Proc. Odyssey, The Speaker and Language Recognition Workshop*, 2006, pp. 1–6.

[56] H. Saevanee, N. L. Clarke, and S. M. Furnell, "SMS linguistic profiling authentication on mobile devices," in *Proc. 5th Int. Conf. Network and Syst. Security*, 2011, pp. 224–229.

[57] A. Primo, V. Phoha, R. Kumar, and A. Serwadda, "Context-aware active authentication using smartphone accelerometer measurements," in *Proc. IEEE Conf. Comput. Vision and Pattern Recognition Workshops*, June 2014, pp. 98–105.

[58] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, "CASA: Context-aware scalable authentication," in *Proc. 9th Symp. Usable Privacy and Security*, 2013, pp. 3:1–3:10.

[59] T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. Shi, "Tips: Context-aware implicit user identification using touch screen in uncontrolled environments," in *Proc. Workshop on Mobile Comput. Syst. and Applicat.*, 2014, pp. 9:1–9:6.

[60] A. Ross and A. K. Jain, "Multimodal biometrics: An overview," in *Proc. Euro. Signal Processing Conf.*, 2004, pp. 1221–1224.

[61] H. Zhang, V. M. Patel, and R. Chellappa, "Robust multimodal recognition via multitask multivariate low-rank representations," in *Proc. IEEE Int. Conf. Automatic Face and Gesture Recognition*, May 2015, vol. 1, pp. 1–8.

[62] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, GPS location, web browsing behavior, and application usage patterns," *IEEE Syst. J.*, 2015.

[63] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong, "Senguard: Passive user identification on smartphones using multiple sensors," in *Proc. IEEE Int. Conf. Wireless and Mobile Comput., Networking and Commun.*, 2011, pp. 141–148.

[64] H. Lu, J. Yang, Z. Liu, N. D. Lane, T. Choudhury, and A. T. Campbell, "The jigsaw continuous sensing engine for mobile phone applications," in *Proc. 8th ACM Conf. Embedded Networked Sensor Syst.*, 2010, pp. 71–84.

[65] C. McCool, S. Marcel, A. Hadid, M. Pietikainen, P. Matejka, J. Cernocky, N. Poh, J. Kittler, A. Larcher, C. Levy, D. Matrouf, J. F. Bonastre, P. Tresadern, and T. Cootes, "Bi-modal person recognition on a mobile phone: Using mobile phone data," in *Proc. IEEE Int. Conf. Multimedia and Expo Workshops*, July 2012, pp. 635–640.

[66] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Trans. Inform. Forensics Security*, vol. 11, no. 5, pp. 877–892, May 2016.

[67] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Text-based active authentication for mobile devices," in *ICT Systems Security and Privacy Protection*, N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, Eds. Berlin, Heidelberg: Springer, 2014, pp. 99–112.

[68] N. Clarke, S. Karatzouni, and S. Furnell, "Flexible and Transparent User Authentication for Mobile Devices," in *Emerging Challenges for Security, Privacy and Trust*, D. Gritzalis and J. Lopez, Eds. Berlin, Heidelberg: Springer, 2009, pp. 1–12.

[69] H. Crawford and K. Renaud, "Understanding user perceptions of transparent authentication on a mobile device," *J. Trust Manage.*, vol. 1, no. 7, pp. 1–28 2014.

[70] C. Braz and J.-M. Robert, "Security and usability: The case of the user authentication methods," in *Proc. 18th Conf. L'Interaction Homme-Machine*, 2006, pp. 199–203.

[71] V. M. Patel, R. Gopalan, R. Li, and R. Chellappa, "Visual domain adaptation: A survey of recent advances," *IEEE Signal Processing Mag.*, vol. 32, no. 3, pp. 53–69, May 2015.

[72] H. Zhang, V. M. Patel, S. Shekhar, and R. Chellappa, "Domain adaptive sparse representation-based classification," in *Proc. IEEE Int. Conf. Automatic Face and Gesture Recognition*, vol. 1, May 2015, pp. 1–8.

[73] J. Sedenka, S. Govindarajan, P. Gasti, and K. Balagani, "Secure outsourced biometric authentication with performance evaluation on smartphones," *IEEE Trans. Inform. Forensics and Security*, vol. 10, no. 2, pp. 384–396, Feb. 2015.

[74] D. F. Smith, A. Wiliem, and B. C. Lovell, "Binary watermarks: A practical method to address face recognition replay attacks on consumer mobile devices," in *Proc. IEEE Int. Conf. Identity, Security and Behavior Anal.*, Mar. 2015, pp. 1–6.

[75] D. F. Smith, A. Wiliem, and B. C. Lovell, "Face recognition on consumer devices: Reflections on replay attacks," *IEEE Trans. Inform. Forensics and Security*, vol. 10, no. 4, pp. 736–745, Apr. 2015.

[76] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Mag.*, vol. 32, no. 5, pp. 54–65, Sept. 2015.