Journal of Pattern Recognition Research 1 (2016) 74-110

Received November 2, 2016. Revised December 6, 2016. Accepted November 23, 2016.

Surveying Biometric Authentication for Mobile Device Security

Tempestt J. Neal *tempesn@ufl.edu*
Dept. of Computer and Information Science and Engineering, University of Florida
Gainesville, FL 32611, USA

Damon L. Woodard *dwoodard@ufl.edu*
Dept. of Electrical and Computer Engineering, University of Florida
Gainesville, FL 32611, USA

Abstract

Mobile devices, such as smartphones and tablets, are frequently used for creation and transmission of private and sensitive messages and files. While personal identification numbers and passwords have been the standard for mobile device security, users tend to forget complex character combinations or reuse them for multiple accounts. These disadvantages have caused researchers to explore biometric authentication for accurate and convenient mobile device security by taking advantage of refined sensing technologies which capture environmental, positional, and interactive information. This information has been found useful in uniquely modeling physical and behavioral characteristics such that biometric recognition is feasible. In this paper, over 100 biometric approaches to mobile device security are surveyed. The advantages and research challenges associated with ten biometric modalities are provided, along with discussion of various commercial implementations and biometric template protection schemes.

Keywords: Authentication, biometrics, mobile device, passwords, security

1. Introduction

The expansion of storage and computational capabilities on mobile platforms offers the potential to completely revolutionize the technology market. Moreover, expansions in local memory and cloud storage encourages use of mobile devices for file manipulation and transmission, and a recent survey finds such information housed in these devices the most important aspect to consumers [1]. With this comes great responsibility for mobile device manufacturers to revamp and, perhaps, reconsider current security measures. Technical workarounds for device access, such as a recent hack discovered on Android devices, jeopardize distribution of private and/or sensitive information [2]. Moreover, according to a leading cybersecurity company, 10% of smartphone owners are phone theft victims, with consequences ranging from productivity and corporate data loss to fraudulent charges. Even worse, 9% of phone theft victims have suffered from identity theft [3]. Initiatives, such as Secure Our Smartphones, are strong indicators that mobile device theft is a quickly growing issue [4, 5].

Mobile devices currently employ methods based on *user knowledge*, such as personal identification numbers (PINs) and alphanumeric passwords. However, the simplicity and lack of use (it is shown that approximately half of mobile device users use PINs [3, 6–9]) associated with such methods coupled with authentication restricted to the point-of-entry may lead to great security breaches [10]. Of over 200,000 four-digit numeric passwords, it was found that 10 of these made up 15% of the collection, while the top two included patterns as simple as '1234' and '0000' [11]. Similar studies suggest identical trends, mainly due to the undesired burden of remembering complex combinations of characters [12]. In fact, a survey conducted in 2008 found that 55.7% of its participants had at some point forgotten their PIN [13]. How, then, should manufacturers incorporate security measures that simultaneously offer convenience and flexibility? One option is a token-based method which would establish an identity based on some object, such as an identification card. Though an approach is presented which embeds fingerprint recognition into the device's charger such that the charger serves as a token, there lacks empirical evidence to support such techniques without limiting the key advantage of mobility [14]. Hence, biometric researchers have attempted to address these concerns via consideration of *physiological* and *behavioral* authentication solely on the device.

Physiological biometric authentication uses the distinctiveness of physical characteristics, such as fingerprint and iris patterns, for access control. Apple and Google (Android) have implemented biometric authentication via fingerprint and face recognition, respectively, in recent years. Currently, fingerprint recognition technology relies on cutting-edge hardware to capture fine details of fingerprint patterns. Because no two patterns are alike, the service relies on this uniqueness to accurately match a new fingerprint scan with an existing one [15]. On the other hand, face recognition relies on measurements of facial features, such as shape and position, to create a unique face representation [16]. A 2010 study found that 95% and 64% of subjects felt fingerprint and face recognition, respectively, to be secure. While 95% of the subjects also felt that they would use fingerprint recognition, only 27% reported to likely use face recognition, reflecting an obvious disconnect between perceived security and usability [17]. Furthermore, physiological systems may result in the need for refined sensors for data capture, such as in the proposed electrocardiogram based system [18, 19], and may fail when presented with an engineered characteristic, such as a fingerprint mold.

On the other hand, behavioral biometrics measure the consistency and distinctiveness of behavioral tendencies. In the context of mobile devices, such tendencies could include application use [20], calling habits [6], and keystroke statistics [21]. Hence, while knowledge-based methods require users to remember and re-enter passwords as needed, behavioral biometrics have no memory load and can continuously monitor device usage for active and transparent authentication. Further, compared to both knowledge-based methods and physiological biometrics, behavioral biometrics rely on data captured as the user naturally interacts with the device. As a result, behavioral biometrics provide cost-effective and intuitive access control, and have appropriately been referred to as "transparent, continuous, implicit, active, passive, non-intrusive, non-observable, adaptive, unobtrusive, and progressive" [22].

This survey aims to provide thorough insight into mobile device security via biometrics. The overall intent is to provide fundamental knowledge of several modalities, while offering experimental evidence from various implementations which support the applicability of biometric solutions on mobile device platforms. Unlike previous surveys [23–26], this survey includes discussion of ten biometric modalities and multimodal approaches and is the first to include periocular recognition. This survey also details various motion-based implementations beyond gait recognition and includes discussion on template security. Finally, this paper reviews the most recent publications while providing details on commercially available implementations. As a result, this survey is arguably the most up-to-date and comprehensive.

The paper is outlined as follows: Section 2 motivates the use of biometric recognition via discussion of the flaws found in point-of-entry techniques. Section 3 provides fundamental definitions regarding biometric authentication. Sections 4 and 5 survey various physiological and behavioral biometric implementations on mobile devices, respectively. Section 6 provides information on various multimodal schemes. Section 7 discusses several security concerns regarding inappropriate access to the device and biometric templates. Finally, Section 8 describes the various research challenges associated with biometric recognition on mobile devices, followed by conclusions in Section 9.

2. Motivation

Manufacturers have employed knowledge-based methods as the core security scheme on mobile platforms. As implicated by the name, knowledge-based methods rely on the knowledge of the consumer; the consumer must know a certain (alpha)numeric password, PIN, graphical sequence (typically based on connecting a subset of nine nodes in a 2D grid), or more recently, picture gesture [27] for device access. While these methods are generally accepted due to ease of implementation, design simplicity, and user familiarity, knowledge-based methods suffer from memory load, shoulder surfing and smudge attacks [1], password reuse, and user inconvenience from frequent re-entering [28–31]. Knowledge-based methods also assume an equivalent security level across all applications [32]. For instance, while accessing bank records is a more private action compared to creating a new contact, a password-based method can only provide the same level of security for both actions. Further, it is suggested that biometric authentication can allow for adaptable authentication via sensing of environmental factors and adjusting accordingly for use of the most suitable trait (i.e., fingerprint recognition is used instead of face recognition when poor lighting is detected [33]). Thus, knowledge-based methods fail to offer application-specific and adaptable security [34].

Researchers have attempted to address some of these issues by proposing more complicated security schemes that are mostly variations of existing implementations. For instance, Yu *et al.* [35] propose 3D graphical passwords for mobile devices. The authors claim that 3D passwords are easier to remember and have a larger password space. Hence, sequences of touched cubes in a 3D virtual space are recorded, which are later translated into a unique password. The user is only responsible for remembering his or her sequence. Unfortunately, the authors provide very little experimental support for this technique. Furthermore, a commercial hand tracking device is employed for capturing the user's activity in the virtual space, which may not be commercially available to the average consumer. The authors also neglect to analyze the usability of this approach. While Amin *et al.* [30] claim that graphical sequences are easier to remember than typical passwords, a recent study revealed that 2D patterns are possibly as equally predictable as textual passwords, as 40% of patterns start in the top-left corner and most users only use five of the nine nodes [36].

Shin *et al.* [37] propose an alternative lock scheme similar to graphical passwords. Six circles are presented, where the user can touch each circle up to seven times. Each touch changes a circle's color. Once each circle is the appropriate color, the phone will unlock. This work decreases the chances that an intruder can easily guess the correct circle color combination, given that more password combinations are possible. The number of password combinations can be increased further by allowing more circles on the screen or allowing more colors. However, this requires the user to remember complex combinations, which is a core flaw in knowledge-based methods.

To combat the need to remember complicated codes, a Rutgers University study investigates free-form gestures, or doodling, as a security scheme [38, 39]. Users have the liberty

[1] Shoulder surfing is the direct observation of a password as it is being entered, while smudge attacks are the inferring of passwords based on finger residue left on the screen.

to draw any shape with any number of fingers. The study indicated that utilizing free-form gestures reduced log-in time by 22% compared to passwords and claims that doodling is easier to remember and harder to hack. However, it is unclear how this approach can reduce shoulder surfing and smudge attacks.

Each of these solutions carry at least one fundamental problem of knowledge-based security, such that coupling these methods with biometric solutions offers improvements in accuracy and usability. For example, two similar implementations display many images to the user, where he or she is instructed to either draw a line connecting the images or select an image, during which touch gesture and keystroke dynamic measurements are collected [21, 40]. These implementations support the need for and advantages of stronger security measures on mobile devices via biometric authentication.

3. Biometric Authentication

Biometric authentication is defined as the use of physical and/or behavioral traits for human identification or verification via application of pattern recognition and machine learning techniques. Verification is the main mode considered in mobile device security as it is the responsibility of the biometric system to verify that the person using the device is the rightful owner. Verification implies a one-to-one match, where an individual's captured trait is compared to his or her supposed template. The individual claims an identity, and it is the responsibility of the system to verify if the claimed identity is correct based on a given threshold. This scenario is represented mathematically in Eq. 1, where S measures the similarity between input characteristic X and template Y, t is an established threshold value, and C can take on values c_1 (genuine match) or c_2 (impostor match).

$$C = \begin{cases} c_1 & \text{if } S(X,Y) \geq t \\ c_2 & \text{if } S(X,Y) < t \end{cases} \tag{1}$$

Figure 1 depicts the verification process and the separate modules of the biometric system. Biometric traits are detected and captured for feature extraction, in which important attributes, or features, are stored as a biometric template in a database. This phase is typically referred to as enrollment. On subsequent visits to the system, the template is retrieved, and the individual re-presents his or her trait for feature extraction. These features are compared to the template to obtain a matching score, which indicates if the subject can access the respective system. Therefore, these separate components have been termed sensing, feature extraction, matching, and database modules.

Mobile device sensors, such as accelerometers and gyroscopes, play a key role in the sensing phase of the biometric system. Understanding sensor operation and proper resource management when using these sensors is key to efficient utilization of the information they provide [41]. As this survey will show, this information has proven valuable in enhancing mobile device security as researchers continue to exploit these measurements for exploration of "on-the-move biometry" [42].

Analysis of biometric systems is key in determining its success and ability to generalize to different populations. This is very important for mobile devices, as the chosen feature representation and matching algorithms should accommodate a very large and diverse population. Thus, several metrics are available for assessing system performance, i.e., how often a biometric system succeeds and fails. Two popular metrics include false accept and false reject rates (FAR and FRR, respectively.) In the case of mobile device security, a false accept occurs when an intruder is allowed access to the device and a false reject occurs

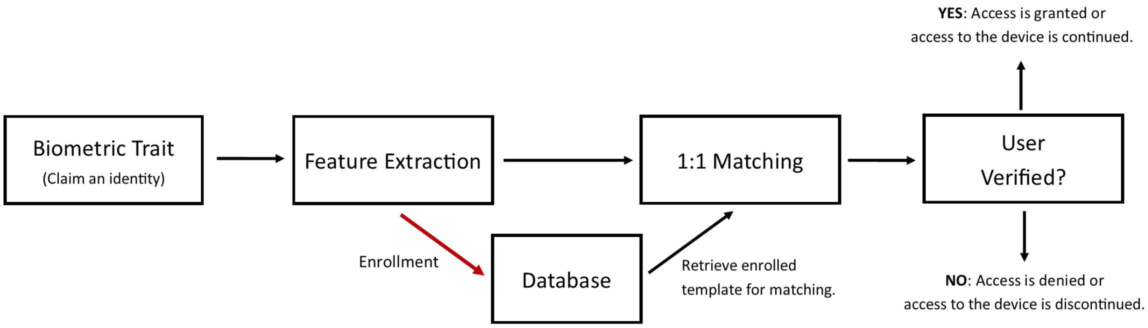
YES: Access is granted or access to the device is continued.
Biometric Trait
(Claim an identity)
Feature Extraction
1:1 Matching
User Verified?
Enrollment
Database
Retrieve enrolled template for matching.
NO: Access is denied or access to the device is discontinued.

Fig. 1: Biometric authentication for mobile devices operating in verification mode.

when the true owner of the device is denied access. Additional metrics include equal error rate (EER), true positives and negatives, false positives and negatives, accuracy, precision, and recall. The EER is the point at which the FAR is approximately equal to the FRR, and it is one of the most commonly used metrics for analyzing system error. True positives and negatives occur when the true owner and impostor are identified as such. False positives and negatives occur when the true owner and impostor are classified as an intruder and owner, respectively. Accuracy is the ratio of true positives and negatives to true positives, true negatives, false positives, and false negatives. Precision measures how often the system gets positive classifications correct as the ratio of true positives to true and false positives. Recall measures how often the system correctly classifies positive samples when it encounters them as the ratio of true positives to true positives and false negatives.

4. Physiological Biometrics

The growing need to identify individuals with unquestionable precision has allowed biometric recognition to penetrate several areas of human life. Fingerprint recognition is likely the most used biometric due to its reliability, cost-effective implementation, and high user acceptance. A prime example is the use of fingerprints in law enforcement for the identification of criminals. Biometric technology is also useful in health care, and has been projected to significantly simplify several administrative procedures. For instance, it is suspected that nurses will soon be able to use biometric recognition to access digital records, and patients will be allowed to use biometric traits to authenticate themselves instead of wearing wristbands. This is expected to significantly reduce medication and billing errors and assist when patients are physically unable to provide identifying information [43].

Additional applications include fingerprint recognition for monitoring student activity in schools [44], fingerprint, hand geometry, and iris recognition for tracking inmates in correctional facilities [45,46], Malaysia's MyKad fingerprint-based governmental smart card system [47], and well-known Touch ID on Apple's mobile devices [48]. However, all of these applications require knowledge of the service by the user. The user must actively interact with the biometric scanner and is aware that his or her trait is being captured. This is termed *overt recognition.*

Overt recognition is a key characteristic of physiological biometry. Thus, in regards to physiological biometrics, emphasis is placed on the intrusive nature of the authentication process. 'Intrusiveness' in this context represents the disruptive and/or invasive aspects of the authentication procedure. Because use of physiological traits on mobile platforms is an overt process, there is an unavoidable requirement for the user to present his or her biometric, yielding the disruptive aspect. Further, these systems are similar to knowledge-based methods in that they authenticate at the point-of-entry. However, physiological biometrics reduce the need to remember complex passwords or pictorial representations of lock patterns. As a result, several modalities have been considered for securing mobile devices, including face, periocular, fingerprint, and iris.

4.1 Face

Face recognition applications range from controlled (e.g., mug-shots) to dynamic settings (e.g., airport) [49]. Face recognition has been applied to surveillance security, border control, forensics, etc. [50, 51]. While face recognition is highly studied, its usability and acceptance on mobile platforms has been questionable. A recent survey analyzed the opinions of individuals that use, have used, or have never used face unlocking services on capable devices [52]. It was found that 36% of participants considered the service annoying, slow, inconvenient, and difficult to use. Further, it was felt that capturing facial images for authentication is a socially awkward procedure. Moreover, the group of participants that had never used the service were unaware that it existed on the device, suggesting a lack of manufacturer marketing efforts, while the group that had previously used the service discontinued its use due to usability frustration. Overall, the survey suggested likability with fingerprint recognition due to convenience and positive emotional feedback, such as describing its functionality as 'fun' and 'awesome'. Nonetheless, face recognition is a promising security option for mobile devices.

Face recognition involves the following steps [53]:

1. Detection: Face detection captures and scales the face.
2. Normalization: The image is geometrically normalized to a fixed resolution, followed by enhancements to reduce the effects of illumination and rotation.
3. Feature Extraction: Two main approaches are generally used to extract the most discriminative information from the image: (1) location, shape, and spatial relations of facial attributions, such as the nose and mouth, are extracted, or (2) a global representation via the weighted combination of several faces serves as a model [54].
4. Matching: Various machine learning and pattern recognition algorithms are used to match gallery and probe feature vectors for authentication.

A number of facial recognition databases are publically available [55–57], which have allowed a sufficient amount of experimentation on constrained and unconstrained cases. However, state-of-the-art performance is restricted to frontal images with limited influences from pose, illumination, expression, and occlusions. While an ideal face recognition system should reliably capture the face and allow accurate classification regardless of these factors, robustness under uncontrolled conditions remains the fundamental research challenge of facial recognition. However, it has been shown that motion-based sensors, i.e., accelerometers and gyroscopes, assist in decreasing noise introduced by rotation, particularly on mobile devices [58]. Accelerometer and gyroscope measurements indicate the device's orientation; when devices are held at inconsistent angles, these sensors prove very beneficial in assisting in the normalization phase.

Fathy *et al.* attempt to derive a benchmark dataset which captures various elements of noise and other challenges found in real-world mobile device images, such as varying distances from the device's camera, vibrations and blurring from holding the device, partial capturing of the face, and illumination and background variations [59]. The authors employ the well-known and open-source Viola-Jones face detector which scans a frontal face image with a set of Haar-like filters of various window sizes to form reference shapes around the eyes, nose, and mouth [60]. Various classification methods are explored; however, results suggest that current algorithms have yet to cope with the challenges presented in facial recognition on mobile devices.

The effects of noise, specifically illumination, are further evaluated in a work by Riesch *et al.* [61]. The authors acknowledge the challenges of facial recognition due to unconstrained data capture coupled with the constraints of processing resources, such as power efficiency, hardware capabilities, network limitations (i.e., authentication should be performed solely on the device instead of on back-end servers), and end-user acceptability. As a result, the authors attempt to capture Local Binary Patterns as texture descriptors of facial images captured in various lighting conditions. Support vector machines (SVMs) are trained for nine subjects under each condition to allow recognition in various environments. The authors report a 91.3% control accuracy and a 100% accuracy in other environments, providing a strong notion that while face recognition on mobile devices may be hindered in several scenarios, it is particularly robust in regards to illumination.

Despite the challenges associated with face recognition, Tao and Veldhuis [62] argue that face recognition addresses three core issues regarding security implementations on mobile devices: runtime advanced security, convenience, and reduced complexity as indicated by low error rates, transparency at run-time, and storage and authentication primarily on the device with low computational requirements. The authors employ the Viola-Jones detector to form a reference shape indicated by 13 facial landmarks. A feature space is subsequently obtained from construction of a subspace via Eigenfaces, which is further reduced to two features, DIFS (distance in feature space) and DFFS (distance from feature space) using the Singular Value Decomposition. The experimental setup included a collection of 8,000 320x240 images from six subjects combined with a probability-based Parzen classifier to deliver an EER of 1.2%.

Research Challenges

Face recognition on mobile devices introduces new challenges beyond those traditionally found in non-mobile face recognition systems. An attractive aspect of face recognition on mobile devices is the fact that most users capture photos of themselves while being close to the device. As a result, photographs are typically head shots with direct eye contact. On the contrary, the liberty to take a photo whenever and wherever introduces significant variations between similar photographs, including image blur, angles and/or rotations, varying amounts of background and illumination, and partial images [59]. While these are all issues prevalent in most facial recognition applications, mobile devices further complicate this task due to the inability to expect consistent and/or cooperative behavior. Further, while it is likely that users will be instructed on how to present his or her face during data enrollment, it is very unlikely that this controlled presentation will be reciprocated in the future for authentication as users will expect a fast and casual authentication experience. Moreover, in static face recognition systems, the face is typically captured by the same camera of high caliber for all individuals. On mobile devices, however, the hardware can vary depending on the device. This is especially true for front cameras, which are usually lower in quality compared to the rear. As a result, a universal protocol across all devices may not be a suitable or realistic solution.

4.2 Periocular

The periocular area of the face is the surrounding regions of the eyes. Given the availability of high-definition cameras on mobile devices, the periocular region can be reliably extracted from facial images. Periocular recognition is particularly useful when the face is occluded, while the area around the eyes remains available for feature extraction, and a general consensus among researchers is that the periocular region is better suited for biometric authentication compared to other regions of the face [63]. Periocular features can be extracted at two levels:

1. Level 1 features are general and holistic, and include attributes regarding eye folds, eyelids, moles, and wrinkles.
2. Level 2 features are more detailed, including characteristics such as texture and hair follicles [64].

Raja *et al.* implement periocular recognition on mobile devices using Scale Invariant Feature Transform (SIFT), Speeded Up Robust Features (SURF) and Binarized Statistical Image Features (BSIF) for representation of periocular keypoints [65]. SIFT features are robust against scaling and rotation factors, while SURF features are robust against scaling, rotation, illumination, and variations in contrast [66]. The proposed method allows data capture via front and back cameras, with an audio signal indicating when the image is captured successfully. The matching phase employs the Fast Library for Approximate Nearest Neighbors algorithm and Bhattacharya distance measure on 32 subjects to achieve genuine match rates ranging from 80% to 95.31% using BSIF features. The authors note, however, that performance is maximized using the rear camera; currently, rear cameras offer higher resolution, such that the results suggest a correlation between camera resolution and performance.

The authors continue with periocular recognition via investigation of cross-smartphone performance and introduction of a new feature extraction technique [67]. Cross-smartphone authentication involves matching between two data samples acquired from different devices. This inherently introduces variations in data quality between the two samples, which often results in performance degradation. To handle such variations, the authors employ feature extraction via sparse, decomposed Laplacian pyramids for image enhancement in spatial and frequency domains. Results indicate that the proposed feature extraction method outperforms BSIF features, achieving 8.33% to 31.02% EERs.

Research Challenges

The periocular area of the face provides an attractive option for biometric recognition. It is easy to capture and contains texture, color, and shape information, all of which are reliable biometric features. However, on mobile devices, the periocular region is problematic for several reasons. First, periocular recognition suffers from the same problems encountered in face recognition. Beyond this, however, is the fact that occlusions which hinder accuracy in face recognition are likely found in the periocular region, such as eye glasses, hair, and hats. Because the user has sole control over the sensor, these occlusions and unpredictable angles and distances from the camera hinder segmentation of the periocular region. Hence, periocular recognition on mobile devices is highly dependent on the user's ability to present a relatively controlled image. Facial recognition could potentially simplify this process if the algorithm considers several regions of the face as separate components, and can reliably authenticate based on a few regions (for instance, the nose and mouth when eye glasses are worn). Periocular recognition, however, leaves very little room for such flexibility, and as a result, an implementation may require inconvenient and unnatural restrictions for adequate use of the service.

4.3 Fingerprint

Fingerprints are composed of ridges and valleys found in the skin on the finger tips, where hair and oil glands are not present. Fingerprint features are typically described at three levels:

1. Level 1 fingerprint features consist of a ridge orientation map that defines the texture pattern of the finger. Level 1 features identify locations where ridge orientations change, termed loops and deltas. These features are very coarse, and the flow of ridge patterns is visible to the eye under normal circumstances.
2. Level 2 features describe the minutiae of the fingerprint, or areas of the ridges that merge, split, begin, and end. Level 2 features appear as an outline, or a single pixel representation, of Level 1 features.
3. Level 3 features are the most detailed, and represent sweat pores and edges of ridges. Capture of Level 3 features requires advanced imaging technology; as a result, these features are typically only used when minutiae are not available, such as in latent, or partial, fingerprints.

Level 2 fingerprint features are usually extracted for fingerprint recognition due to the compact representation, robustness against degradation, and discriminating capabilities of minutiae. Hence, matching typically involves minutiae detection and extraction from the probe image, alignment for coordinate system normalization between the template and probe, establishing correspondence of minutiae pairs, and score generation [60]. Minutiae detection on mobile devices, however, is a non-trivial task due to the smaller touch sensors. The sensor size results in the need for several enrollment images to detect a sufficient number of minutiae points. This increases user effort, which decreases a core advantage of biometric approaches – convenience. Yamazaki *et al.* [68] addresses this problem via proposal of merging images using the SIFT algorithm during enrollment due to its robustness against rotation, scale, and illumination. SIFT features are extracted by identifying local extrema as candidate keypoints via convolution with a Gaussian filter, filtering of ideal keypoints by excluding those with low contrast and poor localization, and assigning the orientation of the gradient to each keypoint. SIFT keypoints cover a wider area than minutiae, thereby reducing the number of images required to represent the fingerprint region.

Fingerprint recognition has widely established itself as a prominent biometric technology on modern mobile devices for authentication and e-commerce transactions. Apple boasts its fingerprint technology as a "seamless" biometric password, incorporating advanced hardware and software that aids in fingerprint detection, capture, and privacy. The service also self-improves, as each recognition attempt increases the quality of the enrolled template. Furthermore, the manufacturer states that there is only a 1 in 50,000 chance of misclassifying different fingerprints, while the chances of guessing a 4-digit password are 1 in 10,000. Moreover, privacy concerns are addressed by only storing a mathematical representation of the fingerprint instead of the image itself [15]. Due to these advantages, it is no surprise that 90% of current users feel that fingerprint recognition is more convenient than PINs [69].

Research Challenges

Fingerprint recognition is affected by skin and sensor conditions. For instance, authentication is problematic when fingers are wet or the surface of the device is dirty [69]. Other factors, such as scars and workplace injuries, could complicate data capture and matching [60].

Such skin conditions also increase the need for preprocessing, which could add to resource overhead on mobile platforms. For instance, Yamazaki recommends highpass filtering, lowpass filtering, ridge direction detection, and ridge enhancement for preprocessing images for brightness normalization and noise reduction [68]. Finally, as currently implemented commercially, after five failed attempts, a user can access the device via a password [15], thereby subjecting the user to the same disadvantages of a typical knowledge-based system and opening the door for circumvention and adversarial attacks.

Palmprint Recognition

Related to fingerprint recognition is palmprint recognition. There is limited research in regards to palmprint recognition on mobile devices; however, while palmprint recognition traditionally required large and expensive palm scanners, advanced imaging from modern smartphones are likely capable of capturing sufficient palmprints for authentication [24]. Unfortunately, according to [70], research regarding palmprint recognition on smartphones is limited because of no public, standard dataset. Finally, due to the lack of constraints in image capture on mobile devices, palmprint applications would have to cope with illumination and rotation variations which are usually addressed in controlled environments through uniform color backgrounds and finger pegs [71, 72]. However, Javidnia *et al.* consider eliminating illumination variations via a local normalization algorithm prior to feature extraction on mobile platforms [70]. Gaussian smoothing filters are suggested to produce uniform neighborhoods in terms of mean and variance, which improves illumination variations and shading artifacts. Preliminary results suggest that the matching score threshold for preprocessed images via the proposed technique should provide a much smaller false acceptance rate in comparison to images that are not processed.

4.4 Iris

The iris region of the eye arguably provides the most accurate biometric trait [73]. The frontal portion of the iris contains visible muscle which can be captured and used for biometric authentication. The muscles consist of texture patterns which are highly unique and stable over time. Traditional iris recognition systems typically require subjects to present the eye area in a very controlled manner. Several near-infrared images are taken from which a high-quality image is retained [60].

Jeong *et al.* presents an implementation specifically for mobile devices which employs adaptive Gabor filtering for deriving iris features with the intentions of reducing the processing power needed for authentication [73]. After iris detection, blurring and sunlight exposure are measured and compensated for via altering the parameters (i.e., kernel, frequency, and amplitude) of the Gabor filter. Moreover, instead of using the typical normalization technique based on Daugmans rubber sheet model, the authors extract the iris code directly from the pixel coordinates. Subsequently, matching is performed using the Hamming distance. Using a database of 80 subjects, the authors report an EER of 0.14%.

Though premature in regards to mobile device application, commercial vendors are beginning to explore the reality of iris recognition on popular smartphones. Given the inclusion of an infrared light source on the front of the device, Samsung has recently included iris recognition as an authentication method. The company's president boasts introduction of the biometric service as “new experiences we can create with the phone” [74]. Such advances open opportunities for exploration of additional biometric modalities which rely on near-infrared light, such as the use of vein structures found within the finger [75].

Research Challenges

There are several challenges associated with iris recognition in general, but these challenges are further complicated on mobile devices. First, the iris is a moving organ inside of another moving organ (the eye) [60]. Combining this motion with the inevitable movement of the device during data capture creates an immense stabilization problem. Second, iris recognition systems are usually developed for optimal operation indoors [76]. However, mobile devices are used in a variety of environmental conditions. Localization and segmentation of the iris region in non-ideal lighting conditions is an open research problem. According to Cho *et al.*, generalizing the usual method for iris localization (i.e., circular edge detection) to mobile platforms is inefficient due to the constant dilation and constriction of the pupil as light conditions change, ghost regions around the iris, and homogeneous gray levels across several components of the eye [76, 77]. These conditions are all observed when the eye is captured outdoors. Further, near-infrared illumination of the eye is preferred to preserve the iris texture, particularly for dark-colored irides [60]. This imposes hardware and usability issues for mobile device users; the device must be equipped with a near-infrared sensor, the user must be cautious of the distance between the eye and the sensor to avoid any eye damage, and the user must actively cooperate with the system for adequate data capture. Finally, the iris region is described as a "stochastic texture containing numerous edge like features that are randomly distributed" [60]. This implies the need for sophisticated modeling algorithms which have the potential to overwhelm the device's resources. Traditionally, iris recognition involves several steps beyond localization and segmentation, including normalization, encoding, and quality assessment, all of which are expensive mathematical processes.

5. Behavioral Biometrics

According to Clarke and Furnell, an efficient mobile device authentication system should improve security beyond point-of-entry methods, reduce authentication attempts via transparent authentication, provide continuous authentication throughout the entire session of use, and maintain functionality across all mobile platforms regardless of hardware, software, and networking differences [78]. Though physiological biometrics are capable of accomplishing the first task, they fail to provide transparent and continuous authentication and are largely hardware-dependent. Thus, behavioral biometrics are more suitable, as they meet all of the said goals without the need for specific hardware requirements. Moreover, behavioral biometrics allow protection during "user abandonment" [79], or the time in which the owner of the device is not present while the device remains unlocked. Compared to knowledge-based methods, behavioral biometrics decrease the need for the legitimate owner of the device to authenticate by 67% [80], indicating a significant increase in usability. It is also shown that an intruder can complete over 1,000 tasks once access to the device is obtained with only a single knowledge-based authentication attempt; however, multimodal behavioral biometrics reduced this to only the completion of one successful task after over 6,000 attempts. Such advantages are likely the influential factors that resulted in 90% of a survey's participants in favor of transparent authentication [31]. Hence, several behavioral modalities, such as motion, gait, touch gestures, voice, and profiling, have been extensively analyzed for mobile device security.

5.1 Motion

Mobile devices allow motion detection via embedded accelerometers and gyroscopes. The accelerometer measures acceleration is three orthogonal spatial dimensions, x, y, and z, where each axis represents either the vertical, forward-to-backward, or left-to-right components [81]. The gyroscope measures the rotation about each of these axes [82]. The combination of these measurements provide a feature space capable of modeling user movement. Hence, various techniques have been proposed to take advantage of such information.

Such an implementation includes an air-written signature [83, 84]. Signatures (using pen and paper) are a known behavioral biometric used for various government and commercial applications [49, 85, 86]. While the subject is holding the device, he or she motions a signature in the air while accelerometer measurements are recorded. The service requires the user to run an application for data capture, such that it is not covert nor transparent. Further, matching is performed on a server, which poses a security threat if the communication channel is intercepted. However, the algorithm is tested on ten volunteers achieving a promising 1.46% FAR and 6.87% FRR. Nonetheless, while seemingly accurate and robust against shoulder surfing [87], this technique shares several characteristics with knowledge-based methods: (1) the user must actively engage with the authentication service, (2) continuous authentication is not feasible, and (3) the user must know and correctly present a password, which in this case, is the signature. Due to these similarities, the user may be inclined to choose simple signatures for the same reasons of choosing simple passwords or PINs. Similar efforts, such as evaluation of waving gestures [88], free-form gestures [82], and 'picking-up' motion (i.e., retrieving the phone from a pocket or table, raising the arm, and placing the phone near the ear) [89] are also proposed.

Research Challenges

An unfortunate characteristic of motion-based methods is the need to initiate data collection. For instance, the implementation which analyzes picking-up motion requires activation and deactivation of data collection via button presses in a custom application [89]. While it is shown that the curvature of this movement has distinctive qualities given the influences of arm length, upper body shape, and muscles near the wrist, as evident by 12% to 16% EERs, the non-intrusive advantage of behavioral biometrics is unavailable.

5.2 Gait

Gait recognition is the identification of an individual via how he or she walks based on machine vision techniques, floor sensors, or wearable sensors [90]. Machine vision approaches use a segmented portion of images captured while a subject is walking [91]. Floor sensor approaches place sensors in the floor such that gait-related metrics are captured as the subject walks on them [92, 93]. Wearable sensor approaches, which is the approach investigated in mobile devices, are applicable when the subject has the sensing technology somewhere on his or her person [94]. Gait recognition has been found useful as a motion-based, transparent authentication approach through evaluation of accelerometer measurements.

There are four main phases in gait recognition. These include data acquisition, data preprocessing, walk detection, and analysis [81]. Data acquisition involves placement of the device such that walking activity can be recorded. Past efforts have placed the device inside of a holster/pouch [95], in the pants pocket [81, 96], or have had the subjects carry the device in hand [97]. Data collection typically includes 50 subjects or less [95–97], while data is usually collected in controlled conditions; as a result, most studies have little influence from outside factors, such as the effect of different shoes [98]. Only a few studies have attempted real-world data collection in at least one area of data acquisition (i.e., realistic walking patterns, but ideal flooring) [98]. Once the data is acquired, it is preprocessed to reduce the noise introduced by various environmental factors, such as gravitational force, the individual's shoes, or the condition of the floor on which the subject is walking. Moreover, there seems to be a consensus that accelerometer sensors are quite irregular and highly sensitive, which introduces further noise [96]. As a result, linear interpolation is typically used to create equal intervals between samples, followed by filtering to reduce additional noise due to misplacement of the device, screen taps, or automatic vibrations. Environmental noise further complicates the next task of walk detection; to alleviate this problem, activity recognition has been suggested to eliminate any non-relevant data [95].

With normalized data, walks can be detected via cycle or machine learning approaches. Cycles are defined as the time between two steps identified by local maximums or minimums in the three axes. Once an average cycle length is established, cycles are found throughout the data by starting from the middle of the data stream and progressively moving forward (and backward, subsequently) in distances of the average cycle length with some small correction factor. While cycle-based methods are most often used for walk detection, machine learning techniques have been found useful for automatic detection of walking activity [98]. Machine learning techniques work in two steps; first, all data except the very beginning and end are extracted (these excluded values correlate with device manipulation for data collection). Second, a filter is applied to enhance the differences between high and low acceleration values. Walks are then extracted based on some threshold value. Finally, an analysis of the walking signals is required for feature extraction and matching.

Analysis can occur in both time and frequency domains. Time domain features include various cycle statistics, such as average maximum and minimum acceleration and average cycle length and frequency. Further, acceleration moments may be used as features to describe cycle variance and stability [81, 90]. Using such features, the cyclic rotation metric is computed for matching cycle patterns. In the frequency domain, the data is operated on using the Discrete, Discrete Cosine, or Fast Fourier Transforms. The first few output coefficients from each conversion are the most useful in distinguishing between two gait patterns, such that these coefficients serve as biometric features [81].

Research Challenges

Gait recognition is not robust against various aforementioned environmental factors. Further, it is only useful as an authentication method when the user is walking. Once the user is still, an alternative security method is required. Hence, gait recognition is most useful in a multimodal scheme to avoid performance degradation due to various outside factors, and to avoid the lack of authentication when accelerometer data is unavailable. Further, it is interesting to consider how often an average mobile device user will access high-security applications while walking. Intuition suggests that, while possible, it may be more likely that an individual would prefer to access more sensitive data while sitting or standing still to ensure privacy and enhance concentration on the task at hand. Thus, it would interesting to evaluate any experimental correlation between application sensitivity and gait activity.

5.3 Keystroke Dynamics

Keystroke dynamics are a cost-effective solution to biometric authentication on mobile devices [99]. Additional hardware is not required, given that a user must operate the device via key input, continuous authentication is feasible, and typing behavior is unique. Recognition via keystroke dynamics involves the analysis of keystrokes and typing patterns [100]. Common features include:

- *Key press/down*, or the time of a key press event.
- *Key release/up*, or the time of a key release event.
- *Latency*, or the time from press-to-press, release-to-release, or release-to-press events.

- *Hold time*, or the duration of a key press event (i.e., how long the key was pressed).
- *Pressure*, or the measurement of the finger's pressure on the screen.
- *Size*, or the area of the screen pressed by the finger.
- *Error rate*, or the number of times the user presses a backspace or delete key due to erroneous input.

Analysis of keystroke dynamics has traditional application on computers with similar features [101]. However, it is found that authentication on computers is easier as the feature space is less complex. Nonetheless, Joyce and Gupta assert that the physiology of the neurological system responsible for the uniqueness in written signatures are the same factors which establish typing consistencies [102]. Moreover, inclusion of motion detection sensors have shown to improve keystroke authentication; this additional information is unavailable on desktop computers [103, 104]. Mobile devices offer a unique platform for evaluation of keystroke dynamics, given that input mechanisms can vary from the dated 4x3 multiplexed 3D keys to 3D QWERTY keyboards to resistive or capacitive touchscreens [105]. It is unclear, however, how current methods generalize to all of these input forms; this remains as an open research area in keystroke dynamics on mobile devices. Nonetheless, several methods have been proposed.

For instance, McLoughlin and Naidu propose use of key press and release, duration to next key press, and the mean and variance of key timing distances as keystroke features, arguing that the latter two account for the statistical similarities and differences in keystroke behavior [105]. Weights are also employed to reduce the effect of inconsistent keystrokes; values with lower variance are assigned higher weights. Verification is performed at down, up, and all timings to deliver a reported accuracy that exceeded 90%. Hence, the authors argue that keystroke dynamics is an efficient biometric with low computational overhead and user impact.

Similarly, Zahid *et al.* analyze keystroke behavior from 25 phone users [106]. The authors extract hold time, error rate, and digraph measurements, where a digraph is the time between releasing and pressing keys. An identification system composed of three modes, learning, impostor detection, and verification, is presented. The learning mode trains a fuzzy classifier, impostor detection classifies real-time keystroke measurements, and verification is invoked if the user is identified as a potential impostor, where the user is then required to enter an eight-character PIN code. It is argued that a fuzzy classifier is better suited for classification of keystroke behavior, given that a data point is assigned a degree of membership to all classes which accounts for the diffused nature of the features. Furthermore, Particle Swarm Optimization and Genetic Algorithms are employed for improving solution optimization. The authors report 0% and 2% FRR and FAR, respectively, suggesting user-friendliness and high security potential. Moreover, this work suggests that considering classification of keystroke behavior as an optimization task is a more robust approach compared to a distance-based approach [107].

As suspected, however, keystroke dynamics are somewhat inconclusive and have been joined with stronger modalities for improvement in accuracy. For instance, Hwang *et al.* recommend incorporating rhythm and tempo into keystroke dynamics [108]. As a result, a user must follow a specific timing pattern and demonstrate consistency in keystroke behavior for correct authentication. For example, “8374” can be entered as “8_3_7___4”, with two short and one long pause between digits. Pauses are controlled via tempo cues similar to a metronome to aid in counting pause durations. Average EER decreased from 8% to 4% for natural rhythmic input without cues to incorporating artificial rhythms with tempo cues.

However, though tempo cues are given, they require rhythmical sense at some level, along with memorization of established pauses.

Sensor-enhanced keystroke dynamics have also been suggested for improving performance. For instance, Wu *et al.* incorporate velocity measurements to achieve an average accuracy of 98.6% using an SVM classifier and data from ten users [109]. Similarly, Giuffrida *et al.* join samples of keystroke, accelerometer, and gyroscope data, where results indicate that accelerometer measurements are more useful than gyroscope measurements, and combining movement data with keystroke features provides approximately equivalent performance of movement-related features alone [110]. While sensor-related features appear to be more robust than keystroke dynamics, use of such sensors is power consuming. A balanced solution could mostly rely on keystroke dynamics, while periodically including accelerometer readings.

Research Challenges

There remains a need for performance evaluations under uncontrolled conditions, such as typing while walking or lying down. A user may type differently according to his or her emotional or physical state. Injuries to the hands, temporal changes to the device's screen, and even changes in typing speed could result in performance degradations. These are all non-trivial scenarios that are most likely the future of keystroke dynamics for mobile device security [100].

5.4 Touch Gestures

A 2013 study predicted doubling of touchscreen panel shipments by 2016 to reach an astonishing three billion units [111]. Furthermore, the touchscreen market has extended beyond mobile devices for modern updates of LCD monitors, cameras, navigation devices, automobiles, and more [112]. Hence, authentication via touchscreen gestures is convenient, cost-effective, and may, at some point, become necessary. Therefore, several researchers have investigated such gestures (e.g., swipes [113,114], flicks [115,116], pinches, and slides [117]), as well as handwriting as behavioral biometrics [118].

Touch gestures differ from keystroke dynamics in the implication of a touchscreen-enabled device for data acquisition. Keystroke dynamics are mainly based on the nature of pressing and releasing keys. Keystroke dynamics are applicable to a wider range of devices, while touch gestures encompass a wider range of input forms. Similar to keystroke dynamics, however, touch gestures elicit accelerometer measurements as a result of device vibrations when interacting with the screen [115, 119]. Hence, a few efforts have extended touch gestures to include motion-based features [120]. Further, it has been shown that touch gesture features allow authentication with accuracy as high as 99% and EERs as low as 0.03% with simple classifiers such as k-Nearest Neighbors [121] or distance calculations [119].

For feature extraction, researchers take advantage of mobile device-specific operating system calls for logging of x and y-coordinates, gravity, pressure, velocity, finger area, correlation values in multi-finger gestures, average duration of the gesture, and other relevant metrics that help to describe the statistics of the gesture [121–125]. For instance, Antal and Szabó investigate the accuracy of swipe gestures using touch duration, swipe trajectory length, average velocity, acceleration, midstroke finger pressure and area, and mean gravity values in three dimensions [126]. Fifty-eight samples were collected from 40 subjects, and one and two-class classification were performed. Bayes Net, k-Nearest Neighbor, and Random Forests were compared in the two-class problem, where Random Forests provided a 0.004% EER. Parzen density estimators, Gaussian mixtures, incremental Support Vector

Data Descriptors, and k-Nearest Neighbors were compared in the one-class problem. Incremental Support Vector Data Descriptors provided the lowest EERs, while the one-class problem provided higher EERs than the two-class problem. Results also indicated that device movement and holding position were the most user specific and one-class techniques performed better at classifying negative classes than positive.

Touch gestures have also been used in soft biometric classification, which is particularly useful in criminal investigations, where touch gestures indicate gender and proportional relationships that infer otherwise unknown physical characteristics, such as hand size, forearm length, and height. For instance, Miguel-Hurtado *et al.* propose use of swipes for sex prediction via extraction of length, width, height, area, thickness, pressure, speed, acceleration, arc distance, and start-to-end angle as features [127]. Differences were shown between male and female width, area, angle, speed and distance features. Additionally, the authors find that the multilinear logistic regression classifier was most reliable for sex prediction, obtaining 71% accuracy based on an individual swipe direction (down-to-up). Decision-level fusion of all swipe directions rendered a higher accuracy of 78%.

Similarly, Bevan and Fraser consider an interesting approach which analyzes the correlation between swipe gestures, thumb length, and gender [128]. Because one-handed interactions are typically only completed by the thumb, the authors obtain thumb measurements and 21,360 swipe gestures in multiple directions from 178 subjects. Gesture length, completion time, thickness, pressure, speed, and acceleration are extracted as features, revealing a statistically significant relationship between thumb length and swipe gestures, particularly in completion time, speed, and acceleration. Furthermore, results show that male subjects complete gestures faster than women.

The advantages associated with touch gestures have further prompted researchers to consider such screen interactions for improving security schemes on devices used by individuals with disabilities. For instance, PassChords is introduced for those with vision impairments, such that a password equates to a certain sequence of screen taps [129]. Likewise, Zaliva *et al.* investigate the finger's proximity to the screen prior to making contact via modeling the trajectory and posture of the finger [130]. Such an implementation could accommodate users with finger injuries given that contact with the device is no longer necessary.

The research literature suggests that touch data is application-dependent, such that researchers should not expect generalized performance across applications, but should instead consider "context-aware" implementations [131–134]. Khan and Hengartner suggest such an approach with the claim that performance can be improved if the biometric service is controlled by the individual applications themselves, allowing fine tuning of features and more specific classifiers [34]. The core of this work is to investigate the advantages and disadvantages of device and application level authentication. For experimentation, the authors develop four applications (browser, navigation, launcher, and comic viewer) for 32 users to use in an in-the-wild manner for ten weeks. Touchscreen features were recorded, including metrics such as touch point coordinates, finger pressure, area, and finger and screen orientation. For application-specific feature tuning, the authors employ the Kullback-Leibler (KL) divergence measure, where KL-divergence scores differ by application, implying that the significance of features differs according to the application. Experimental results also suggest that this approach is more accurate than the device-centric approach as false acceptance rates decrease.

Research Challenges

It is shown that touch gesture information is hard to mimic, and as a result, it is a secure option compared to knowledge-based methods [135]. Specifically, touch gesture features are independent, suggesting that an intruder's ability to accurately repeat one feature is no indication of his ability to repeat another. Because implementations consider multiple characteristics of touch behavior, it is hard to deceive an authentication system in every dimension simultaneously. Further, when sampling rates are small, it becomes more difficult to precisely learn and mimic touch gestures. Finally, touch gestures are largely dependent on biological anatomy, such that an intruder must consciously be aware of the user's hand geometry. On the other hand, it is shown that the accuracy of systems which depend on touch gestures is affected by the screen's orientation (i.e., portrait or landscape), the device's location (i.e., placed on a flat surface versus held in hand), and the screen size, and as a result, it is suggested that implementations consider posture-dependent feature templates [136]. Research also suggests that due to the behavioral and unconstrained nature of touch gestures, data is further affected by the dominant hand, mobility, usage changes over time, and user location [132].

5.5 Voice

Voice/speaker recognition combines physiological and behavioral characteristics for the identification of a speaker based on his or her speech [49]. Anatomical aspects, such as the vocal tract and lips, coupled with behavioral characteristics, such as age or emotion-related tones, offer a rich feature space which can be statistically analyzed [137, 138].

Two voice recognition modalities exist [139]:

1. Text-dependent: In text-dependent systems, users are asked to speak a predetermined phrase, and are therefore aware of the biometric service (hence, this is not a covert system). Because of the use of a fixed phrase, the system is more accurate.
2. Text-independent: In text-independent systems, the service attempts to recognize the speaker independent of what is spoken. Text-independent systems are useful when there is less control over the input, such as when the user is not aware of the service, which subsequently allows greater flexibility. However, achieving high performance in text-independent voice recognition is more challenging due to its unconstrained nature.

The components of a voice recognition system work cohesively as a pattern recognition system. Having collected speech samples, features are extracted from the raw data similar to feature extraction in face recognition. Such features are categorized into short-term spectral, voice source, spectro-temporal, prosodic, and high-level features. Short-term spectral features are extracted from 20-30ms frames to describe resonance properties of the vocal tract. Voice source features model voice modulation as a result of the openings between the vocal cords. Prosodic and spectro-temporal features cover longer frames to include intonation and rhythm. High-level features represent conversation-level attributes, such as frequent word use. Ideal voice recognition features should differ between various users, but be similar within samples from the same user. Further, these features should be minimally affected by outside noise, behavior, and health, are quantifiably measurable, occur often and naturally, and be hard to mimic [140]. It is found that no one feature has all of these properties; however, though the simplest, spectral features are the most discriminative [139]. Following feature extraction, features are matched via models such as vector quantization, Gaussian mixture models, and SVMs [140].

Traditionally, voice recognition has been applied to access control, law enforcement, and personalization (e.g., intelligent answering machines) [139]. Recently, voice recognition has been used in banking for automatic recognition of customers during telephone transactions. This service supposedly eliminates the need for security questions, and can recognize customers despite voice changes and even gender reassignments [141]. This application shows the true potential of voice recognition beyond forensic and criminal investigations.

Research Challenges

Voice recognition is likely the most universal implementation available for mobile devices. The purpose of mobile devices (specifically, cellular phones) is to facilitate communication primarily through phone calls. Therefore, voice recognition can be applied to any device that can support the required biometric software. However, voice recognition on mobile devices is often considered a weak biometric, and should, therefore, be used in multimodal systems [142–146]. Given the mobility of mobile device users and the lack of controlled environments, voice captured on these devices is often contaminated with various sources of noise. Hence, Section 6 discusses various implementations which have combined voice with additional biometric modalities.

5.6 Behavioral Profiling

This section emphasizes use of mobile device *usage data*, defined as the output or log of trackable activity carried out via available application services. This data is largely based on interactive-level sensing, where the focus is on how the user interacts with the device, such as in making phone calls, sending text messages, and application usage [147]. This is often referred to as *behavioral profiling.*

Previous efforts regarding interactive data mostly involve handling of nominal data in an unsophisticated manner, such as through frequency counts and categorical representations. This is mainly due to the inability to process these values mathematically. Interactive data values usually represent visited entities, such as the names of applications opened or closed or Wi-Fi network names in which the user connects the device for internet access [148]. Therefore, these values rarely reflect any notion of order and any numerical representation typically does not imply meaningful numeric computations. Features are categorized as follows [149]:

- *Categorical Features*: Categorical feature representations group interactive data values. For example, instead of listing the names of each social networking application, the feature vector could simply include 'social networking' itself as the feature. Hence, if there are five social networks that a user visits, the feature vector will only state that the applications were for social networking without providing the exact details of the application. Bassu *et al.* have considered this approach for modeling application traffic by categorizing applications according to marketplace themes [150]. The time of data capture is also grouped according to the time of day (e.g., morning) and the device's movement and location values are discretized to values such as fast and office, respectively. Similarly, Branscomb categorizes application traffic into groups such as audio, messaging, and settings [151]. Obviously, this method reduces the feature values to a smaller set, which may be too general to allow distinction among users when used as a stand-alone method.
- *Frequency Features*: Frequency-based feature representation is seen often in the research literature for interactive data, given that it is trivial to count how many times an action is taken [152]. It is also intuitive to consider the most frequented actions

taken to distinctively model user behavior. Fridman *et al.* considers frequency representation for application and web browsing activity [153].

- *Sequential Features*: Sequences of actions are also considered as features [153, 154]. Here, researchers assume that the order in which actions are taken is significant and unique to each user. This approach is similar to the n-gram representation of text in stylometry applications, where classification is based on frequent n-tuples found in documents as indicators of an author's style.

Various implementations have been considered for behavioral profiling. For instance, Cao *et al.* investigate behavioral profiling as a means of associating contexts with frequent behavior [155]. While this work may be more beneficial for marketing platforms where manufacturers want to customize advertisements to the personal interests of their consumers, it supports the notion of behavioral profiling on mobile devices. Moreover, fifty students were recruited for this study for one month in which GPS, GSM, system, call log, sensor, and interaction data were recorded. All volunteers were able to confirm that 95% of associations discovered by the researchers were correct.

Similarly, Seifert *et al.* consider context-specific behavioral profiling as a means of mobile device security [156]. TreasurePhone is proposed to allow access to specific applications depending on the location of the device. Users are free to set these locations, which are considered spheres, where each sphere allows a different security level. Thereafter, spheres are automatically activated based on location detection. For instance, the sphere that correlates with a work location would restrict access to email and messaging applications, whereas the home sphere would allow access to gaming, email, and calling applications. Hence, the authors couple location and application usage to develop various profiles. This concept suffers, however, in the need for location detection and the requirement of user cooperation for establishing the various spheres. In the event that a user travels often, he or she may need several spheres, which would require an increase in user effort. Additionally, location detection via sensors such as GPS is power-consuming and could cause excessive battery drain on the device [153, 157].

Behavioral profiling has also served as a tool for classifying malicious malware, as Jang *et al.* propose Andro-prolifer as a means to utilize system calls, their arguments, and system logs for detecting malicious and benign software on mobile devices [158]. This work attempts to address the shortcomings found in previous efforts for malware detection that focused mainly on the frequency of system calls, as the number of calls is typically low. The authors employ a database of 709 malware samples and 350 benign samples to reach an average classification accuracy of 99%.

Research Challenges

The research suggests a lack of standard datasets from which benchmark results can be obtained. While several benchmark datasets exists for physiological traits, several behavioral-based studies are based on the actions taken by 10 to 50 subjects, significantly limiting any generalized conclusions. For instance, it seems that accuracy is context-dependent, such that it is important to match templates which arise from the same data source [159]. However, requiring context-dependent feature templates could increase the resources necessary to store such templates. It is also shown that a dependency exists between samples and the time intervals in which samples are obtained, along with an introduction of a bias when using raw samples [160]. There is also uncertainty on how much data is needed for authentication [161]. A large-scale and real-world database is key to evaluation of such issues.

6. Multimodal Authentication

Biometric systems which rely on a single trait (i.e., unimodal) are often problematic. Multimodal systems are often used for enhanced performance and robustness via combination of several modalities. Multimodal systems typically reduce problems associated with universality and enrollment, increase flexibility, and reduce the effectiveness of adversarial attacks [60]. While biometric fusion can indicate the use of multiple sensors, multiple matching algorithms, and multiple samples, the following describes the fusion levels of multiple biometric traits, given that this survey focuses on various traits available from mobile devices. In this context, biometric traits are commonly fused at feature, matching, and decision levels:

- *Feature Level Fusion*: Features from each (or the same) modality are combined immediately after extraction from the raw data and fed into the matching algorithm. Normalization of features is usually required when handling heterogeneous representations.
- *Matching/Score Level Fusion*: Matching scores from each modality are combined as a single score, which is subsequently used at the decision level. Such combinations are based on various rules, such as min, max, product, and sum.
- *Decision Level Fusion*: Matching decisions from each modality are all considered to determine an overall decision. Various rules, such as majority voting, are applied to determine the final decision.

In the context of mobile devices, it is argued that multimodal biometrics is an affordable solution to mobile security given the availability of already-present sensors [162]. However, as with unimodal systems, biometric authentication is data-dependent, such that poor data samples from multiple modalities could fail to boost performance despite the known advantages. Moreover, use of multiple physiological modalities requires use of multiple sensors, which has the potential to increase operating costs [163]. Despite said considerations, overall, multimodal authentication has shown to increase the robustness of mobile device security [164].

Such an implementation combines gait and voice data from 31 subjects [97]. For gait collection, an accelerometer is attached to the hip pocket, breast pocket, and carried while subjects walk at normal and hurried speeds. Correlation and FFT similarity scores are used for matching accelerometer signals. These same subjects also provided speech samples from which MFCC features were extracted. Various noise levels were examined using three SNR measures - 20, 10 and 0 dB. It is found that error rates decrease from 13.7–17.2% and 2.82%–43.09% using gait and voice recognition, respectively, to 1.97%–11.8% using the combined system. However, in the event that the user is not walking or speaking, the service is ineffective.

A similar effort joins face and voice to address sample quality and lack of training data in mobile device authentication [162]. It is stated that sample quality is particularly poor when captured on mobile devices due to unconstrained conditions during data capture and the inclusion of low-cost sensors. Further, the authors argue that consumers are less inclined to offer several training instances during enrollment, though increasing training samples correlates with increases in performance. Therefore, using multiple modalities addresses these issues by increasing the chances of obtaining a larger amount of high-quality samples.

The Fisherface technique is used for face recognition given its robustness in unconstrained conditions (i.e., variations in expression, pose and illumination). Hidden Markov Models and Linear Discriminant Analysis are used for voice recognition when using score-level and feature-level fusion, respectively. Further, quality-based fusion is employed, such that each modality is weighted based on the sample quality while ensuring that high quality in one sample and very poor quality in the other does not essentially equate to a unimodal system. In other words, both weights must meet some threshold to avoid full dependence on one modality. Both score and feature-level fusion decreases error rates, while the best improvement is observed using feature-level fusion (4.29% and 34.72% for face and voice, respectively, to 2.14% for the combined system).

An additional work combines face, voice, and signature for securing PDAs [165]. While experimental results suggest the common trend of considerable improvement in accuracy when all traits are combined (i.e., 3.38%-29.87% to 0.56% decrease in error rates), there are many other points worth mentioning. First, the voice module used the text-dependent approach, as the authors felt that a text-independent system would create large models to compensate for various phonetic variations, and such models would be computationally expensive on mobile devices. Second, the authors take into account the risks and privacy issues associated with processing the data on a server by choosing to perform all processing locally on the device. Further, the authors collect face and voice samples from the same subjects, but include signature samples from different subjects. While the authors assume no correlation between face, voice, and signature such that the presented data collection procedure is valid, this data collection procedure indicates the lack of datasets for performing such multimodal experiments.

Similar works include the combination of face, iris, and periocular recognition [66, 166], authentication based on eye gaze and touch gesture for addressing shoulder surfing-like attacks [167], a multimodal approach which joins linguistic and behavioral profiling with keystroke dynamic features from text messages [168], and the combination of application, Bluetooth, and Wi-Fi traffic [152].

Table 1 summarizes several biometric approaches for mobile devices.

7. Template and System Security

A major aspect of biometrics on mobile devices is security and privacy. For widespread acceptance, users must be confident that their biometric features are protected from outside sources and used for the intended purpose. Unfortunately, biometric systems are vulnerable to adversarial attacks, such as spoofing via fingerprint molds and use of images during face detection. For instance, it is shown that, prior to software patches, it was possible to derive malware capable of acquiring the fingerprint image stored in the local memory of the device, extract the fingerprint template, and restore the fingerprint features [175]. Much research has been directed towards preventing such occurrences in standard biometric systems; these and new implementations are now applied to mobile platforms.

Zafar and Shah note two attack types: direct and indirect [176]. Direct attacks operate on the sensor through the presentation of fake or false traits; this is often referred to as spoofing or presentation attacks. This is alarming on mobile devices as the sensor is an always-available component. For instance, Vasquez-Fernandez *et al.* note that facial recognition is susceptible to spoofing [177]. Anti-spoofing techniques, such as blink detection or analysis of background illumination, are often used to determine if the subject is actually alive; however, due to the flexibility in which mobile devices are handled, the authors indicate

Table 1: Biometric implementations for mobile device security.

Ref.	Modality	Features	Subj.	Matcher	Performance
Physiological Modalities					
Crouse *et al.* [58]	Face	Biologically Inspired Model (BIM) features from the forehead, periocular area, eyes, nose, and mouth.	10	SVM classifier with a RBF kernel.	65% TAR at 1% FAR
Fathy *et al.* [59]	Face	Holistic and mouth, eye, and noise pixel intensity values.	50	Eigenfaces, Fisherfaces, Large-margin Nearest Neighbors, Sparse Representation-based Classification (SRC), Affine/Convex Hull-based Image Set Distance, Sparse Approximated Nearest Points, Dictionary-based Face Recognition, and Mean-Sequence SRC.	17.6% - 74.9% ACC
Raja *et al.* [166]	Face and periocular	SIFT, SURF, and BSIF features.	46	Bhattacharya distance and Fast Approximate Nearest Neighbor Search.	0.99% - 4.69% EER using feature-level fusion.
Riesch *et al.* [61]	Face	Local binary patterns.	9	SVM	91.3% - 100% ACC
Raja *et al.* [67]	Periocular	Concatenated histograms of Short Term Fourier Transform responses from Laplacian pyramid images at various scales.	75	L_1 minimization.	8.33% - 31.02% EER
Raja *et al.* [66]	Face, iris, and periocular	Iris texture, SIFT, SURF, and BSIF features.	78	Bhattacharya distance and Fast Approximate Nearest Neighbor Search.	0.68% EER
Tao *et al.* [62]	Face	DIFS (distance in feature space) and DFFS (distance from feature space) values.	6	Probability-based Parzen classifier.	1.2% EER
Sarkar *et al.* [169]	Face	Features from the first five layers of a deep convolutional neural network.	50	SVM	88% - 96% ACC
Raghavendra *et al.* [170]	Fingerprint	Minutiae	25	BOZORTH3 comparator.	3.74% EER
Han *et al.* [171]	Palmprint	Sum-difference ordinal codes.	40	Hamming distance.	0.92% EER
Behavioral Modalities					
Shih *et al.* [120]	Touch gesture	Time, pressure, and size.	10	Naive bayes, SMO, and J48 classifiers.	88% - 100% ACC
Nickel *et al.* [95]	Gait	Mean, minimum, maximum, and standard deviation in tri-directional accelerometer readings, MFCCs, and BFCCs.	36	k-Nearest Neighbors with Euclidean distance.	3.67% - 5.48% FMR
Saevanee *et al.* [121]	Keystroke dynamics	Finger pressure, inter-key time, and hold time.	10	k-Nearest Neighbors	1% - 35% EER
Vildjiounaite *et al.* [97]	Gait and voice	Gait: normalized steps and Fast Fourier Transform coefficients. Voice: MFCCs.	31	Correlation Score, FFT Score, and Gaussian Mixture Models.	9.1% - 11.8% EER
Li *et al.* [6]	Behavioral profiling	Application usage.	76	Dynamic rule-based classifier	12.91% FRR
Fridman *et al.* [153]	Behavioral profiling	Text (*n*-grams), application usage, Wi-Fi traffic, and location.	200	Maximum likelihood and SVM with a RBF kernel.	1% - 5% EER
Antal *et al.* [126]	Touch gestures	Duration, trajectory length, velocity, acceleration, pressure, area, gravity.	40	Random Forests, Bayes Net, k-Nearest Neighbors, Parzen density estimation, Gaussian mixture models, Incremental Support Vector Data Description	0.002% EER using Random Forests
Nickel *et al.* [98]	Gait	MFCCs and BFCCs	48	Hidden Markov Models	7.45% EER
Kwapisz *et al.* [172]	Gait	Acceleration, time between peaks, and binned distributions.	36	Decision trees and neural networks.	82.1% - 92.9% ACC
Mondal *et al.* [114]	Touch gestures	Stroke duration, initial coordinates, direction, trajectory, velocity, pressure, and area.	71	SVM and Counter Propagation Artificial Neural Network (CPANN)	98% ACC
Feng *et al.* [173]	Touch gestures	Coordinates, direction, speed, pressure, and distance between multi-touch gestures.	40	Decision trees, Random Forest, and Bayes net.	4.66% FAR and 0.13% FRR
Feng *et al.* [89]	Motion	Trajectory, duration, mean, variance, and standard deviation from accelerometer and gyroscope measurements.	31	SVM and Discrete Fretchet Distance	3.67% EER
Cai *et al.* [174]	Touch gestures	Speed, pressure, distance between fingers.	20	Distance Time Warping and Manhattan distances, Neural Networks, SVM, and Bayesian Networks.	4.05% FAR at 3.27% FRR using SVM
Wu *et al.* [109]	Touch gestures	Pressure, position, and area.	10	SVM	98.6% ACC

that a single anti-spoofing measure is not the ideal approach. Further, current methods may not respond to new attacks, which are likely given the widespread use of mobile devices.

Indirect attacks operate on software or interfaces between modules, such as a transmission channel. The service is intercepted at some point, and identifying information is retrieved or altered. Malware is also a big concern for mobile devices; because applications are freely developed and made publicly available, bypassing application permissions during installations can be detrimental. Template protection is key to preventing indirect attacks.

Template protection plays a key role in ensuring user privacy within and across multiple applications. Unlike passwords, biometrics are permanently embedded. They cannot be changed or reissued if compromised, and exposure of biometric features to the wrong individual is likely disastrous. As a result, there are five common properties associated with protected templates [178, 179]:

1. Protected biometric features should be *noninvertible* such that derivation of the original template is computationally difficult.
2. A protected template is *revocable* given generation of a new template derived from the original features.
3. Templates should be *unlinkable* given access to multiple protected traits; in other words, it should be difficult to determine if multiple templates were provided by the same individual.
4. Protected templates should be *diverse* across different applications.
5. System *performance* should be maintained when using protected templates.

Salting, noninvertible transform, key-binding biometric cryptosystem, and key-generating biometric cryptosystem are four common template protection schemes [180]. Salting provides protected templates through a key or password that the user provides during authentication. Therefore, while the user must ensure the security of the key, the template is revocable if the key is compromised by simply generation of a new key without having to regenerate biometric features. Template differences between users is also enhanced through the user-specified key [181]. Further, the transformed template is invertible. However, maintaining performance is a concern, particularly on mobile devices, as matching is performed in the transformed space. Because users will likely exhibit large variations in their biometric traits, matching in the transformed space will likely be faulty as even minor changes in the original space result in major deviations in the transformed space [181]. Noninvertible transform is similar to salting where a one-way function which depends on a key and the biometric features maps the features to a new space. Unlike salting, noninvertible transform does not require the user to maintain a secret key, and knowledge of the key does not imply the ability to revert the protected template back to its original state. Because protected templates can be regenerated with only a new key, salting and noninvertible transform are considered cancelable biometrics [179]. Biometric cryptosystem approaches use helper data to either bind or generate a key based on the biometric data presented during an authentication attempt. The helper data uses error correction schemes to derive a match between the gallery and probe templates.

Hybrid approaches are often superior, similar to multimodal biometrics. For example, Supriya and Manjunatha derive a secure implementation of iris recognition using chaotic theory, biometric cryptography, and noninvertible transform [182]. Chaos introduces a high level of randomness due to the inability to predict future behavior; as such, including chaotic output into the transformation process lends a suitable protected template with a significant amount of entropy. While their method is not directly stated to operate within mobile devices, elements of the technique may actually scale well to mobile units. For instance, the template transformation is done through simple bitwise XNOR and XOR operations on the iris code and the chaotic key, which is claimed to have a space of 2^{319}. Therefore, resource-draining computations are avoided, which is necessary on mobile devices, and it becomes very computationally difficult to derive the chaotic key used in the transformation.

However, a challenge for typical protection schemes is the requirement of simple matchers or distance calculations [178]. This ‘challenge’, however, may be beneficial on mobile platforms. If feature vectors are simple, complex algorithms may not be required. As a result, resource drain is controlled and fast and secure authentication is carried out. An additional challenge is the tradeoff between maintaining noninvertibility and satisfactory performance. Noninvertibility implies that the protected template does not reveal any identifying information which would allow an intruder to produce the original template from the protected template. However, high performance implies that the templates retain the maximum amount of discriminating information. Hence, there is an obvious issue of maintaining discrimininability while simultaneously suppressing it. Nandakumar and Jain claim that to achieve both properties, the protection scheme should use the knowledge of the underlying statistical structure of the features. However, deriving complex distributions is often non-trivial [178]. On the other hand, the authors also state that the majority of protection schemes are optimized for verification schemes (i.e., one-to-one matching). While this may be problematic in larger applications, this is ideal for mobile devices as the authentication process is a verification problem. Therefore, applying existing techniques may be a suitable solution to protecting mobile device authentication.

Fortunately, modern devices are developed to handle sensitive transactions and processes via application of template protection schemes along with various protocols [183]. These protocols work to provide private and secure environments to avoid data leaks and malware intrusions. Such environments are consequently highly beneficial in securing local biometric systems and much effort has been directed towards providing isolated processing environments for biometric authentication on mobile devices. The Fast Identity Online Alliance (FIDO), Biometric Open Protocol Standard (BOPS), Trusted Execution Environment (TEE), Trusted Mobile Zone (TMZ), and Secure Enclave Processor (SEP) provide the necessary protocols and specifications to achieve said tasks.

According to Stokkenes *et al.*, FIDO and BOPS are protocols to support and regulate biometric authentication. FIDO is developed as a cohesive effort by several organizations to produce specifications for the Universal Authentication Framework. This framework facilitates local authentications (such as biometric identifications on mobile devices) via cryptography and the FIDO authenticator. Hoyos Labs' BOPS is similar to FIDO; however, it provides more detailed specifications regarding biometric services, including guidelines for liveness detection and error rate thresholds. The TEE works to prevent unauthorized access to sensitive applications, such as a biometric service, by providing an isolated and secure operating environment. "Trusted systems" operate within these environments, which is referred to as ARM's TrustZone technology on mobile devices [183]. TrustZone extends security to various hardware components, dividing the memory space and other hardware into secure and normal zones. Components designated as secure are restricted in how they interact with, accept, and deliver information. For instance, Zhang implements facial recognition for mobile devices within TrustZone for a secure authentication process [184]. Every phase of the biometric service is housed within a secure environment; it is claimed that the service is protected even from those having root access to the operating system. Paul and Irvine discuss secure fingerprint recognition on mobile devices via TrustZone as well [185]. However, the authors note that non-secure applications often access the sensing device, indicating that the isolation desired in TEEs is perhaps a work-in-progress concept [186]. Apple introduced the SEP as a means of securing its fingerprint recognition service [187]. It serves as a TEE acting as a separate operating system.

The many attack points of biometric systems reflect serious privacy concerns, particularly when biometric systems are implemented on unattended platforms such as mobile devices.

There has to be some level of technical understanding from mobile device users of biometrics to ensure proper use of the service without unintended exposure of the trait to others. Second, users must be reassured that all data is gathered for authentication purposes, and proper measures will be taken to encrypt and/or anonymize the data accordingly. Further, in the event that the service is intercepted, manufacturers, service providers, and consumers must be knowledgeable of the steps required for addressing the potential issues associated with such occurrences. These concerns leave several questions, such as who is responsible for the biometric service – service providers or manufacturers? Is authentication possible without network access? Should the data be stored on the device, on a back-end server, or in the cloud?

8. Open Problems

Biometric authentication is often considered a stronger form of security compared to knowledge-based methods for obvious reasons; biometric traits cannot be forgotten or stolen and are hard to spoof. However, these benefits do not implicate a flawless and seamless authentication experience. Several issues remain a bottleneck in terms of precision, generalization, and scalability in biometric systems. Beyond template security, four specific research challenges regarding mobile devices have proven difficult to address; these include hardware limitations, environmental and user-induced noise, inconsistent data, and balancing transparency with usability.

8.1 Hardware Limitations

A major concern in terms of hardware lies in constant user access to the sensor. In traditional biometric systems, users only have temporary and brief encounters with the sensor. Further, the sensor is likely tailored to the biometric modality in which it is engineered to capture (i.e., finger pegs are included for palmprint recognition). On mobile devices, however, the sensor is a general component of the device's architecture, lacking any mechanisms for preventing tampering with and spoofing of the sensor. As a result, an open problem is how to properly secure the device's sensor without inhibiting its intended operation beyond biometric authentication.

Second, there are variations in hardware specifications from one device to the next. While one biometric modality is suitable for one device, the sensor it requires may be unavailable on other platforms. This implies the need for platform-specific implementations. Additionally, hardware variations, such as those which affect sensor quality, introduce sources of undesired noise. Outdated sensors may provide poor data samples which lack discriminating features. If, for instance, a camera produces blurry images, the quality of facial images could be too poor to extract reliable information for face recognition.

Finally, some modalities may impose additional hardware costs, reduce the convenience of the device's design, or require additional storage or processing power. For example, there are suggested implementations which require unrealistic items for operation, such as an approach which combines touch gesture features with sensor information from a digitalized glove [173]. Important aspects of mobile devices are usability and portability, but inclusion of biometric technology has the potential to significantly reduce normal operation of the device.

8.2 Environmental and User-Induced Noise

Environmental influences consist of variations in lighting, background scenes, and other noise sources that all affect the ability to properly capture a high-quality sample. Such influences require segmentation algorithms to separate the actual biometric characteristic from environmentally-induced noise [188]. Further, modality-specific noise poses a challenge, such as cuts on fingers, make-up and accessories in facial recognition, and illnesses that affect the vocal tract in voice recognition. Hence, while the biometric characteristic can be reliably captured, there are noisy aspects of the sample that degrade performance. Algorithms, such as Principal Component Analysis, are denoising techniques which can assist in reducing this noise, but further challenges are how to distinguish between noise and discriminating information, and how to balance the computational load on resource restrained mobile devices when implementing such algorithms. Further, there is little research to address how to properly quantify data quality, recognize when the sample is poor, and instruct the subject on how to re-present him or herself to the sensor to allow proper data collection [189].

The unpredictable use of mobile devices introduces further noise sources that complicate the authentication process. Individuals are free to use mobile devices in various settings; physiological traits in particular are highly influenced by these settings. It becomes nontrivial to reduce these characteristics given the restrictions of the device's resources, the inability to predict and quantify these noise sources, and the inability to expect consistent and/or cooperative interaction from the user.

8.3 Inconsistent Data

Physical and/or behavioral variations introduce inconsistencies in data samples that usually correspond with lower quality data samples or poor matching. Physical variations include unavoidable changes such as aging and illness. The effects of aging are prominent in nearly all biometric modalities, and a core research challenge lies in the ability to identify the same subject over extended periods of time [188]. On the other hand, behavioral changes are likely influenced by emotion, and include changes such as facial expression and typing behavior. When such variations are introduced, it could result in mismatches between gallery and probe features.

Behavioral modalities in particular are not as distinct or stable as physiological biometrics. For instance, though no two iris patterns are identical between different individuals, groups of individuals may share a common call pattern or connect to the same Wi-Fi networks. Moreover, implementations must consider conscious and unconscious behavioral changes that can occur on a daily basis, requiring constant updates to enrolled templates. Such requirements debunk the expectation of behavioral systems that consistent user behavior is exhibited; these same requirements introduce additional needs for software which maintains updated biometric templates.

8.4 Balancing Transparency with Usability

Physiological modalities may be inconvenient to users as they require as many authentication attempts as knowledge-based methods. These traits also fail to provide transparent and continuous protection [22]. On the other hand, there is a lack of transparency in behavioral systems due to the inability to authenticate when the user is not providing the information that the system is created to monitor. Due to the sporadic nature of human behavior, it currently seems impossible to solely rely on a behavioral system. Hence, some explicit form of authentication is required at some point when biometric methods fail to provide a high enough confidence level to allow device access. In such cases, services, such as PRISM (Policy-driven Risk-based Implicit Locking for Improving the Security of Mobile End-user Devices) which allows users to understand and alter its decisions, are reasonable solutions for minimizing the need for knowledge-based authentication [190]. PRISM monitors location and application usage for hierarchical decision-making functionality based on several user-defined policies. These policies were shown to reduce knowledge-based authentication attempts by up to 75%. However, in these cases, the system is no longer transparent [22]. These challenges reflect the balancing of transparency with usability as an open research problem.

Table 2 summarizes the impact of the discussed open problems on each of the aforementioned biometric modalities. This table helps to put into perspective the various challenges which may be significant issues for each service. Each open problem is ranked from 1 to 5, where rank 1 implies minimal impact and rank 5 implies maximal impact.

9. Conclusion

Mobile devices offer services ranging from location detection and navigation to web browsing. Consumers now benefit from these high-tech devices, performing tasks normally requiring a standalone computer in a mobile and efficient manner. Moreover, the growing resources available in these devices, such as increases in memory and processing power, along with optimization of battery consumption, have allowed sufficient storage and use of various file formats. In regards to smartphones in particular, studies suggest that consumers are more inclined to use these devices for practical reasons (i.e., utilities, communication, and productivity), in comparison to the typical entertainment and gaming use of tablets, leaving manufacturers and consumers increasingly concerned about mobile device security [191].

Security methods on mobile devices have relied on user knowledge, such as in numerical and graphical passwords. These methods, however, are susceptible to theft, given that they do not address shoulder-surfing attacks. Password and PINs are also easily forgotten, posing an inconvenience to the user to retrieve or change the password. Hence, consumers are inclined to use those easiest to remember, such as those with repetitive and consecutive characters or digits. Knowledge-based methods are also efficient only at the point-of-entry; once a user has been authenticated, the device and its content is available to anyone with possession of the device. Therefore, these security measures do not ensure continuous and robust protection.

Biometric authentication has been explored to address the issues associated with knowledge-based techniques. Physiological modalities, such as face, periocular, fingerprint, and iris, depend on user cooperation and various sensing technologies for data capture. These traits reduce the need for remembering passwords and PINs, and offer improved mobile device security. Behavioral modalities, like keystroke dynamics, touch gestures, and behavioral profiling, also improve upon knowledge-based methods by allowing continuous and transparent authentication. However, biometric security on mobile devices remains a complex procedure due to hardware limitations, noisy and inconsistent data, and adversarial attacks. Nonetheless, this survey aims to present the many advantages associated with biometric authentication, while encouraging further research of mobile device security beyond familiar standards.

Table 2: Impact of open problems on each biometric modality.

Modality	**Hardware Limitations**	**Noise**	**Data Inconsistency**	**Usability and Transparency**
Face/Pericular	**3**: Performance may vary across users given differences in camera resolution. Though front cameras continue to improve in resolution, rear cameras capture higher quality images and have adaptive abilities per variations in the environment.	**3**: Numerous sources of motion along with variations in rotation, angles, distances, and backgrounds complicate the recognition process. These factors can be minimized with operating instructions to the user.	**4**: Variations in facial expression and occlusions affect recognition. Facial attributes also change over time.	**5**: Face recognition is a point-of-entry technique, and is not a transparent service. Users frustrated with multiple authentication attempts required in password-based security may similarly be frustrated with face recognition.
Fingerprint	**5**: While fingerprint recognition is becoming increasingly popular on mobile devices, a large portion of devices have yet to incorporate fingerprint scanners. Once scanners are included, users have access to the sensor component, resulting in concerns regarding hardware integrity.	**3**: Dirty sensors and handling the device at various angles when presenting the finger affect the recognition process.	**3**: Wet or injured fingers affect recognition, but it is likely that these factors can be compensated for via on-screen instructions and/or robust feature extraction algorithms.	**3**: While fingerprint recognition is non-transparent and quite intrusive, a large majority of users have suggested that the service is a user-friendly and convenient security option in multiple surveys.
Iris	**5**: Few devices have a near-infrared light source.	**5**: Iris images captured outdoors are contaminated with ghost regions, homogeneous gray levels, and size variations.	**5**: The iris region constantly changes size as the environment and lighting conditions is always changing due to the mobility of the user. These factors are harder to avoid as they are largely based on biological processes.	**5**: Iris recognition is a non-transparent service, and it is quite intrusive as near-infrared light can potentially damage the eye.
Motion/Gait	**3**: Devices should be equipped with accelerometers and gyroscopes. Sensor quality and specifications may vary across devices.	**5**: The device is constantly moving, so a significant portion of signals will be noise instead of meaningful data.	**4**: Users will move differently based on various factors; an overall pattern should be noticeable, but exact movement and walking behavior across consecutive samples is not possible.	**3**: While movement-based recognition is transparent, users will have idle periods. During these times, an alternative service is required.
Keystroke Dynamics/Touch Gestures	**3**: The majority of today's mobile devices use a touch screen as the input mechanism; when this is not the case, however, only keystroke dynamic statistics can be extracted as biometric features.	**3**: Algorithms which include accelerometer and gyroscope measurements introduce noise into data samples from device movement.	**4**: Users type differently based on emotional state, location, finger injuries, environmental conditions, etc.	**1**: Touch behavior is expected to operate the device; hence, it is a transparent service which offers guaranteed data.
Voice	**1**: Mobile devices are equipped with microphones to facilitate phone calls.	**4**: Background noise will widely vary on mobile devices as the user's environmental conditions change.	**4**: Various components of voice (i.e., pitch) are always changing according to the user's emotional state and health. These changes will be reflected as feature inconsistencies.	**3**: Voice recognition is transparent as long as the user is speaking, but it may require combination with a non-transparent service as it is often considered a weaker biometric.
Behavioral Profiling	**1**: Hardware restrictions pose little to no issues for behavioral profiling; however, it should be possible to access system logs for tracking usage data.	**2**: Use of the device's services may be affected by environmental factors or the condition of the user, but compared to other modalities (mostly those which require a sensor), intuitively, outside noise sources will likely be minimal or expected and filtered.	**5**: Though human behavior tends to be habitual, it is highly unpredictable with no guarantee that what was once a repetitive action will continuously be observed in the future.	**1**: Behavioral profiling is completely transparent which provides continuous and user-friendly authentication.

References

[1] F. Parker et al. Security awareness and adoption of security controls by smartphone users. In *Proc. Second Int. Conf. Information Security and Cyber Forensics (InfoSec)*, pages 99–104, 2015.

[2] Jose Pagliery. To hack an android phone, just type in a really long password, sep 2015.

[3] Phone theft in america. https://www.lookout.com/resources/reports/phone-theft-in-america.

[4] Secure our smartphones initiative statement. http://www.ag.ny.gov/sos/secure-our-smartphones-initiative-statement, June 2013.

[5] Richard Nieva. California senate approves smartphone kill-switch bill. http://www.cnet.com/news/california-senate-approves-smartphone-kill-switch-bill/, May 2014.

[6] Fudong Li et al. *An Evaluation of Behavioural Profiling on Mobile Devices*, pages 330–339. Springer International Publishing, Cham, 2014.

[7] Noam Ben-Asher et al. On the need for different security methods on mobile phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, MobileHCI '11, pages 465–473, New York, NY, USA, 2011. ACM.

[8] N.L. Clarke et al. Acceptance of subscriber authentication methods for mobile telephony devices. *Computers & Security*, 21(3):220 – 228, 2002.

[9] Herb Weisbaum. Most americans don't secure their smartphones. http://www.cnbc.com/2014/04/26/most-americans-dont-secure-their-smartphones.html, April 2014.

[10] S. Shaji et al. Review of continuous touch based user authentication. In *Proc. Int Soft-Computing and Networks Security (ICSNS) Conf*, pages 1–5, 2015.

[11] Daniel Amitay. Most common iphone passcodes. http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes, June 2011.

[12] Ashlee Vance. If your password is 123456, just make it hackme. http://www.nytimes.com/2010/01/21/technology/21password.html?_r=0, January 2010.

[13] Alexander De Luca et al. Eyepass - eye-stroke authentication for public terminals. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '08, pages 3003–3008, New York, NY, USA, 2008. ACM.

[14] D. J. Ohana et al. Preventing cell phone intrusion and theft using biometrics. In *Proc. IEEE Security and Privacy Workshops (SPW)*, pages 173–180, 2013.

[15] About touch id security on iphone and ipad, nov 2015.

[16] Richard Devine. Face unlock in jelly bean gets a 'liveness check'. http://www.androidcentral.com/face-unlock-jelly-bean-gets-liveness-check, June 2012.

[17] T. Drflinger et al. My smartphone is a safe! the user's point of view regarding novel authentication methods and gradual security levels on smartphones. In *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on*, pages 1–10, July 2010.

[18] J. S. Arteaga-Falconi et al. ECG authentication for mobile devices. *IEEE Transactions on Instrumentation and Measurement*, 65(3):591–600, 2016.

[19] T. Feng et al. Secure session on mobile: An exploration on combining biometric, trustzone, and user behavior. In *Mobile Computing, Applications and Services (MobiCASE), 2014 6*th *International Conference on*, pages 206–215, 2014.

[20] Fudong Li et al. Active authentication for mobile devices utilising behaviour profiling. *Int. J. Inf. Secur.*, 13(3):229–244, 2014.

[21] Ting-Yi Chang et al. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *Journal of Systems and Software*, 85(5):1157–1165, 2012.

[22] Abdulwahid Al Abdulwahid et al. Continuous and transparent multimodal authentication: reviewing the state of the art. *Cluster Computing*, 19(1):455, 2016.

[23] A. Alzubaidi and J. Kalita. Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys Tutorials*, PP(99):1, 2016.

[24] P. Corcoran and C. Costache. Biometric technology and smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts. *IEEE Consumer Electronics Magazine*, 5(2):70–78, 2016.

[25] S. Alotaibi et al. Transparent authentication systems for mobile device security: A review. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 406–413, 2015.

[26] W. Meng et al. Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys Tutorials*, 17(3):1268–1293, 2015.

[27] Ziming Zhao et al. Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation. *ACM Trans. Inf. Syst. Secur.*, 17(4):14:1–14:37, April 2015.

[28] Alexander De Luca et al. Touch me once and i know it's you!: Implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 987–996. ACM, 2012.

[29] N.L. Clarke and S.M. Furnell. Authentication of users on mobile telephones – a survey of attitudes and practices. *Computers &amp; Security*, 24(7):519–527, 2005.

[30] Reham Amin et al. *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*, chapter Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues, pages 423–446. Springer Berlin Heidelberg, 2014.

[31] Heather Crawford and Karen Renaud. Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management*, 1(1):1–28, 2014.

[32] Steven Furnell et al. Beyond the PIN: Enhancing user authentication for mobile devices. *Computer Fraud &amp; Security*, 2008(8):12–17, 2008.

[33] Adam Wójtowicz and Krzysztof Joachimiak. Model for adaptable context-based biometric authentication for mobile devices. *Personal and Ubiquitous Computing*, 20(2):195, 2016.

[34] Hassan Khan and Urs Hengartner. Towards application-centric implicit authentication on smartphones. In *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*, pages 10:1–10:6. ACM, 2014.

[35] Z. Yu et al. Usable authentication mechanisms for mobile devices: An exploration of 3D graphical passwords. In *Proc. Int. Conf. Platform Technology and Service (PlatCon)*, pages 1–3, 2016.

[36] Cailyn Finkel. Your smartphone lockscreen combo is way too easy to guess, aug 2015.

[37] K. I. Shin et al. Design and implementation of improved authentication system for android smartphone users. In *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, pages 704–707, 2012.

[38] Todd B. Bates. Smartphone security: Why doodling trumps text passwords, mar 2016.

[39] Yulong Yang et al. Free-form gesture authentication in the wild. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 3722–3735, New York, NY, USA, 2016. ACM.

[40] K. Nivethaa Shree and N. Uma. Behavioral biometrics for continuous authentication in smartphones. *Proceedings of National Conference on Communication and Informatics*, 2016.

[41] N. Micallef et al. Sensor use and usefulness: Trade-offs for data-driven authentication on mobile devices. In *Proc. IEEE Int Pervasive Computing and Communications (PerCom) Conf*, pages 189–197, 2015.

[42] Anastasios Drosou and Dimitrios Tzovaras. Activity and event related biometrics. *Second Generation Biometrics: The Ethical, Legal and Social Context*, 2012.

[43] Biometrics as a security measure in health care. January 2014.

[44] Stephen Mayhew. Biometrics use at massachusetts school raise privacy concerns from parents. http://www.biometricupdate.com/201409/biometrics-use-at-massachusetts-school-raise-privacy-concerns-from-parents, September 2014.

[45] Alex and Dorothy Fox. Fox tech watch: Sheriff deploys iris scanning technology. http://www.correctionalnews.com/articles/2012/03/14/fox-tech-watch-sheriff-deploys-iris-scanning-technology, March 2012.

[46] Christopher A. Miles and Jeffrey P. Cohn. Tracking prisoners in jail with biometrics: An experiment in a navy brig.

[47] Introduction to mykad. http://www.jpn.gov.my/en/informasimykad/introduction-to-mykad/.

[48] Use touch id on iphone and ipad. https://support.apple.com/en-us/HT201371, 2016.

[49] A. K. Jain et al. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):4–20, 2004.

[50] L. J. Spreeuwers et al. Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at schiphol airport. In *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG - Proceedings of the International Conference of the*, pages 1–6, Sept 2012.

[51] 7 surprising ways facial recognition is used. http://www.cbsnews.com/pictures/7-surprising-ways-facial-recognition-is-used/.

[52] Alexander De Luca et al. I feel like i'm taking selfies all day!: Towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1411–1414. ACM, 2015.

[53] Manuel Günther et al. *Face Recognition in Challenging Environments: An Experimental and Reproducible Research Survey*, pages 247–280. Springer International Publishing, Cham, 2016.

[54] Jian Huang et al. Face recognition using local and global features. *EURASIP Journal on Advances in Signal Processing*, 2004(4):1–12, 2004.

[55] Andrzej Kasinski et al. The put face database. *Image Processing and Communications*, 13(3-4):59–64, 2008.

[56] Gary B Huang et al. Labeled faces in the wild: A database for studying face recognition in unconstrained environments. Technical report, Technical Report 07-49, University of Massachusetts, Amherst, 2007.

[57] P.Jonathon Phillips et al. The feret database and evaluation procedure for face-recognition algorithms. *Image and Vision Computing*, 16(5):295 – 306, 1998.

[58] D. Crouse et al. Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data. In *Proc. Int. Conf. Biometrics (ICB)*, pages 135–142, 2015.

[59] M. E. Fathy et al. Face-based active authentication on mobile devices. In *Proc. Speech and Signal Processing (ICASSP) 2015 IEEE Int. Conf. Acoustics*, pages 1687–1691, 2015.

[60] Anil Jain et al. *Introduction to biometrics*. Springer Science & Business Media, 2011.

[61] P. J. Riesch et al. Face recognition with environment tolerance on a mobile device. In *Proc. IEEE 2nd Int Cyber Security and Cloud Computing (CSCloud) Conf*, pages 342–348, 2015.

[62] Q. Tao and R. N. J. Veldhuis. Biometric authentication for a mobile personal device. In *Mobile and Ubiquitous Systems - Workshops, 2006. 3rd Annual International Conference on*, pages 1–3, 2006.

[63] D. L. Woodard, S. J. Pundlik, J. R. Lyle, and P. E. Miller. Periocular region appearance cues for biometric identification. In *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Workshops*, pages 162–169, June 2010.

[64] Philip E. Miller, Allen W. Rawls, Shrinivas J. Pundlik, and Damon L. Woodard. Personal identification using periocular skin texture. In *Proceedings of the 2010 ACM Symposium on Applied Computing*, SAC '10, pages 1496–1500, New York, NY, USA, 2010. ACM.

[65] K. B. Raja et al. Smartphone authentication system using periocular biometrics. In *Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the*, pages 1–8, 2014.

[66] K. B. Raja et al. Multi-modal authentication system for smartphones using face, iris and periocular. In *Proc. Int. Conf. Biometrics (ICB)*, pages 143–150, 2015.

[67] K. B. Raja et al. Improving cross-smartphone periocular verification in visible spectrum using time-frequency features of laplacian decomposition. In *Proc. 11th Int. Conf. Signal-Image Technology Internet-Based Systems (SITIS)*, pages 576–582, 2015.

[68] M. Yamazaki et al. Sift-based algorithm for fingerprint authentication on smartphone. In *Proc. 6th Int Information and Communication Technology for Embedded Systems (IC-ICTES) Conf. of*, pages 1–5, 2015.

[69] Chandrasekhar Bhagavatula et al. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. *Proc. USEC*, 2015.

[70] H. Javidnia et al. Palmprint as a smartphone biometric. In *Proc. IEEE Int. Conf. Consumer Electronics (ICCE)*, pages 463–466, 2016.

[71] Xiangqian Wu et al. Fisherpalms based palmprint recognition. *Pattern recognition letters*, 24(15):2829–2838, 2003.

[72] Adams Kong et al. A survey of palmprint recognition. *Pattern Recognition*, 42(7):1408–1418, 2009.

[73] Dae Sik Jeong et al. *Iris Recognition in Mobile Phone Based on Adaptive Gabor Filter*, pages 457–463. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[74] Aaron Tilley. Samsung goes beyond the fingerprint with an iris scanner in the note 7. http://www.forbes.com/sites/aarontilley/2016/08/02/samsungs-note-7-iris-scanner/#69a119eb7355, August 2016.

[75] S. Bazrafkan et al. Finger vein biometric: Smartphone footprint prototype with vein map extraction using computational imaging techniques. In *Proc. IEEE Int. Conf. Consumer Electronics (ICCE)*, pages 512–513, 2016.

[76] Dal ho Cho et al. Pupil and iris localization for iris recognition in mobile phones. In *Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'06)*, pages 197–201, June 2006.

[77] Stan Kurkovsky et al. Experiments with simple iris recognition for mobile phones. *ITNG*, 10:1293–1294, 2010.

[78] N.L. Clarke and S.M. Furnell. Advanced user authentication for mobile devices. *Computers &amp; Security*, 26(2):109–119, 2007.

[79] K. B. Schaffer. Expanding continuous authentication with mobile devices. *Computer*, 48(11):92–95, 2015.

[80] Heather Crawford et al. A framework for continuous, transparent mobile device authentication. *Computers &amp; Security*, 39, Part B:127–136, 2013.

[81] R. Ferrero et al. On gait recognition with smartphone accelerometer. In *Proc. 4th Mediterranean Conf. Embedded Computing (MECO)*, pages 368–373, 2015.

[82] A. L. Fantana et al. Movement based biometric authentication with smartphones. In *Proc. Int Security Technology (ICCST) Carnahan Conf*, pages 235–239, 2015.

[83] A. Laghari et al. Biometric authentication technique using smartphone sensor. In *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pages 381–384, 2016.

[84] J. Guerra Casanova et al. *A Real-Time In-Air Signature Biometric Technique Using a Mobile Device Embedding an Accelerometer*, pages 497–503. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[85] P. Kartik et al. Multimodal biometric person authentication system using speech and signature features. In *TENCON 2008 - 2008 IEEE Region 10 Conference*, pages 1–6, Nov 2008.

[86] Indrajit Bhattacharya et al. Offline signature verification using pixel matching technique. *Procedia Technology*, 10:970 – 977, 2013.

[87] Alireza Sahami Shirazi et al. Assessing the vulnerability of magnetic gestural authentication to video-based shoulder surfing attacks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 2045–2048, New York, NY, USA, 2012. ACM.

[88] Feng Hong et al. Waving authentication: Your smartphone authenticate you on motion gesture. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '15, pages 263–266, New York, NY, USA, 2015. ACM.

[89] T. Feng et al. Investigating mobile device picking-up motion as a novel biometric modality. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*, pages 1–6, 2013.

[90] M. O. Derawi et al. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on*, pages 306–311, 2010.

[91] Liang Wang et al. Fusion of static and dynamic body biometrics for gait recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(2):149–158, Feb 2004.

[92] L. Middleton et al. A floor sensor system for gait recognition. In *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*, pages 171–176, Oct 2005.

[93] Gang Qian et al. *People Identification Using Gait Via Floor Pressure Sensing and Analysis*, pages 83–98. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[94] D. Gafurov et al. Gait authentication and identification using wearable accelerometer sensor. In *Automatic Identification Advanced Technologies, 2007 IEEE Workshop on*, pages 220–225, June 2007.

[95] C. Nickel et al. Authentication of smartphone users based on the way they walk using k-nn algorithm. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on*, pages 16–20, 2012.

[96] Thang Hoang et al. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *International Journal of Information Security*, 14(6):549, 2015.

[97] Elena Vildjiounaite et al. *Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices*, pages 187–201. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[98] C. Nickel and C. Busch. Classifying accelerometer data via hidden markov models to authenticate people by the way they walk. *IEEE Aerospace and Electronic Systems Magazine*, 28(10):29–35, Oct 2013.

[99] M. Karnan et al. Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*, 11(2):1565–1573, 2011. The Impact of Soft Computing for the Progress of Artificial Intelligence.

[100] Baljit Saini et al. Keystroke dynamics for mobile phones: A survey. *Indian Journal of Science and Technology*, 9(6), 2016.

[101] Fabian Monrose and Aviel D. Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 16(4):351–359, 2000.

[102] Rick Joyce and Gopal Gupta. Identity authentication based on keystroke latencies. *Commun. ACM*, 33(2):168–176, February 1990.

[103] Valeriu-Daniel Stanciu et al. On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks. In *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, CODASPY '16, pages 105–112, New York, NY, USA, 2016. ACM.

[104] Z. Sitová et al. Hmog: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security*, 11(5):877–892, 2016.

[105] I. V. McLoughlin and M. s. Naransamy. Keypress biometrics for user validation in mobile consumer devices. In *2009 IEEE 13th International Symposium on Consumer Electronics*, pages 280–284, May 2009.

[106] Saira Zahid et al. *Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23-25, 2009. Proceedings*, chapter Keystroke-Based User Identification on Smart Phones, pages 224–243. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[107] E. V. Cunha Urtiga and E. D. Moreno. Keystroke-based biometric authentication in mobile devices. *IEEE Latin America Transactions*, 9(3):368–375, 2011.

[108] Seong seob Hwang et al. Keystroke dynamics-based authentication for mobile devices. *Computers &amp; Security*, 28(12):85–93, 2009.

[109] J. S. Wu et al. Smartphone continuous authentication based on keystroke and gesture profiling. In *Proc. Int Security Technology (ICCST) Carnahan Conf*, pages 191–197, 2015.

[110] Cristiano Giuffrida et al. *Detection of Intrusions and Malware, and Vulnerability Assessment: 11th International Conference, DIMVA 2014, Egham, UK, July 10-11, 2014. Proceedings*, chapter I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics, pages 92–111. Springer International Publishing, 2014.

[111] Global touch-screen panel shipments to double by 2016, ihs analyst announces at sid. https://technology.ihs.com/435487/global-touch-screen-panel-shipments-to-double-by-2016-ihs-analyst-announces-at-sid, May 2013.

[112] Rich Brown. Touchscreen refrigerators and talking everything at ces 2016. http://www.cnet.com/news/touchscreen-refrigerators-and-talking-everything-at-ces-2016/, January 2016.

[113] S. Mondal and P. Bours. Swipe gesture based continuous authentication for mobile devices. In *2015 International Conference on Biometrics (ICB)*, pages 458–465, 2015.

[114] S. Mondal and P. Bours. Continuous authentication and identification for mobile devices: Combining security and forensics. In *Information Forensics and Security (WIFS), 2015 IEEE International Workshop on*, pages 1–6, 2015.

[115] Takumi Nohara and Ryuya Uda. Personal identification by flick input using self-organizing maps with acceleration sensor and gyroscope. In *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication*, IMCOM '16, pages 58:1–58:6, New York, NY, USA, 2016. ACM.

[116] C. C. Lin et al. A new non-intrusive authentication method based on the orientation sensor for smartphone users. In *Software Security and Reliability (SERE), 2012 IEEE Sixth International Conference on*, pages 245–252, 2012.

[117] L. Lu and Y. Liu. Safeguard: User reauthentication on smartphones via behavioral biometrics. *IEEE Transactions on Computational Social Systems*, 2(3):53–64, 2015.

[118] Fawaz A. Alsulaiman et al. *Haptics: Perception, Devices and Scenarios: 6th International Conference, EuroHaptics 2008 Madrid, Spain, June 10-13, 2008 Proceedings*, chapter User Identification Based on Handwritten Signatures with Haptic Information, pages 114–121. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[119] Ankita Jain and Vivek Kanhangad. Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures. *Pattern Recognition Letters*, 68, Part 2:351–360, 2015. Special Issue on Soft Biometrics.

[120] D. H. Shih et al. A flick biometric authentication mechanism on mobile devices. In *Proc. Int Informative and Cybernetics for Computational Social Systems (ICCSS) Conf*, pages 31–33, 2015.

[121] H. Saevanee and P. Bhatarakosol. User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device. In *Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on*, pages 82–86, 2008.

[122] Hui Xu et al. Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. In *Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 187–198, 2014.

[123] Liang Cai and Hao Chen. Touchlogger: Inferring keystrokes on touch screen from smartphone motion. *HotSec*, 11:9–9, 2011.

[124] K. W. Nixon et al. Slowmo - enhancing mobile gesture-based authentication schemes via sampling rate optimization. In *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 462–467, 2016.

[125] J. Nader et al. Designing touch-based hybrid authentication method for smartphones. *Procedia Computer Science*, 70:198–204, 2015. Proceedings of the 4th International Conference on Eco-friendly Computing and Communication Systems.

[126] Margit Antal and Lszl Zsolt Szab. Biometric authentication based on touchscreen swipe patterns. *Procedia Technology*, 22:862 – 869, 2016.

[127] Oscar Miguel-Hurtado et al. Predicting sex as a soft-biometrics from device interaction swipe gestures. *Pattern Recognition Letters*, 79:44–51, 2016.

[128] Chris Bevan and Danaë Stanton Fraser. Different strokes for different folks? revealing the physical characteristics of smartphone users from their swipe gestures. *International Journal of Human-Computer Studies*, 88:51–61, 2016.

[129] Shiri Azenkot et al. Passchords: Secure multi-touch authentication for blind people. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility*, pages 159–166. ACM, 2012.

[130] V. Zaliva et al. Passive user identification using sequential analysis of proximity information in touchscreen usage patterns. In *Mobile Computing and Ubiquitous Networking (ICMU), 2015 Eighth International Conference on*, pages 161–166, 2015.

[131] A. Primo and V. V. Phoha. Music and images as contexts in a context-aware touch-based authentication system. In *Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on*, pages 1–7, 2015.

[132] Tao Feng et al. Tips: Context-aware implicit user identification using touch screen in uncontrolled environments. In *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*, pages 9:1–9:6. ACM, 2014.

[133] C. Shen et al. Performance analysis of touch-interaction behavior for active smartphone authentication. *IEEE Transactions on Information Forensics and Security*, 11(3):498–513, 2016.

[134] Hassan Khan et al. Itus: An implicit authentication framework for android. In *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking*, pages 507–518. ACM, 2014.

[135] N. Zheng et al. You are how you touch: User verification on smartphones via tapping behaviors. In *2014 IEEE 22nd International Conference on Network Protocols*, pages 221–232, 2014.

[136] Z. Syed et al. Effect of user posture and device size on the performance of touch-based authentication systems. In *Proc. IEEE 16th Int. Symp. High Assurance Systems Engineering*, pages 10–17, 2015.

[137] Speaker recognition. http://www.biometric-solutions.com/solutions/index.php?story=speaker_recognition.

[138] B. S. Atal. Effectiveness of linear prediction characteristics of the speech wave for automatic speaker identification and verification. *The Journal of the Acoustical Society of America*, 55(6):1304–1312, 1974.

[139] Douglas A. Reynolds. Overview of automatic speaker recognition. http://147.229.9.23/study/courses/SRE/public/prednasky/2009-10/07_spkid_doug/sid_tutorial.pdf, 2008.

[140] Tomi Kinnunen and Haizhou Li. An overview of text-independent speaker recognition: From features to supervectors. *Speech Communication*, 52(1):12 – 40, 2010.

[141] Kevin Peachey. Banks turning to voice recognition. http://www.bbc.com/news/business-36939709, August 2016.

[142] Elena Vildjiounaite et al. Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices. In *International Conference on Pervasive Computing*, pages 187–201. Springer, 2006.

[143] D. J. Kim et al. Person authentication using face, teeth and voice modalities for mobile device security. *IEEE Transactions on Consumer Electronics*, 56(4):2678–2685, 2010.

[144] H. A. Shabeer and P. Suganthi. Mobile phones security using biometrics. In *Proc. Int Conf. Computational Intelligence and Multimedia Applications Conf*, volume 4, pages 270–274, 2007.

[145] W. Shi et al. Senguard: Passive user identification on smartphones using multiple sensors. In *2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 141–148, 2011.

[146] Attaullah Buriro et al. Itsme: Multi-modal and unobtrusive behavioural user authentication for smartphones. *Technology and Practice of Passwords*, 2016.

[147] Y. Tang et al. User authentication on smart phones using a data mining method. In *Proc. Int Information Society (i-Society) Conf*, pages 173–178, 2010.

[148] R. Kobayashi and R. S. Yamaguchi. A behavior authentication method using wi-fi bssids around smartphone carried by a user. In *Proc. Third Int. Symp. Computing and Networking (CANDAR)*, pages 463–469. Institute of Electrical and Electronics Engineers (IEEE), December 2015.

[149] Tempestt Neal, Damon Woodard, and Aaron Striegel. *Mobile Biometrics*, chapter Mobile Device Usage Data as Behavioral Biometrics. The Institution of Engineering and Technology, to be published.

[150] Devasis Bassu et al. A new mobile biometric based upon usage context. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 441–446. IEEE, 2013.

[151] Andrew S Branscomb. Behaviorally identifying smartphone users. 2013.

[152] T. J. Neal, D. L. Woodard, and A. D. Striegel. Mobile device application, bluetooth, and wi-fi usage data as behavioral biometric traits. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–6, Sept 2015.

[153] L. Fridman et al. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal*, PP(99):1–9, 2016.

[154] Marcelo Luiz Brocardo et al. Authorship verification for short messages using stylometry. In *Computer, Information and Telecommunication Systems (CITS), 2013 International Conference on*, pages 1–6. IEEE, 2013.

[155] Huanhuan Cao et al. An effective approach for mining mobile user habits. In *Proceedings of the 19th ACM International Conference on Information and Knowledge Management*, CIKM '10, pages 1677–1680, New York, NY, USA, 2010. ACM.

[156] Julian Seifert et al. Treasurephone: Context-sensitive user data protection on mobile phones. In *Pervasive Computing*, pages 130–137. Springer, 2010.

[157] Ling Pei et al. Human behavior cognition using smartphone sensors. *Sensors*, 13(2):1402–1424, 2013.

[158] Jae-wook Jang et al. Andro-profiler: Anti-malware system based on behavior profiling of mobile malware. In *Proceedings of the 23rd International Conference on World Wide Web*, WWW '14 Companion, pages 737–738, New York, NY, USA, 2014. ACM.

[159] S. Mondal and P. Bours. Does context matter for the performance of continuous authentication biometric systems? an empirical study on mobile device. In *Proc. Int Biometrics Special Interest Group (BIOSIG) Conf. of the*, pages 1–5, 2015.

[160] P. Kasprowski and I. Rigas. The influence of dataset quality on the results of behavioral biometric experiments. In *Proc. Int Biometrics Special Interest Group (BIOSIG) Conf. of the*, pages 1–8, 2013.

[161] Hassan Khan et al. *A Comparative Evaluation of Implicit Authentication Schemes*, pages 255–275. Springer International Publishing, Cham, 2014.

[162] Mikhail I. Gofman and Sinjini Mitra. Multimodal biometrics for enhanced mobile device security. *Commun. ACM*, 59(4):58–65, 2016.

[163] A. K. Jain et al. Biometrics: a tool for information security. *IEEE Transactions on Information Forensics and Security*, 1(2):125–143, 2006.

[164] F. Rahman et al. Seeing beyond visibility: A four way fusion of user authentication for efficient usable security on mobile devices. In *Proc. IEEE Eighth Int Software Security and Reliability-Companion (SERE-C) Conf*, pages 121–129, 2014.

[165] Andrew C. Morris et al. Multimodal person authentication on a smartphone under realistic conditions, 2006.

[166] K. B. Raja et al. Fusion of face and periocular information for improved authentication on smartphones. In *Proc. 18th Int Information Fusion (Fusion) Conf*, pages 2115–2120, 2015.

[167] Mohamed Khamis et al. Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '16, pages 2156–2164, New York, NY, USA, 2016. ACM.

[168] Hataichanok Saevanee et al. Continuous user authentication using multi-modal biometrics. *Computers &amp; Security*, 53:234–246, 2015.

[169] S. Sarkar et al. Deep feature-based face detection on mobile devices. In *2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, pages 1–8, February 2016.

[170] R. Raghavendra et al. Scaling-robust fingerprint verification with smartphone camera in real-life scenarios. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*, pages 1–8, Sept 2013.

[171] Yufei Han et al. *Embedded Palmprint Recognition System on Mobile Devices*, pages 1184–1193. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[172] J. R. Kwapisz et al. Cell phone-based biometric identification. In *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on*, pages 1–7, 2010.

[173] T. Feng et al. Continuous mobile authentication using touchscreen gestures. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 451–456, 2012.

[174] Zhongmin Cai et al. *Mobile Authentication through Touch-Behavior Features*, pages 386–393. Springer International Publishing, Cham, 2013.

[175] Young-Hoo Jo et al. Security analysis and improvement of fingerprint authentication for smartphones. *Mobile Information Systems*, 2016, 2016.

[176] M. R. Zafar and M. Ali Shah. Fingerprint authentication and security risks in smart devices. In *2016 22nd International Conference on Automation and Computing (ICAC)*, pages 548–553, Sept 2016.

[177] Esteban Vazquez-Fernandez and Daniel Gonzalez-Jimenez. Face recognition for authentication on mobile devices. *Image and Vision Computing*, 55, Part 1:31 – 33, 2016. Recognizing future hot topics and hard problems in biometrics research.

[178] K. Nandakumar and A. K. Jain. Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine*, 32(5):88–100, Sept 2015.

[179] Y.J. Chin, T.S. Ong, A.B.J. Teoh, and K.O.M. Goh. Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. *Information Fusion*, 18:161 – 174, 2014.

[180] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. *EURASIP J. Adv. Signal Process*, 2008:113:1–113:17, January 2008.

[181] Padma Polash Paul and Marina Gavrilova. Cancelable biometrics: Securing biometric face template. *IJAIT*, 4(1):25–34, 2012.

[182] V. G. Supriya and R. Manjunatha. Design and analysis of secured, revocable iris based biometrics authentication system. In *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, pages 314–319, Feb 2016.

[183] Shijun Zhao, Qianying Zhang, Guangyao Hu, Yu Qin, and Dengguo Feng. Providing root of trust for arm trustzone using on-chip sram. In *Proceedings of the 4th International Workshop on Trustworthy Embedded Devices*, TrustED '14, pages 25–36, New York, NY, USA, 2014. ACM.

[184] Dongli Zhang. Trustfa: Trustzone-assisted facial authentication on smartphone.

[185] Greig Paul and James Irvine. Fingerprint authentication is here, but are we ready for what it brings?

[186] Windsor Holden. Securing public faith in biometrics. *Biometric Technology Today*, 2016(9):7 – 9, 2016.

[187] Tarjei Mandt, Mathew Solnik, and David Wang. Demystifying the secure enclave processor.

[188] Anil K. Jain et al. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79:80 – 105, 2016.

[189] Whither Biometrics Committee et al. *Biometric recognition: challenges and opportunities.* National Academies Press, 2010.

[190] Arun Ramakrishnan et al. Prism: Policy-driven risk-based implicit locking for improving the security of mobile end-user devices. In *Proceedings of the 13^{th} International Conference on Advances in Mobile Computing and Multimedia*, pages 365–374. ACM, 2015.

[191] Eiji Hayashi et al. Goldilocks and the two mobile devices: Going beyond all-or-nothing access to a device's applications. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 2:1–2:11, New York, NY, USA, 2012. ACM.