Continuous User Authentication on Mobile Devices: Recent Progress and Remaining Challenges

Vishal M. Patel, *Senior Member, IEEE,*, Rama Chellappa, *Fellow, IEEE*, Deepak Chandra, and Brandon Barbello

Abstract

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, one has to constantly worry about the security and privacy as the loss of a mobile device could compromise personal information of the user. To deal with this problem, continuous authentication (also known as active authentication) systems have been proposed in which users are continuously monitored after the initial access to the mobile device. In this paper, we provide an overview of different continuous authentication methods on mobile devices. We discuss the merits and drawbacks of available approaches and identify promising avenues of research in this rapidly evolving field.

Index Terms

Mobile authentication, continuous authentication, biometrics, active authentication, transparent authentication.

Vishal M. Patel is with the department of Electrical and Computer Engineering (ECE) at Rutgers University, Piscataway, NJ 08854 USA vishal.m.patel@rutgers.edu.

Rama Chellappa is with the Center for Automation Research, UMIACS, University of Maryland, College Park, MD 20742 USA rama@umd.edu.

Deepak Chandra, and Brandon Barbello are with Google Inc, Mountain View, CA 94043 USA {dchandra,bbarbello}@google.com.

I. 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 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 photo, one can easily deduce the secret pattern (see Figure 1) [3].

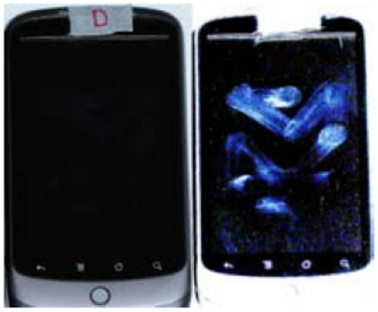

Fig. 1: Smudge attack [3]. Secret pattern can be determined with special lighting and high-resolution camera.

Furthermore, recent studies have shown that about 34% or more users did not use any form of authentication mechanism on their devices [4], [5], [6], [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]. In their study, [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 unlocking the screens. 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 mobile device. Thus, unauthorized individuals may improperly 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.

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 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 2 highlights some of the sensors and accessaries available in a modern mobile device. These sensors are capable of providing raw data with high precision and accuracy, and are useful to monitor three-dimensional 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.

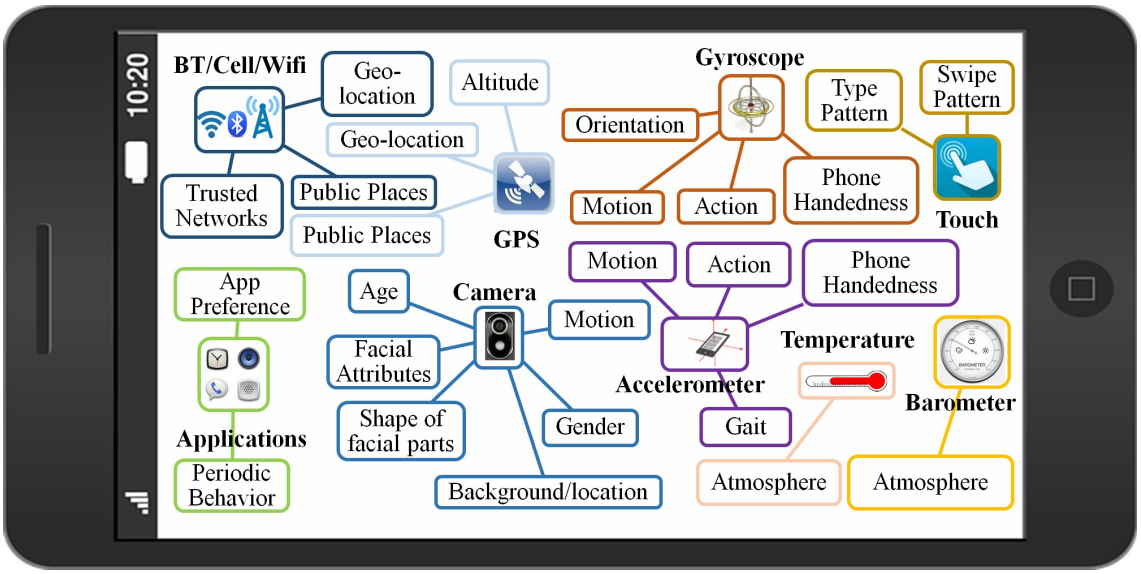

Fig. 2: Sensors and accessories available in a mobile device. Raw information collected by these sensors can be used to continuously authenticate a mobile device user.

Our goal in this paper 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 mobile devices is important as we are becoming increasingly dependent on mobile devices.

Rest of the paper is organized as follows. Section II reviews various recent continuous authentication approaches. Usability and security issues are discussed in Section III. Finally, Section IV concludes the paper with a brief summary and discussion.

II. 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 the legitimate user then the biometric system will continue processing the new incoming data. However, if the biometric system produces a negative response then 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 verify his identity then he will be able to use the mobile device, otherwise the device will be locked.

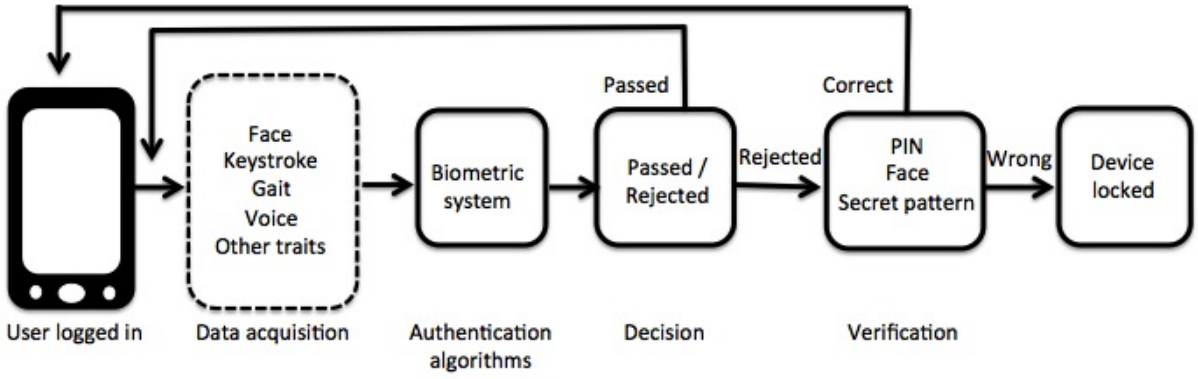

Fig. 3: A biometrics-based mobile continuous authentication framework [12].

In a practical continuous authentication system the entire processing 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.

A. Touch Dynamics

Touch dynamics is one of the most commonly used continuous authentication methods for mobile devices. In touch dynamics, touchscreen input is used as a data source. In particular, screen touch gestures, the way users swipe their fingers on the touchscreen of their mobile devices, are used as a behavioral biometric to continuously authenticate users while they perform basic operations on the smartphone.

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 pressures, the screen areas covered by each finger and time information can be used to extract useful features.

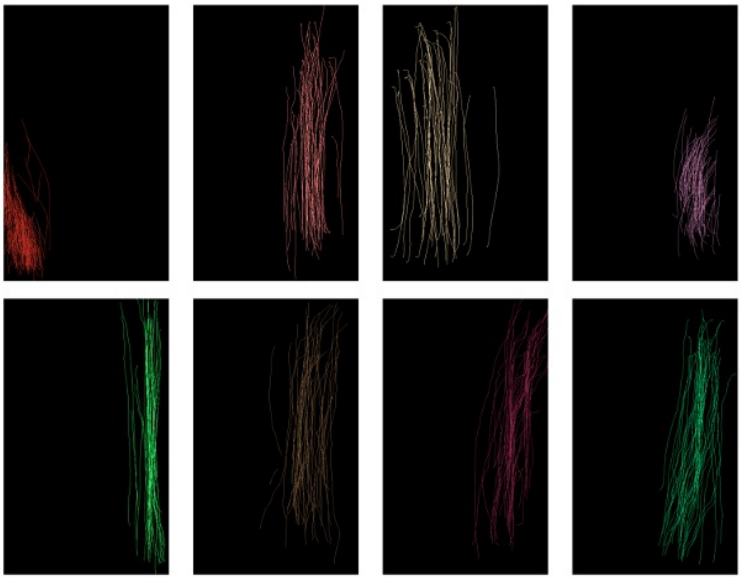

Fig. 4: Swipes of 8 different users while reading text [13]. Different colors are used to show swipes from different users.

A swipe or a stroke on the touchscreen 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

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

where x_i, y_i are the location points, and $t_i, p_i, A_i, O_i^f, O_i^{ph}$ 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. These features are: mid-stroke area covered, 20%-perc. pairwise velocity, mid-stroke 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%-perc. pairwise velocity, median velocity at last 3 pts, 50%-perc. pairwise velocity,

20%-perc. pairwise acceleration, ratio end-to-end dist and length of trajectory, largest deviation from end-to-end line, 80%-perc. pairwise acc, mean resultant length, median acceleration at first 5 points, 50%-perc. dev. from end-to-end line, inter-stroke time, 80%-perc. dev. from end-to-end line, 20%-perc. dev. from end-to-end line, 50%-perc. pairwise acceleration, phone orientation, mid-stroke finger orientation, up/down/left/right flag, and change of finger orientation. After feature analysis, 3 of these features were discarded and the remaining 27 features were evaluated using a kernel support vector machine (SVM) and k-nearest-neighbors (kNN) classifiers on a dataset 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 also been used in [14], [15] and [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].

The methods presented in [13], [14], [15], [16] are essentially based on the fact that only a single finger is in contact with the touchscreen while users are performing basic operations. In practice, many applications require users to use 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, directions of the 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 that the dynamics of swipes can be explicitly modeled. Furthermore, the pressure dynamics is emphasized by fusing it 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 intra-person 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 swipes and multifinger swipes. Figure 5 shows the GTGF features extracted from two users in the first and second row, respectively.

Table I compares all of the aforementioned touch dynamics-based continuous authentication methods. Here, FAR and FRR stand for false accept rate and false reject rate, respectively. As can be seen from this table, some methods achieve very low EER values on certain datasets. These works have demonstrated

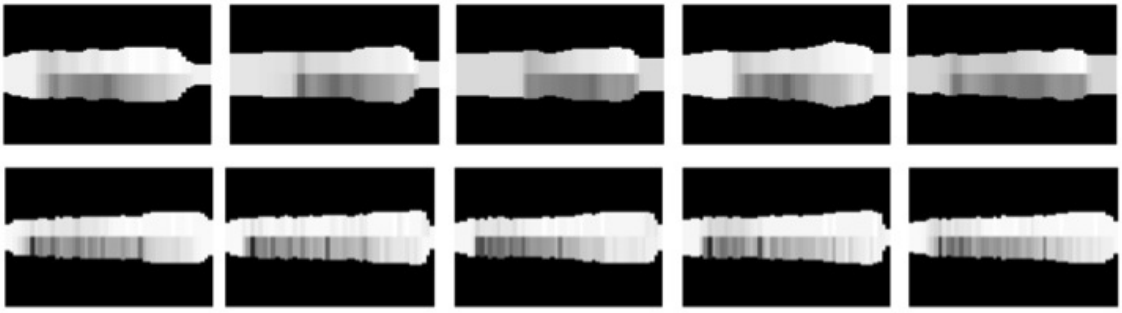

Fig. 5: The GTGF features corresponding to two different users [19]. First row shows the GTGF features corresponding to five touch gestures of a single user while the second row shows the GTGF features extracted from five swipes from a different user.

that touch gestures can be used as a promising behavioral biometric for continuous user authentication of mobile devices.

TABLE I: Key touch dynamics-based continuous authentication methods. Best results from the corresponding papers are reported.

Study	# of Users	Classifiers	Feature Dimension	Performance (%)
Frank *et al.* [13]	41	SVM, kNN	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: $\sim$ 7.50 , FRR: $\sim$8.00
Serwadda *et al.* [15]	138	10 different classifiers	28	EER: 10.50
Zhao *et al.* [20]	78	L_1 distance	100×150 image	EER: 6.33 - 15.40

B. 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 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 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 and a built-in memory of 31 MB, their work 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 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 5 layers of Alexnet [25]. 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 an overlap criteria. 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 UMD-AA dataset [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.

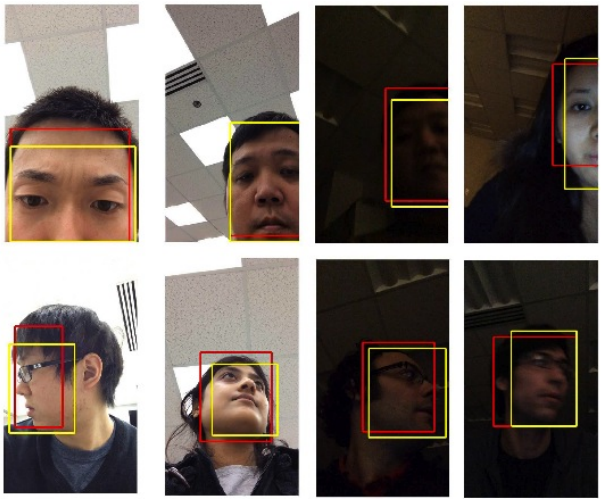

Fig. 6: Examples of positive detections with pose variations and occlusion on the UMD-AA dataset. The detector's output is in red, while ground truth is in yellow [24].

In terms of face recognition on mobile devices, a method based on 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, bi-dimensional Fourier transform features are extracted from the normalized images and are fed into one-class SVM for authentication. In additional 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 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 [21]. In [26], several face recognition methods were evaluated on a dataset 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] which uses the 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 which 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 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 are trained using the PubFig dataset [30] 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 with an LBP-based method such as [21] to obtain improved matching performance.

Table II summarizes key face-based continuous authentication methods. Here, RR TAR, and AAR stand for recognition rate, true accept rate, and average authentication rate, respectively.

C. Gait Dynamics

Gait dynamics-based continuous authentication systems identify users based on how they walk. Data needed for gait-based authentication is often measured by the built-in accelerometer and gyroscope sensors. Once the raw data is measured, discriminative features are extracted which are then fed into a classifier to distinguish users. In recent years, a number of different methods have been developed for gait-

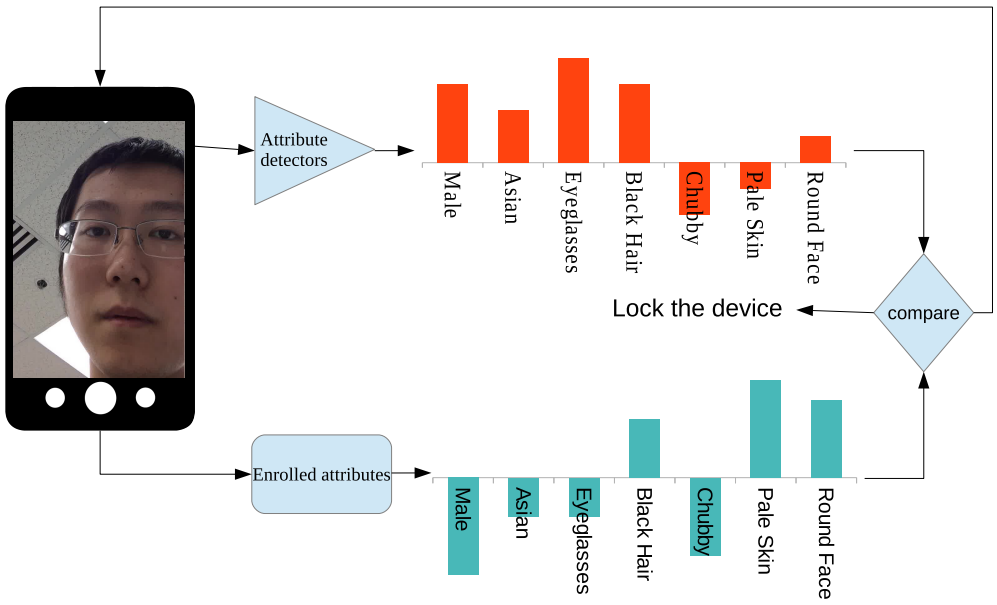

Fig. 7: Overview of the attribute-based authentication method proposed in [31].

TABLE II: Summary of key face-based continuous authentication methods.

Study	# 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: $\sim$ 95
Crouse *et al.* [12]	10	SVM/Biologically inspired model	TAR:$\sim$40-50 @FAR 0.1
Samangouei *et al.* [31]	50	Attributes	EER: 13-30
Perera & Patel [32]	50	Soft biometrics	EER: 10.9-24.1

based recognition on mobile devices [33], [34], [35], [36], [37], [38], [39]. These methods essentially differ in the types of features extracted from 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 [33], while methods based on Dynamic Time Warping (DTW) are used in [37], [38]. Rather than using gait cycles for extracting features, [36] 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 [40]. Given a 3-D time series captured by 3-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 3-axis accelerometer data and its corresponding GDI. As can be seen from this figure, since GDI is invariant to sensor orientation, it shows much better consistency before and after sensor rotation. Also, pace independent gait recognition frameworks have also been proposed in [35] and [39]. In [39], GDIs are used while in [35] cyclostationarity and continuous wavelet transform spectrogram analysis is used for gait-based recognition. Table III summarizes key gait dynamics-based continuous authentication methods in terms of their performances on various datasets. In this table, VR, FNMR and FMR stand for verification rate, false non match rate and false match rate, respectively.

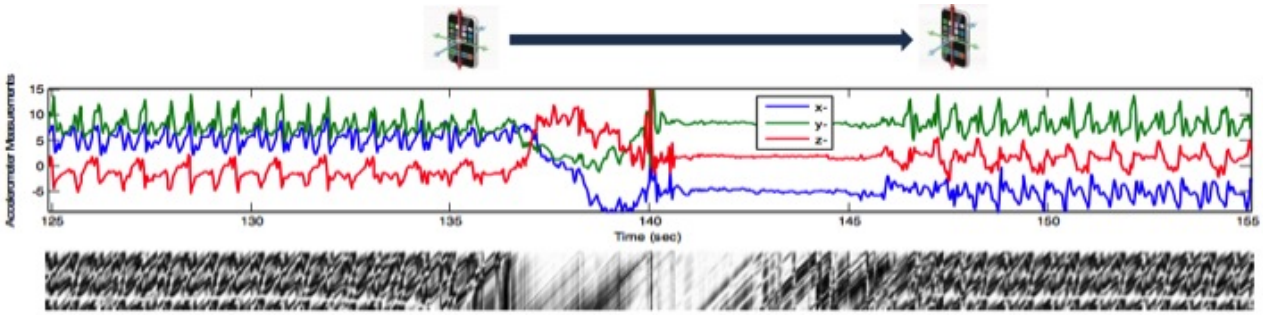

Fig. 8: Top: Data measurements from a 3-axis accelerometer embedded in a mobile phone carried by a walking user. Bottom: the corresponding GDI.

TABLE III: Key gait-based continuous authentication methods for mobile devices.

Study	# of users	Feature	Classifier	Performance (%)
Mantyjarvi *et al.* [33]	36	Raw data	Correlation Coefficients	EER: 7
Thang *et al.* [37]	11	FFT	SVM	Accuracy: 92.7
Muaaz *et al.* [38]	51	Raw data	SVM	EER: 22.49 - 33.30
Nickel *et al.* [36]	48	Raw data	HMM	FNMR 10.42 @ FMR10.29
Zhong *et al.* [39]	51	GDI	Nearest Neighbor	EER: 3.88-7.22
Juefei-Xu *et al.* [35]	36	Wavelets	SVM	61.1 - 99.4 VR @ 0.1 FAR

D. Behavior-based Profiling

The 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 90's focusing mainly on developing

Intrusion Detection System (IDS) to detect telephony service fraud by monitoring user calling and migration behavior [41], [42], [43]. In these systems, user profiles are created by monitoring user activities for a period of time and compared against the current activity profiles of the user. If a significant deviation is observed, a possible intrusion is detected.

Recently, a number of different techniques have been developed in the literature that focus on the use of such methods for continuous authentication [44], [45], [46]. In these methods, application-level as well as application-specific features such as cell ID, date, time and number of calling, duration of call, application time, name and time of application usage are used to continuously monitor the user identity. For instance, an EER of 5.4%, 2.2% and 13.5% have been reported in [44] for telephony, text messaging and general application usage, respectively on the MIT Reality dataset [47]. Historical application usage data has also been utilized to verify mobile users in a continuous manner. [45] 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 [46]. A privacy-preserving implicit authentication system based on behavior profiling has also been proposed in [48]. In [49] a data driven approach was proposed for continuous authentication based on incremental training. They argued that a few weeks of data may not be sufficient for training, but 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 [50]. Discriminative features from these modalities were extracted and a categorical nearest-neighbor classifier was used to produce matching scores. They 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 IV summarizes the results for all the behavior-based profiling methods discussed above.

E. 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, inter-key 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, [51] proposed the use of keystroke dynamics based on the way of user typing graphical-based password to classify the mobile device users. Some of the other keystroke dynamics-based method include [52], [53] and [54].

TABLE IV: Key behavior profiling-based continuous authentication methods for mobile devices.

Study	Behavior	Dataset (Users)	Classifier	Performance (%)
Li *et al.* [44]	Application usage	MIT Reality	Neural Net	EER: 13.5
Li *et al.* [44]	Text message	MIT Reality	Neural Net	EER: 2.2
Li *et al.* [44]	Calls	MIT Reality	Neural Net	EER: 5.4
Li *et al.* [45]	Historical usage data	MIT Reality	Neural Net	EER: 9.8
Neal *et al.* [50]	Application usage, bluetooth & Wi-Fi	UND dataset (200)	Nearest Neighbor	RR: 80-93

Mobile device movement as well as the ambient noise measured by the microphones were used in [55] to implicitly authenticate mobile device users. Based on the data captured from 9 subjects, they reported recognition accuracy of 88.3%, 47.8% and 90.1% for movement, audio and combination of these two features, respectively. Furthermore, [56] studied the feasibility of voice biometric 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 [57] linguistic profiling was used to authenticate users based on their writing vocabulary and style of SMS message. Experimental results based on 30 participants showed that linguistic profiling can be successfully used to authenticate users with low error rates.

Several works have used contextual information to enhance the performance of continuous authentication. For examples, [58] investigates how the position in which the smartphone is held affects user authentication. Another context-aware continuous authentication method [59] proposes to use passive as well as active factors to continuously authenticate the users. They argue that digital sensors combined with models of people and places can give some information about the user identity. In [60] contextual application information is used to improve user authentication based on touch gestures.

F. Fusion of Multiple Modalities

Unimodal continuous authentication systems rely on a single source of information such as touch gestures, faces or behavior profiling for authentication. Unimodal continuous authentication systems have to deal with some of the following inevitable problems [61]: (1) Noisy data: poor lighting on a user's face or occlusion are examples of noisy data. (2) Non-universality: 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 system may extract incorrect patters of certain users due to leg injury. (c) Intra-class variations: These types of variations often occur when a user incorrectly interacts with the sensor. (d)

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.

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 leave fusion method based on multitask multivariate low-rank representations was recently proposed in [62] for fusing touch gestures and faces for continuous authentication. A decision level fusion method was proposed in [63] 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 dataset of 200 Android mobile device users whose data were collected for a period of at least 30 days showed that their method can achieve an EER of 0.05 using 1 minute window and an EER below 0.01 using the 30 minute window. Similarly in [64], a SenGuard system was proposed in which multiple modalities are fused at decision level for continuous authentication. Data from accelerometer, touch screen, microphone as well as location history are used to continuously monitor the user identity on a mobile device. In their approach, they rely on the Jigsaw continuous sensing engine [65] to process the motion and voice data. Furthermore, their touch-based method can handle single as well as multi-touch gestures.

A bi-modal continuous authentication method based on face and speaker recognition was proposed in [66]. Their 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 3 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 which 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) were proposed in [67] to continuously authenticate smartphone users. HMOG is essentially based on the accelerometer, gyroscope, and magnetometer readings and captures subtle hand micro-movements and

orientation patterns generated when a user taps on the screen. A set of 96 HMOG features was proposed and evaluated on a dataset 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 [67]. Table V summarizes the key multimodal fusion methods for continuous authentication in terms of their performances on various datasets. In this table, HTER stands for half total error rate.

In [68] 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 dataset which consists of these three text-based biometric modalities for the same individual, these modalities were combined from different datasets to create a virtual dataset of 30 users. Based on this dataset, they reported an average EER of 3.3% when linguistic profiling, behavioral profiling and keystroke dynamics are fused.

TABLE V: Key multimodal fusion-based continuous authentication methods for mobile devices.

Study	Modalities	# of Users	Fusion Method	Performance (%)
Zhang *et al.* [62]	Face, touch gestures	50	Feature level	RR: 83.75
Fridman *et al.* [63]	Stylometry, Application Usage, Web Browsing, GPS Location	200	Decision level	EER: 5 (1 min), 1 (30 min)
Shi *et al.* [64]	Accelerometer, touch screen, microphone, location history	7	Decision level	EER: -
McCool *et al.* [66]	Face, voice	152	Score level	HTER: 11.9 (male), 13.3 (female)
Sitova *et al.* [67]	HMOG, tap, keystroke	100	Score level	EER: 7.16 (walking), 10.05 (sitting)
Saevanee *et al.* [68]	Linguistic profiling, behavioral profiling & keystroke dynamics	30	Score level	EER: 3.3 (weighting) - 4.4 (sum)

G. Summary of Continuous Authentication Approaches

As discussed above, several physiological and behavioral biometrics-based techniques have direct application 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 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 in order 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, 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 sub-algorithms 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 than unimodal continuous authentication systems.

III. Usability and Security Issues

The usability of transparent continuous authentication systems on mobile devices has become a major issue in research [5], [69], [70]. A balance needs to be made 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, 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 [71] 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 development 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 [69] a prototype was developed using keystroke, voice and face biometrics for continuous authentication. Their prototype was evaluated using 27 participants and they reported that 92% of the participants considered it more secure in comparison to the traditional methods of authentication. Similarly, [70] conducted an in-lab study of security perception of implicit authentication with 30 users based on behavioral biometrics. In their study, they 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. Their study indicated that 91% of participants found implicit authentication to be convenient and 81% perceived the provided level of protection to be satisfactory. Furthermore, they 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.

IV. Discussions and Future Directions

This article presented an overview of recent advances in mobile-based continuous authentication methods which 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, but obviously it cannot cover all the literature on continuous authentication, and we have chosen a representative subset of the latest progress made in biometrics and security community to focus on. 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.

1) The biometric data at enrollment time may have different characteristics than one presented during authentication. For example in the case of face biometric, the enrolled faces are usually frontal and well illuminated. However, during authentication one 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 has different distribution from the data on which the model is applied is often known as domain adaptation [72]. One such method based on faces and touch gestures for continuous authentication using domain adaptation was recently proposed in [73]. 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 as a service and identity assurance as a service because deploying and maintaining these technologies requires specialized expertise and infrastructure. This raises privacy concerns because biometric information is disclosed to a third party. In order to deal with this issue, methods for securely outsourcing continuous authentication systems are needed [74].
3) Some of the behavioral biometrics-based continuous authentication methods discussed in this paper 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 geometry as well as dynamics of touch gestures into a feature extraction algorithm can significantly enhance the performance of a touch gesture-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 [75], [76]. 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 biometric, making use of additional sensors for liveness detection would counter the problem of spoof attacks.
5) 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.
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. In order to prevent the theft of biometric patterns of mobile device users, biometric template protection schemes such as

cancelable biometrics [77] should be incorporated within the continuous authentication framework.

8) Most mobile-based continuous authentication techniques discussed in this paper have been evaluated on small and midsize 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.

AUTHOR BIOGRAPHIES

Vishal M. Patel is an Assistant Professor in the Department of Electrical and Computer Engineering (ECE) at Rutgers University. Prior to joining Rutgers University, he was a member of the research faculty at the University of Maryland Institute for Advanced Computer Studies (UMIACS). His research interests are in signal processing, computer vision and machine learning with applications to radar imaging and biometrics. He was a recipient of the ORAU postdoctoral fellowship in 2010. He is a member of the IEEE, Eta Kappa Nu, Pi Mu Epsilon, and Phi Beta Kappa.

Rama Chellappa is a Professor of Electrical and Computer Engineering (ECE) and an affiliate Professor of Computer Science at the University of Maryland (UMD), College Park. He is also affiliated with the Center for Automation Research, the Institute for Advanced Computer Studies (Permanent Member) and is serving as the Chair of the ECE department. In 2005, he was named a Minta Martin Professor of Engineering. His current research interests are clustering, 3D modeling from video, image and video-based recognition of objects, events and activities, dictionary-based inference, compressive sensing, domain adaptation and hyper spectral processing. He is a Fellow of IEEE, ACM, AAAS, AAAI, OSA and IAPR.

Deepak Chandra heads authentication at the Machine Intelligence and Research group at Google. The project aims at completely redefining authentication for digital and physical world. Prior to this he was the program lead in Googles Advanced Technology and Projects (ATAP) organization, where he heads all product, engineering, and design for mobile authentication projects. Deepak 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 is a Product Manager at Google Research & Machine Intelligence, where he works on privacy-sensitive on-device machine learning. He was previously at Google Advanced Technology

and Projects (ATAP) on the Project Abacus team, where he managed efforts to develop a multimodal continuous authentication system for smartphones. Prior to Google, Brandon co-founded four companies across electronics, fintech, and private equity.

REFERENCES

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

[2] A. Vance. (2010, Jan) If your password is 123456, just make it hackme. [Online; posted JAN. 20, 2010]. [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 *Proceedings of the 4th USENIX Conference on Offensive Technologies*, 2010, pp. 1–7.

[4] D. Tapellini. (2014, May) Smart phone thefts rose to 3.1 million in 2013: Industry solution falls short, while legislative efforts to curb theft continue. [Online; posted May 28, 2014]. [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 *Eleventh Symposium On 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 *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications 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 *Symposium On 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 2013.

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

[10] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," in *Proceedings of the 13th International Conference on Information Security*, 2011, pp. 99–113.

[11] N. L. Clarke, *Transparent User Authentication - Biometrics, RFID and Behavioural Profiling.* 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 *International Conference on Biometrics*, 2015.

[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 Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, Jan 2013.

[14] L. Li, X. Zhao, and G. Xue, "Unobservable reauthentication for smart phones," in *Proceedings of the 20th Network and Distributed System Security Symposium*, 2014.

[15] A. Serwadda, V. Phoha, and Z. Wang, "Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms," in *IEEE International Conference on 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 *IEEE Winter conference on Applications of Computer Vision*, 2015.

[17] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in *IEEE Conference on Technologies for 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 *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, 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 *IEEE International Conference on Biometrics: Theory, Applications and Systems*, Sept 2013, pp. 1–6.

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

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

[22] P. A. Viola and M. J. Jones, "Robust real-time face detection," *International Journal of Computer 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 Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971–987, Jul 2002.

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

[25] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Advances in Neural Information Processing Systems*, p. 2012.

[26] M. E. Fathy, V. M. Patel, and R. Chellappa, "Face-based active authentication on mobile devices," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2015.

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

[28] P. Abeni, M. Baltatu, and R. D'Alessandro, "Nis03-4: Implementing biometrics-based authentication for mobile devices," in *IEEE Global Telecommunications Conference*, 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 *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, 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 Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 10, pp. 1962–1977, Oct 2011.

[31] P. Samangouei, V. M. Patel, and R. Chellappa, "Attribute-based continuous user authentication on mobile devices," in *IEEE International Conference on Biometrics: Theory, Applications and Systems*, 2015.

[32] P. Perera and V. M. Patel, "Active mobile authentication based on soft biometrics," in *IEEE International Conference on Image Processing*, 2016.

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

[34] M. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait

recognition," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Oct 2010, pp. 306–311.

[35] 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 *IEEE International Conference on Biometrics: Theory, Applications and Systems*, Sept 2012, pp. 8–15.

[36] C. Nickel, C. Busch, S. Rangarajan, and M. Mobius, "Using Hidden Markov Models for accelerometer-based biometric gait recognition," in *IEEE International Colloquium on Signal Processing and its Applications*, March 2011, pp. 58–63.

[37] H. M. Thang, V. Q. Viet, N. D. Thuc, and D. Choi, "Gait identification using accelerometer on mobile phone," in *International Conference on Control, Automation and Information Sciences*, Nov 2012, pp. 344–348.

[38] M. Muaaz and R. Mayrhofer, "An analysis of different approaches to gait recognition using cell phone based accelerometers," in *Proceedings of International Conference on Advances in Mobile Computing & Multimedia*, 2013, pp. 293:293–293:300.

[39] Y. Zhong, Y. Deng, and G. Meltzner, "Pace independent mobile gait biometrics," in *IEEE International Conference on Biometrics Theory, Applications and Systems*, Sept 2015, pp. 1–8.

[40] Y. Zhong and Y. Deng, "Sensor orientation invariant mobile gait biometrics," in *IEEE International Joint Conference on Biometrics*, Sept 2014, pp. 1–8.

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

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

[43] J. Hall, M. Barbeau, and E. Kranakis, "Anomaly-based intrusion detection using mobility profiles of public transportation users," in *IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, vol. 2, Aug 2005, pp. 17–24 Vol. 2.

[44] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Behaviour profiling for transparent authentication for mobile devices," in *European Conference on Information Warfare and Security*, 2011, pp. 307–314.

[45] ——, "Active authentication for mobile devices utilising behaviour profiling," *International Journal of Information Security*, vol. 13, no. 3, pp. 229–244, June 2014.

[46] D. Bassu, M. Cochinwala, and A. Jain, "A new mobile biometric based upon usage context," in *IEEE International Conference on Technologies for Homeland Security*, Nov 2013, pp. 441–446.

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

[48] N. A. Safa, R. Safavi-Naini, and S. F. Shahandashti, *ICT Systems Security and Privacy Protection: 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, ch. Privacy-Preserving Implicit Authentication, pp. 471–484.

[49] 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*, vol. abs/1410.7743, 2014.

[50] T. Neal, D. Woodard, and A. Striegel, "Mobile device application, bluetooth, and wi-fi usage data as behavioral biometric traits," in *IEEE International Conference on Biometrics Theory, Applications and Systems*, Sept 2015, pp. 1–6.

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

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

[53] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," *International Journal of Information Security*, vol. 6, no. 1, pp. 1–14, Dec 2006.

[54] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous authentication on mobile devices by analysis of typing motion behavior," in *Proceedings of GI Conference Sicherheit (Sicherheit, Schutz und VerlŁsslichkeit)*, 2014.

[55] 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 *The Fourth International Conference on Advances in Computer-Human Interactions*, 2011, pp. 188–191.

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

[57] H. Saevanee, N. L. Clarke, and S. M. Furnell, "Sms linguistic profiling authentication on mobile devices," in *Proceedings of the 5th International Conference on Network and System Security*, 2011, pp. 224–229.

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

[59] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, "Casa: Context-aware scalable authentication," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 2013, pp. 3:1–3:10.

[60] 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 *Workshop on Mobile Computing Systems and Applications*, 2014, pp. 9:1–9:6.

[61] A. Ross and A. K. Jain, "Multimodal biometrics: an overview," in *European Signal Processing Conference*, 2004, pp. 1221–1224.

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

[63] 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 Systems Journal*, 2015.

[64] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong, "Senguard: Passive user identification on smartphones using multiple sensors," in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2011, pp. 141–148.

[65] 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 *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, ser. SenSys '10. ACM, 2010, pp. 71–84.

[66] 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 *IEEE International Conference on Multimedia and Expo Workshops*, July 2012, pp. 635–640.

[67] Z. Sitova, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: A new biometric modality for continuous authentication of smartphone users," *CoRR*, vol. abs/1501.01199, 2015.

[68] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Text-based active authentication for mobile devices," in *ICT Systems Security and Privacy Protection*, ser. IFIP Advances in Information and Communication Technology, N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, Eds. Springer Berlin Heidelberg, 2014, vol. 428, pp. 99–112.

[69] N. Clarke, S. Karatzouni, and S. Furnell, *Emerging Challenges for Security, Privacy and Trust: 24th IFIP TC 11*

International Information Security Conference, SEC 2009, Pafos, Cyprus, May 18–20, 2009. Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, ch. Flexible and Transparent User Authentication for Mobile Devices, pp. 1–12.

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

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

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

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

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

[75] 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 *IEEE International Conference on Identity, Security and Behavior Analysis*, March 2015, pp. 1–6.

[76] ——, "Face recognition on consumer devices: Reflections on replay attacks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 736–745, April 2015.

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