Chapter 16
Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues

Reham Amin, Tarek Gaber, Ghada ElTaweel and Aboul Ella Hassanien

Abstract Currently, mobile smartphone devices contain a critical and sensitive data. In addition, they provide access to other data, on cloud for example, and to services somewhere on the Internet. Mobile authentication aims to protect against unauthorized access. The current operating systems of mobile smart phones offer different authentication mechanisms. Nonetheless, in some situations, these mechanisms are vulnerable and in other situations, they are not user friendly enough, thus not widely adopted. In this chapter, we will give an overview of the current mobile authentication mechanisms: traditional and biometric, and their most commonly used techniques in the mobile authentication environment. In addition, the pro and cons of these techniques will be highlighted. Moreover, a comparison among these techniques will be conducted. The chapter also discuss the other techniques which could much suitable for the current environment of the mobile applications. Furthermore, it discuss a number of open issues of the mobile authentication which needs further research in the future to improve the adoption of the biometric authentication in the smartphones environment.

16.1 Introduction

Mobiles are considered the largest market portion. Mobile phone has become incredible device which can be used for various tasks including telephony, multi-networking, entertainment, business functions, computing and multimedia. In other words, mobile

R. Amin · T. Gaber (✉) · G. ElTaweel
Faculty of Computers and Informatics, Suez Canal University, Ismailia, Egypt
e-mail: tarekgaber@ci.suez.edu.eg

A. E. Hassanien
Faculty of Computers and Information Science, Cairo University, Cairo, Egypt

T. Gaber · A. E. Hassanien
Scientific Research Group in Egypt (SRGE), Cairo, Egypt

A. E. Hassanien et al. (eds.), *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*, Intelligent Systems Reference Library 70,
DOI: 10.1007/978-3-662-43616-5_16,

devices are being used worldwide, not only for communication purposes, but also for personal affairs and for processing information obtained anywhere at any time. Tesng et al. in [1], have reported that more than 4 billion users are using mobile phones around the world. They also expected that by 2015, around 86 % of the world population would own at least one mobile phone.

Most of mobile phones are currently embedded with digital imaging and sensing softwares. Examples of these sensors include voice sensors (microphones), GPS sensors, optical/electrical/magnetic sensors, temperature sensors and acceleration sensors. Such sensing softwares have many applications including medical diagnostics, e.g. heart monitoring, temperature measurement, hearing and vision tests, thus helping in the improvement of the health care [2].

Due the high capabilities of mobile phones, they had confirmed themselves to be highly attractive aims for theft. This theft is usually not only because of the mobile cost but also because of gaining access to the owner's information. For instance, steal owner's identity to buy goods online at the owner expense or to explore new functionality are considered the prime motivations for theft [3].

How precious your phone is not only depending on its price or new technology added to it but also on the information saved on it. Examples of this information include some information related to your work, to your online banking, or your health case. Such information is considered much important than the mobile itself. Therefore, it is a crucial mission to protect the way to access the mobile. Mobile authentication is the first step to protect mobile's access. It could be seen as a gateway to get access to a mobile. The main aim of the authentication technique is addressing the question: "How user proves to device that he is who is claimed to be?".

There are two major categories of authentications: *traditional and biometric*. A summary of these two categories are shown in Fig. 16.1. The more easy to use the authentication method, the more attractive the method will be to the user. However, the user attractiveness is not only the accurate proof of the method's efficiency but also there are other factors to evaluate the authentication method.

In this chapter, we will give an overview of the current mobile authentication mechanisms: traditional and biometric, and their most commonly used techniques in the mobile authentication environment. It will also conduct a comparison between these common techniques and highlight some open issues to improve the usability and security of the authentication systems to suit the mobile constraints. The rest of the chapter is divided into four sections. Section 16.2 introduces the traditional authentication techniques while Sect. 16.3 presents overview of the biometric authentication system then reviews the most commonly used biometrics which is divided into physiological and behavioral biometric techniques. Section 16.4 presents the difference between the traditional and the biometric authentication techniques. Section 16.5 gives a comparison between the various authentication techniques. Section 16.6 presents the comparison between the explicit and implicit authentication techniques. Section 16.7 gives some open points for further search and finally Sect. 16.8 concludes the overall chapter.

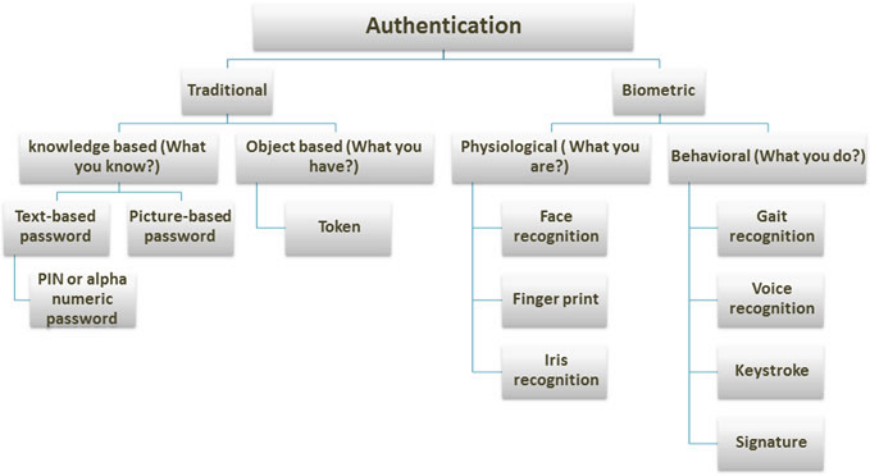

Fig. 16.1 Classification of authentication techniques

16.2 Traditional Authentication Methods

Traditionally, authentication methods are either knowledge-based or object-based authentication [4, 5]. Knowledge-based method depends on what user already knows, whereas object-based method depends on what user already has. In the next sections, an overview of these two classes is given.

16.2.1 Knowledge-Based Authentication

Knowledge-based techniques are the most common used authentication techniques. They are based on "What user knows?" to identify his/her. They include two classes: text-based and picture-based passwords [6].

Text-based password Text-based password includes Personal Identification Numbers (PINs), Personal Unblocking Key (PUK), and alpha numeric password. The most widely known is the PIN. Upon switch-on the mobile device, a user is asked to enter the correct 4–8 digit PIN [5, 7].

PIN is also used to protect the SIM card. After 3 failed attempts to enter the PIN, the SIM locks out and the PUK (PIN Unlock) is then requested. If the PUK is also falsely inputted for 10 times, the SIM becomes useless [8]. PIN achieved probability of as low as 10^{-n} to accept imposters falsely, where 10 is the range of numbers from 0 to 9 that could be used for PIN and n is the length of the PIN digits [9].

Another advance to the text-based password was to use the *alphanumeric password*. This makes password more difficult to guess and maximize the probability to

accept imposters. This enhances the quality of PIN by using Non-Dictionary words to avoid risk of dictionary based attacks. However alphanumeric password could be violated by the brute-force approach (testing every combination of characters for every length of password). One solution to this problem was to use passwords that mixed between case/symbols or the Password ageing to change password regularly [7]. Nonetheless, this technique suffers from the following problems:

- The memory load to remember
- Shoulder surfing attack
- Reusing of the same password for multiple accounts
- Disturbing user with frequently entering
- Writing password down
- Need for additional customer service with the incorrect PUK code.

These problems push people to use weak passwords or irregularly change them or never use any password at all. In addition, password isn't actually representing its owner. This makes theft of owner's identity is much easier. Although the previously mentioned password problems, password authentication method has a good advantage over the other methods. It can be changed anytime [10].

Picture-based passwords The main problem with PIN was a memorization. To address this problem, Graphical Password was suggested. This method is based on the fact that people are easily remember images than strings. Graphical Password (GP) was originally introduced by Greg Blonder in 1996 [11]. There are three ways to implement it. It could be implemented by drawing curve connecting selected picture or by selecting some specific images or by pointing to points at some image.

Gao et al. [12] proposed authentication system by drawing a curve to connect specific degraded pictures. These pictures make a story for the user, thus enabling him to easily remember the password. For example, "mom and dad takes baby to doctor to get medicine" is password. Although the system is resistant against shoulder surfing, it takes time from user to login or differentiate the degraded pictures. According to user behavior: this method starts and ends with random pictures which could be forget by users at the first stage.

Khan et al. [6] presented a hybrid technique which combines recognition (select specific symbols) and recall (try to redraw selected symbol on screen). Firstly, a user has to enter username and password. Secondly, the user has to select at minimum 3 symbols using recognition. Then, the user draws these symbols on touch screen using recall by stylus or pen which is needed to get access. Then, a processing of the drawn symbol by normalization, noise removal, and other operations, e.g. feature extraction and hierarchial matching are performed. The feature extraction is used to extract (hyper stroke, bi-stroke and stroke) features while the hierarchical matching is used to check that the user has drawn objects by the same order during the selection stage. This method is illustrated at Fig. 16.2.

This technique makes hacking more difficult as the user not only enters a username/select symbol but also draws the object. However entering a username and a password are still related with the password problems mentioned above. In addition,

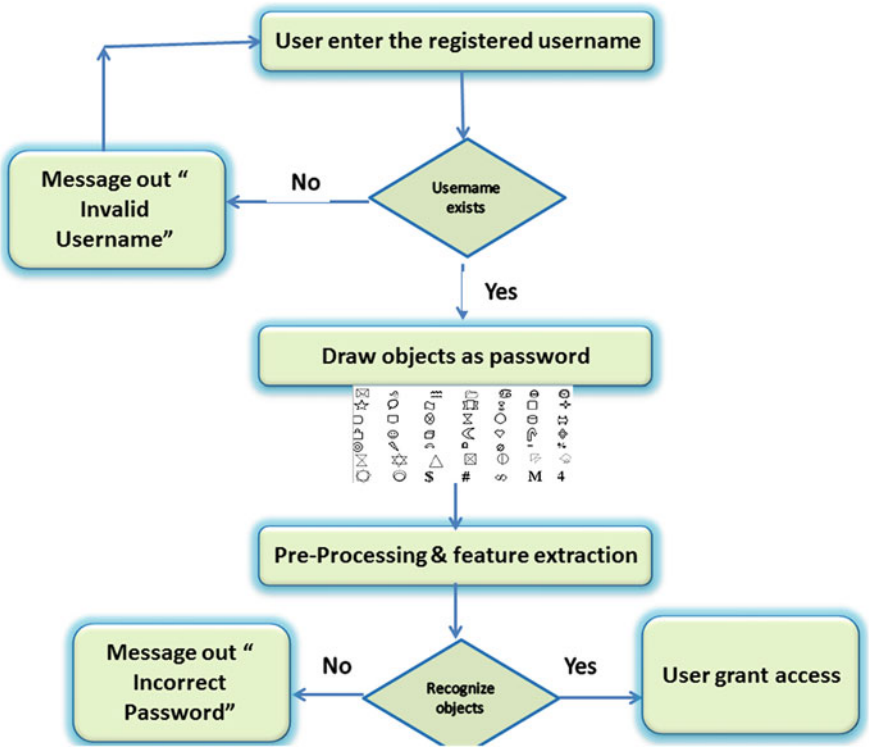

Fig. 16.2 Authentication phase for graphical password

it takes time to perform preprocessing on the drawn image and the other operations used to compare the drawn and stored objects. Moreover, when the user uses different hand for drawing, symbol differs, this is another problem.

16.2.2 Object-Based Authentication

Using passwords is the easiest authentication methods to access all mobile's data. However, as shown above, it is subject a number of problems. To avoid these problems, object-based authentication techniques were developed as a second factor for authentication besides password. These techniques include tokens-based authentication. The tokens are physical devices storing passwords. Examples of tokens include driver license and remote garage door opener [13].

Using token for authentication means that a user deals with some hardware to carry out the authentication process. This hardware contains software programs that implement a One-Time Password (OTP) algorithm to provide changed-over-time

PIN (random password) which is synchronized with a server [14]. Seed value of the PIN and a timestamp are given to a token algorithm to make predicting the random password more difficult to attackers [15].

For example, in order for a user access to his bank account through his credit card (token), he must first enter his username and corresponding password [6].

In mobile's environment, a SIM card is considered as an authentication token for a network subscribers. Every SIM consists of two unique identifiers: *IMSI* and *Ki*. *IMSI* (International Mobile Subscriber Identity) is 15 digits that uniquely identify mobile subscriber. *Ki* (Individual subscriber authentication Key) is a random number of 128-bits which is cryptographic key to be used to generate session keys. These identifiers are used to uniquely identify a legitimate user [8]. The secrecy of both *IMSI* and *Ki* provides authentication of the user's data. SIM-based authentication enables a user to subscribe with a network. Nonetheless, it doesn't check whether the mobile's user is the registered subscriber or not [16].

In general, tokens are more efficient than passwords as with them it is very difficult for an attacker to guess or remember tokens. However, the tokens-based authentication suffer from the following problems/limitations [15, 16]:

1. Additional cost comes from manufacturing/maintenance and installation/deploying for both the hardware and software.
2. Need for high computation in the poor constrained mobiles.
3. Effort to manage.
4. Possibility to be lost or stolen.
5. User has to hold or wear the token.

Clarke et al. [16] proposed a system which accommodates the above problems by developing tokens that authenticate users through using the wireless connection provided by mobiles. So that, tokens do not require passwords to be physically stored at a server synchronized with the token. These tokens could be worn like jewelry. However, at most cases mobiles are used as a stand-alone OTP Token [17, 18].

16.3 Biometric Authentication Techniques

The word biometrics comes from two ancient Greek words: bios = "life" and metron = "measure" [6]. In Paris, in the 19th century, Alphonse Bertillon, who worked as a chief of the criminal identification division of the police department, practiced the usage of body properties (biometrics) (e.g. fingers, height, or feet) to identify criminals. He also discovered the uniqueness of human fingerprints. Soon after this discovery, police started to save criminals fingerprints using card files. Later, police started to lift fingerprints from crime scenes and compare it with the stored ones to know criminals identities. Since then, biometrics has become a subject of interest in many areas for personal recognition such as: authentication in sensitive jobs such as people working at national security organization [19]. In the following sections, an overview of biometric authentication and its types are presented.

16.3.1 Biometric Authentication and Its Types

As explained in Sect. 16.2, the traditional techniques do not actually represent users. On the other hand, biometric authentication techniques depends on the users' unique features to identify the users [20]. The biometric authentication is a process in which a user is recognized automatically based on a feature vector extracted from his physiological or behavioral characteristics. Based on this, biometric methods are typically categorized into two types: physiological and behavioral. Physiological biometrics depends on physical attributes of a person such as what user already has (e.g. face, fingerprint or hand). Generally, it is based on the fact that these person's attributes do not change over time. Conversely, behavioral biometrics depends on an associated behavior of a person such that what user does (e.g. how a person writes or speaks) [16]. This behavior is recorded in a period of time while the person is doing his job from his temporal trait [21].

The main difference between the physiological and the behavioral biometrics is that the latter is more difficult to detect and emulate because it depends on an interaction of users with their own devices to extract specific and accurate habits. A detailed information about physiological and behavioral biometrics is given below.

16.3.2 Components of a Typical Biometric System

A typical biometric authentication system consists of five modules/components which are shown in Fig. 16.3.

- Sensor module: It is used to capture user's raw biometric data. An example is camera used to take a picture of human face.
- Feature extraction module: It is used to process the acquired biometric data to extract a set of features. For example, features on the surface of a face, such as the contour of the eye sockets, nose, and chin can be extracted.
- Matcher module: It is used to compute matching scores of comparing the extracted features against the stored ones.
- System database module: It is used to store the biometric templates of features the enrolled users [21].
- Decision-making module: It is used to either determine the user's identity or confirm the users claimed identity [22].

16.3.3 How Biometric Authentication Works?

Biometric system depends on comparing the recent feature set against the set stored in a database. It works in two stages: enrollment and recognition (verification or identification) [23].

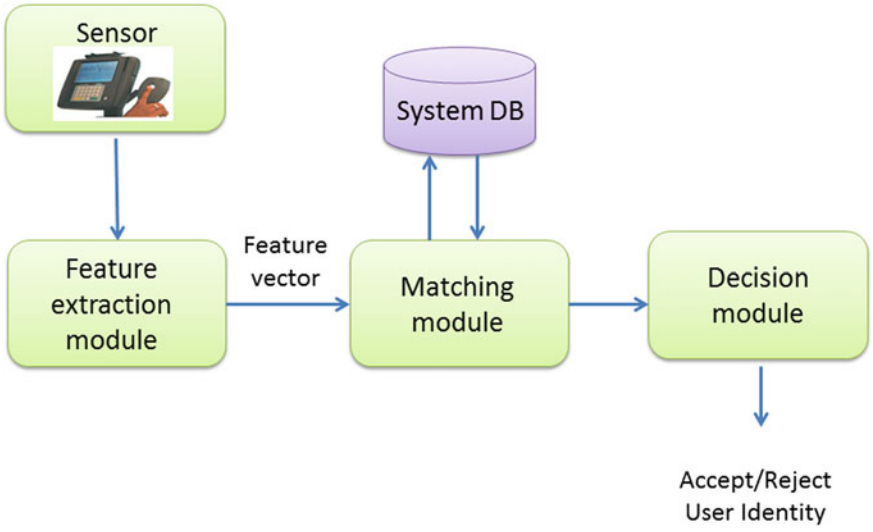

Fig. 16.3 Biometric modules

In the enrollment stage, a set of feature is extracted from the raw biometric template and then is stored in a database [24]. Along with some biographic information (e.g. name or PIN) which describing the user can be possibly stored with the feature set. The user's template can be extracted from either a single biometric or multiple samples. Thus, multiple samples of an individual's face, captured from different poses with respect to the camera generate the user's template.

In the recognition stage, an individual is verified whether he/she was really enrolled in the system. Depending on the application context, the recognition process can be achieved either in identification mode or in verification mode. With the identification mode, as seen in Fig. 16.4), a user does not claim his/her identity but the system searches all stored templates for all enrolled users in the database for a positive match. This means that the identification mode conducts a one-to-many comparison between the given user's template and the stored templates in the database [21].

In the verification mode, as shown in Fig. 16.5, a user first claims an identity, usually by entering a PIN, and then the system confirms whether this user is the one who has just claimed the identity corresponding to the PIN [21, 25]. Unlike the identification mode, the verification one performs a one-to-one comparison between a live biometric template (just built by the system) and the retrieved one from the database [24].

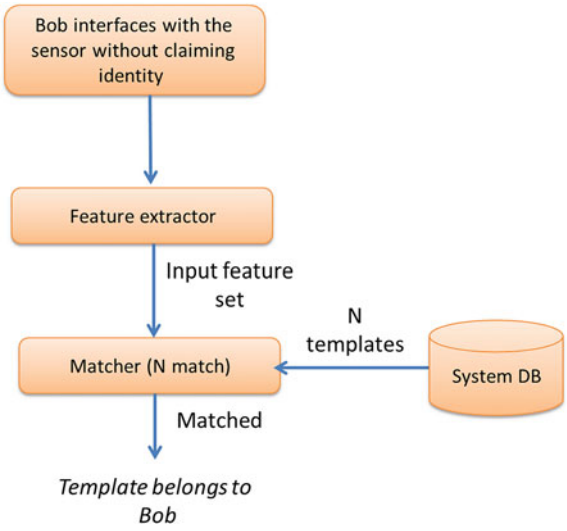

Fig. 16.4 Identification stage

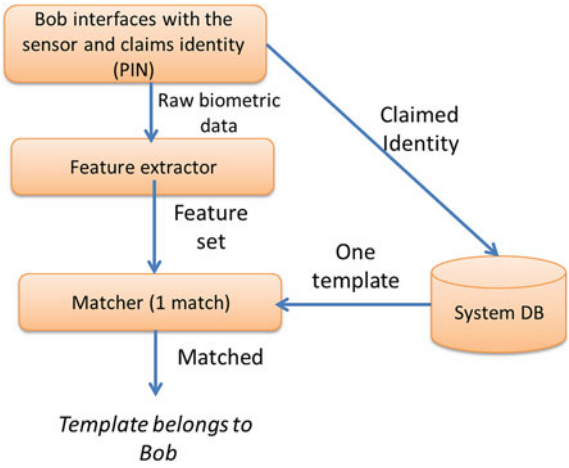

Fig. 16.5 Verification stage

16.3.4 Performance Evaluation of Biometric Authentication

The most widely used method to evaluate the performance of biometric systems include False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Rate (EER) (defined in ISO/IEC FDIS 19795-1). The FAR means the probability of accepting an impostor falsely, while the FRR means the probability of rejecting a rightful owner falsely. These probabilities depend on a predefined threshold which determines when the system accepts or rejects a user. However, the value of this threshold could affect the overall result of accepting or rejecting users. In case, a low threshold value is used, the system could output a high FAR value. In case, a high threshold value is

used, the system could result in a high FRR value. Generally speaking, decreasing the FRR increases the FAR and vice versa. To achieve a tradeoff between the two cases, EER (Equal Error Rate) is employed to get the intersection of the values of FRR and FAR [26].

16.3.5 Physiological Biometrics

The first type of the biometric authentication approaches is the physiological which depends on what a user already owns. There are many physiological techniques including face, fingerprint, iris hand vascular, palm-print, and hand or ear geometry recognition. Due to usability and hardware constraints, not all of these biometric methods are suited for mobiles. Such methods include hand vascular, palm-print, and hand or ear geometry recognition [5, 27]. Below, we will give a review of most common biometric techniques used in mobile authentication.

Face Recognition Face recognition method is the one in which a human face is captured using a mobile's camera then this face is used to authenticate this human to the mobile. The face recognition authentication makes use one of two ways: (1) shape and location of facial properties such as the eyes, nose, lips and their spatial relationships, or (2) the overall face image [21]. Tao et al. [9] have developed a biometric system using a user's mobile camera which takes 2D face image to ensure the existence of user. This authentication system consists of five modules: *face detection, face registration, illumination normalization, face authentication and information fusion*.

The mobile camera first takes a sequence of images for the user and then processes them at the mobile's processor. Face detection then specifies the location of face in the self-taken photos. Face registration then identifies the face by localizing face attributes which are also saved in the database. Illumination normalization is a pre-processing step which is needed to eliminate an illumination causing a variability of the face images. This is done by noise removal techniques. Face verification is then invoked to match the most recent captured image with the one stored in the database. Information fusions is finally called by using different frames (calculating the Mahalanobis distance) to improve the system reliability and performance. A summary of this system is illustrated in Fig. 16.6.

The authentication-based face recognition confirms the physical presence of the user. In addition, it reduces the cost of getting tokens since the mobile's camera is already embedded in the mobile and can be used to capture the human face. However, this method suffers from a number of limitations. The human face changes over time or may get injured. Also, image capturing is subject to different lightning changes [28].

Fingerprint Fingerprint authentication is a method in which a user's fingerprint is scanned by a mobile's fingerprint sensor to check an identity of a mobile's user. This determines features such as pressure, the 3D shape of the contacted finger, ridges and

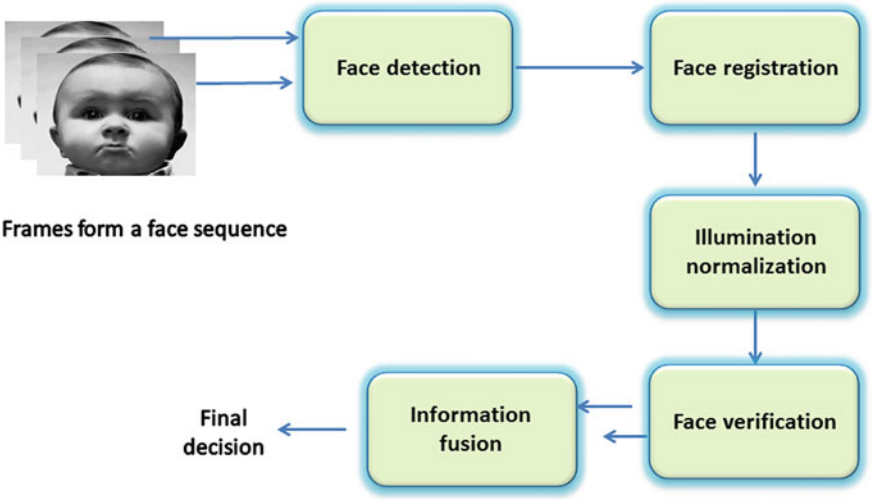

Fig. 16.6 Face recognition system [9]

valleys on the fingertip and other features [29]. Khan et al. [30] proposed two factor authentication system including fingerprint as one factor. This system identifies the user by sensing the ridges and furrows on the user's fingers. This scheme is composed of four phases: registration, login, authentication, and password change phase. In the registration phase, a user submits two types of information: his ID and password, and his fingerprint by the sensor included in the mobile. In the login phase, the user opens the login window to enter his ID and password and then imprints his fingerprint by the sensor. The mobile then verifies the user's fingerprint. If it is valid, the mobile sends the entered ID and password to a remote server. In the authentication phase, the remote server validate the message received. In the password change phase, when the user wants to change his old password, the user has to firstly login with his old password and his fingerprint. Then, the user is allowed to change his password.

As reported in [19], attacking applications with biometric-based authentications shows a much smaller risk comparing with attacking applications with password-based authentications. However, this method is subject to a number of problems to extract the accurate fingerprint information. The human fingerprint is affected by genetic factors, hurtled fingers, and aging. Also the finger reader can not differentiate between the live and the severed finger [31].

Iris recognition This technique depends on scanning a human iris[1] by a separate camera or a mobile's camera [21, 27]. Lee et al. [32] have developed an automated iris recognition system. As shown in Fig. 16.7, this system composes of seven components: Image Acquisition, Segmentation, Normalization, Feature Extraction and Encode, and Similarity Matching Templates.

[1] The iris is the annular part of the eye bounded by the sclera and the pupil.

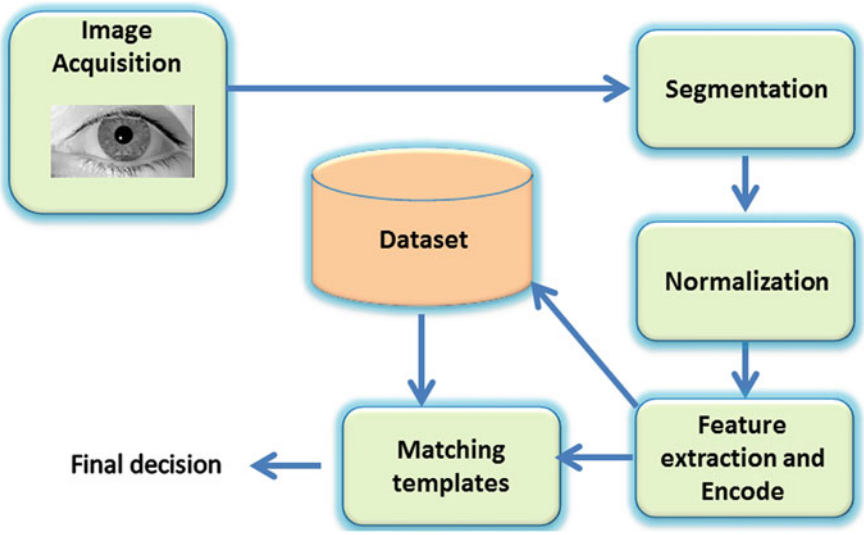

Fig. 16.7 Iris authentication system [32]

In the image acquisition, this system captures a sequence of images from a video frame for the same person using two different cameras at different positions. In segmentation phase, the iris region is isolated from eye images and the image with the best quality is chosen. In normalization phase, 2D representation of the iris pattern is constructed and the noise is removed by masking filters. In Feature Extraction and encode phase, both the edge and line features are extracted from the iris image. Edge features are compared with the intensities of eye regions and the region across the upper cheeks. Line features are compared with the intensities of eye regions and the nose. These features are filtered by classifiers (e.g. Wavelet Transform, Laplacian-of-Gaussian filter, Discrete Cosine Transform, etc.). Then, the iris image is encoded into binary format. In the similarity matching templates, Hamming Distance (HD) is computed between the two iris templates (the existing one and the recent generated one) to decide whether the iris pattern belongs to the same person or not.

Park et al. [33] proposed iris-based authentication system taking an iris image even if a user is wearing glasses by turning on/off the dual (left and right) infra-red (IR) illumination iteratively. Then, the system detects the occluded areas such as the eyelid, eyelash, and corneal specular reflections (SRs) which happen on surface of glasses. To detect the boundaries of the pupil and the iris, the Adaboost classifier was used. This classifier uses a one-step greedy strategy for a sequential learning method. Then, the iris code bits were extracted from the detected areas. The detected iris image was normalized and divided into rectangular polar coordinates (8 tracks and 256 sectors). Finally, the extracted iris code bits were compared to the enrolled template using the hamming distance (HD). If the calculated HD is higher than the specified threshold, the user was accepted. Otherwise user was rejected.

In contrast to face recognition which can be changed over time, the iris is stable. Also, compared to the fingerprint using a sensor which cannot differentiate between the live and the severed finger, the iris's sensor could ensure the live eye as it can measure the depressions and dilations of the pupil [19]. However, this technique takes a quite long time to authenticate a user. In addition, the eye's alignment and any eye's hurt affect the accuracy of users' authentication [16].

In general, we can conclude that the physical biometric authentication techniques suffer from the following problems [14, 29]:

- They require additional hardware (i.e. camera, finger print reader, etc.) which may be already available in mobiles.
- There is a cost for maintenance and the authentication failure.
- There is a high computation done in the poor constrained mobiles.
- A number of biometric identifiers are prone to wear and tear, accidental injuries, and pathophysiological development (accidents, manual work, etc.).
- They are not adaptable to people with disabilities (i.e. blind user can't use face recognition but may use voice biometric).

16.3.6 Behavioral Biometrics

In addition to the authentication techniques which is based on what a user has or knows. There are other techniques which identify users based on what they are usually doing in their own lives. Such techniques are known as *behavioral biometrics*. There are a number of behaviors which can be used to authenticate users. This includes gait, signature, keystroke, etc. Authentication techniques, based on these behaviors, are highlighted below.

Gait Recognition Gait is a behavioral biometric that uses a sequence of video images of a walking person to measure several movements to identify a mobile's user. Typically, shown in Fig. 16.8, gait recognition system consists of five stages: video capture, silhouette segmentation, contour detection, feature extraction and classification. Firstly, a video of a walking person is captured by a camera. Secondly, using some segmentation and motion detection methods, the person is segmented from the surrounding area. Thirdly, the contours of the person are detected to specify the outer boundary of human body [34]. Fourthly, gait features are then extracted. Finally, a classifier is used to identify a person. In the classification, the similarity between the extracted gait feature and the stored ones is computed to identify the walking person.

Derawi et al. [20] have proposed the gait authentication for mobile's user. They have used the low embedded accelerometers found at Google G1 phone. In this system, each volunteer placed a mobile device at his hip. When he walks while wearing his normal shoes, gait data is collected at each four walks (2 walking down and 2 walking back). To identify the person, background segmentation was used to isolate the person from the surrounding background. The first walk was stored as a reference template in a database whereas the others walks were used for extracting

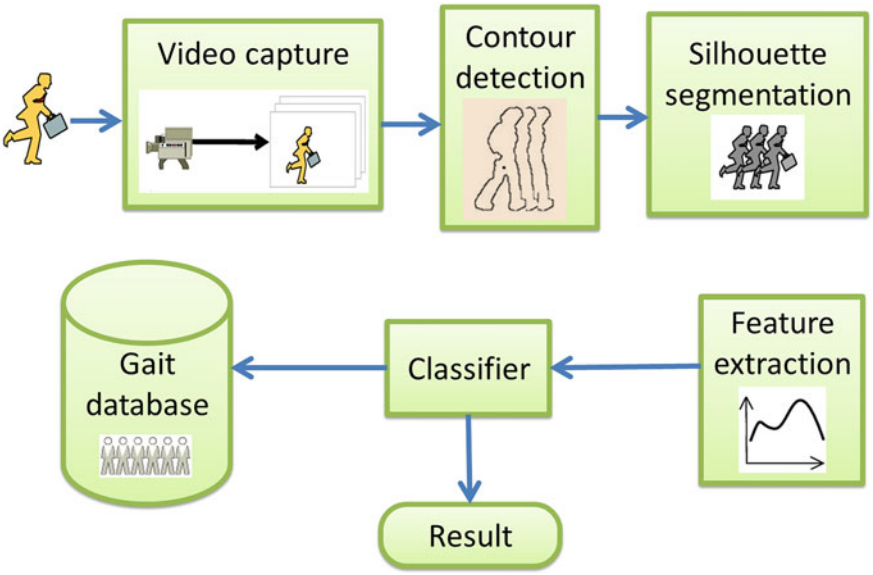

Fig. 16.8 Gait recognition [34]

feature vectors. Features are extracted from each walk, e.g. the acceleration of gait. To identity the mobile's user, Dynamic Time Warping (DTW) is used to compare the extracted feature vectors with the reference ones (enrolled templates). If DTW found a match, then the user is granted the access to the mobile. Otherwise he is rejected.

Compared to other methods, the gait-based authentication enjoys a number of advantages. The gait data is a unique identifier for each person and cannot be shared. Also, none could fake the other's gait. Images building this data can be taken at a distance and it does not require users' involvement [35]. However gait data differs at some cases such as: walking for a long time, injury, weight or footwear changes.

Voice Recognition The voice recognition is an authentication technique in which a user say his password to authenticate himself to his mobile. This technique uses different acoustic features of individuals to authenticate the user. These acoustic patterns reflect both learned behavioral patterns (i.e. voice pitch, speaking style) and anatomy (i.e. shape and size of throat and mouth) [27]. The voice recognition system may be either text-dependent (user speaks a predetermined phrase) or text-independent (user speaks what he/she wants).

Riva et al. [36] developed a progressive authentication system composed of three factors, *face, voice* and *PIN*, to authenticate a user. There are three protection levels: public (access all public applications), private (access both public and private applications) and confidential level (access to all applications). These levels are used to protect important applications against unauthorized use, while providing a way to use the less sensitive applications. The voice recognition of this system depends on Speaker Sense Algorithm. This algorithm uses Gaussian Mixture Model (GMM)

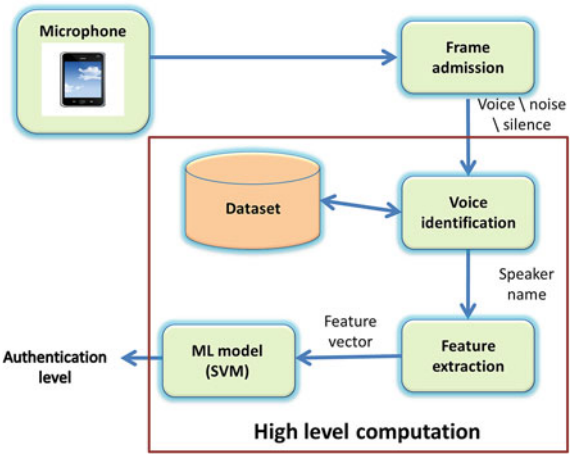

Fig. 16.9 Voice recognition authentication system

classifier to train system by audial recording for 2 min during a phone call. Then, the user's voice is recorded every 20 ms to continuously validate user.

There are two phases for voice recognition: *Frame Admission* and *Voice Identification*. In the frame admission, the recorded sound is analyzed to identify voice, noise and silence frames. In Voice Identification, voice frames are used to recognize the speaker. Voice Identification and high-level processing are done into the cloud (Windows Azure) or a remote device. Then, using the attached mobile's sensors, the system extracts features (e.g. Time elapsed since the last the phone was on the table, or pocket) and then produces a feature vector. This vector is redirected to a machine learning (ML) model to associate a label to the vector. This label maps the user to one of the three protection levels (see above). A summary of this system is demonstrated in Fig. 16.9.

The voice-based technique might be preferable because any mobile already contain a microphone, so no an additional cost is imposed on the users [19]. However, human voice is sensitive to various factors like: aging, noise, medical conditions (such as a common cold) and emotional state, etc. [21]. Such factors affect the accuracy of the authentication results.

Keystroke This technique was developed to enhance the text-based authentication one. The keystroke technique is based on extracting keystroke features (e.g. the time of key holding or intervals between two keystrokes) when a user enters his/her PIN. A typical a keystroke system [37] is composed of fours modules : *data acquisition, feature extraction, matching and scoring*. Firstly, Keystroke dynamics data is collected when a user presses keys. This data is then examined to extract some features forming a biometric pattern. This biometric pattern is then compared to biometric templates enrolled during a training stage. Such comparison produces either a distance or score describing the similarity between the learned pattern and the stored templates. This similarity must exceed a threshold value. If similarity is less than

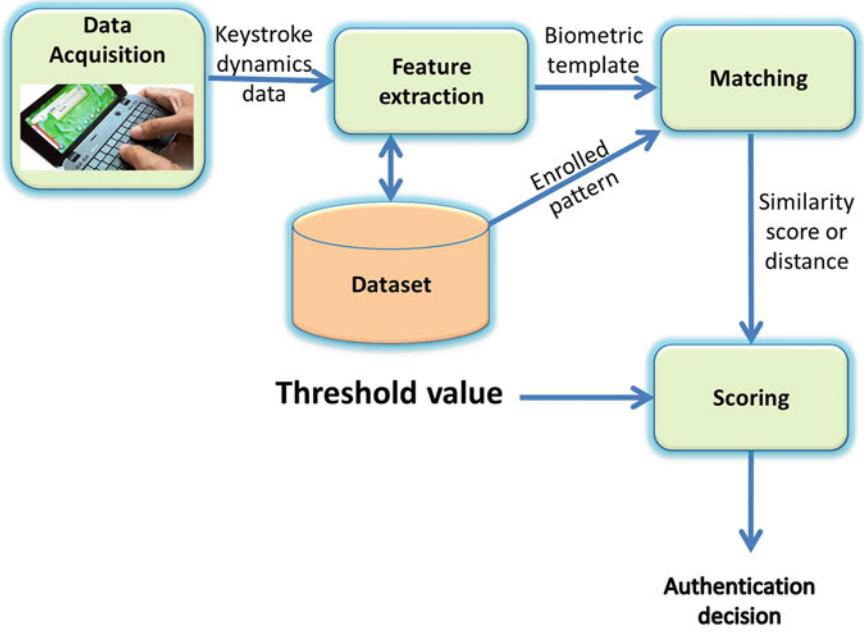

Fig. 16.10 Keystroke system [38]

this threshold, the pattern is rejected. Otherwise, the pattern is accepted and the user is granted the access to the system. This system is described in Fig. 16.10.

Chang et al. [39] proposed an authentication solution using keystroke dynamics besides the pressure feature. This is recorded using graphical-based password for touch screen mobile to enlarge the password space size. While mobile's owner is selecting 3–6 thumbnails into an image in some sequence representing the graphical password, the system is extracting and comparing the keystroke features. These features include pressure and time features such as Down-Up (DU) time, Up-Down (UD) time, Down-Down (DD) time and Up-Up (UU) time. To enroll a user's template in a database, five training samples were needed from each user. To verify the user's identity, a statistical classifier was used. This classifier compares the most recent template with the registered one in the enrollment phase. If they do not match, the system rejects the user's login request. Otherwise, the user is granted an access to the system.

The keystroke technique overcomes the shoulder surfing attack and is done implicitly without disturbing the user. In addition, compared to other biometrics, the keystroke does not add an additional hardware. However, its usability is not good on touchscreen mobiles. This is because the hold time is nothing compared to the normal sized keyboards [40]. This is affected by different keypad sizes or layouts of mobile devices in QWERTY keyboards.

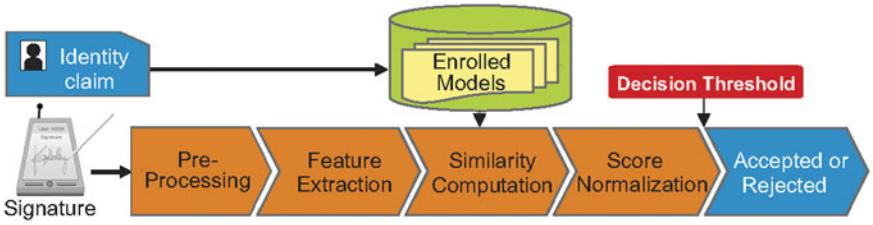

Fig. 16.11 Signature recognition [43]

Signature recognition In this technique, a user signs on a touch-screen of a mobile, then a system analyzes how the user types on the screen [41]. This is done by extracting some features like: time, speed, acceleration, pressure, and direction [42]. A typical signature recognition system is composed of five modules: *pre-processing, feature extraction, enrollment, similarity computation and score normalization*. This system first acquires digitized signals obtained from a touchscreen or a pen movement on a tablet while its user is holding the device. In the preprocessing step, the missing parts of the acquired signals are completed [42].

In the feature extraction, a feature vector, consisting of signature duration or average speed, is generated from each acquired signal. These features are either enrolled as templates or used by a statistical model representing the generated signatures [43]. The similarity computation module matches the claimed identity to the enrolled templates by computing a similarity score. This is done using distance-based classifiers (e.g. Euclidean distance or Mahalanobis distance) or statistical models (e.g. Dynamic Time Warping (DTW) or Hidden Markov Models (HMM)) [43]. To grant an access to the claimed user, a score normalization is used to normalize similarity scores to a given range of values and the compares the produced score with a pre-defined threshold value. This normalization is useful when multiple algorithms are used in a system and scores must be fused for a final decision [43]. A summary of a typical signature system is shown in Fig. 16.11.

Compared to other authentication methods, the signature technique is considered the most common used one in many verification tasks [44]. It has a high user's acceptance [43]. Unlike sensors and cameras used in fingerprint and face recognition, a mobile devices do not require any additional acquisition hardware. However, the signature technique seems different when signing on smart phones or signature pads or pen-based tablets. Signature on the touchscreen devices is less qualified because information about pressure or pen orientation is not available. Also person's signature differs at some cases such as using different style over time or in case of injury, mimicking the owner's signature using the other hand to sign [43].

16.4 Biometric Versus Traditional Authentication

As shown previously, each technique has its strengths and weaknesses. Choosing one of these methods depends on the user needs [29]. No technique is optimal but may satisfy what the user needs. There are a number of dissimilarities between the traditional and biometric authentications. Firstly, the traditional techniques are active that asks user to enter select carry the user credentials, while the biometric one is passive (user transparent) in which user has nothing to type select and also no devices to carry around [45]. Secondly, biometric data are linked to its owner but traditional credentials cannot do, since they can be forgotten or shared or lent or stolen [24]. Thirdly, biometric provides a reliable and natural way for identification because user has to be present at the time of authentication and can't repudiate access to system [29]. However, with traditional techniques users can deny the login by sharing the password. Last but not the least biometric data is fairly unique for each person. At the same time the biometric data is noisy which requires measurements to be accurate and this makes biometric authentication very challenging and emerging [46].

16.5 Comparison Among Authentication Techniques

This section provides a comparison among the various authentication techniques described earlier. This comparison is conducted based on the following metrics:

1. Usability (ease of use): This means that authentication should be fast and as unobtrusive as possible [47]. A determination of *High, Medium or Low* denotes how fast and easy the technique is to user.
2. Cost (need for additional hardware): With the cost here, we mean adding additional cost for a user's authentication, e.g. using camera/sensor to capture some features or from the additional support needed when mobile is blocking the access to users. Such cost should be minimized.

   A determination of *High, Medium or Low* denotes how much cost the technique requires.
3. Performance: This is related to the computational cost and time needed for a user's authentication. This includes the following characteristics:

   (a) Time complexity: This is concerned with decreasing both the calculation speed and the detection latency. The calculation speed is the time needed to build a user's model (i.e. extracting a user's features) and also to grant access to the user. Detection latency is the time consumed to detect an attacker usage of mobile and this must be minimized. It's desirable to increase user actions while decreasing waiting time for user input.

   (b) Minimum Consumption: This means to use the minimum resource requirements. Mobile can be thin client where limited computation and storage is done to minimize power (battery) consumption at mobile phones.

A determination of *High, Medium or Low* denotes how much time and computation the technique consumes.

4. Explicit or Implicit Technique(user direct interaction): This shows whether there is a need for a physical involvement of users during the authentication process or the authentication is done transparently with normal user activity without an explicit action from the users.

   A determination of Explicit or Implicit denotes if technique requires direct user interaction or not.

5. Robustness against any (aural or visual) eavesdropping: Checking whether a system is robust to various fraudulent methods and attacks that could be mounted during an authentication session, e.g. watching or listening a password during login time or selecting pictures that represent s passcode.

   A determination of *Yes or No* denotes whether a technique is robust or not.

6. Circumvention: indicates to whether a technique can detect the change of users. In other words, checking whether an illegitimate user can mimic the legitimate owner's behaviors to grant access to system.

   A determination of *Yes or No* denotes whether an owner can be mimicked or not.

7. Continuous Authentication: This is related to the length of the time during which the authentication is done either only at login time or during the runtime [9].

   A determination of Login time or Runtime denotes when authentication takes place.

Table 16.1 shows a compassion of various authentication techniques described above in relation to the previous mentioned metrics. A determination of High (H), Medium (M) or Low (L) denotes how well the technique adheres the metrics. The individual determinations are based on the authors' opinions and knowledge of techniques.

16.6 Explicit and Implicit Authentication

Traditional or biometric authentication techniques can be done explicitly or implicitly. This depends mainly on if it requires user interaction or not. This means that if it was user intrusive or not. If technique requires an explicit action from user for authentication like putting the finger on a fingerprint scanner, then this technique is considered to be explicit way for authentication. In contrast to this, technique is considered to be implicit way for authentication if it was user transparent (unobtrusive) [9], Effortless as possible and may be continuous authentication. The user transparency means that user deals normally without any explicit action because the relevant data is continuously recorded while the person is walking or writing a message for example. Continuous authentication provides protection goes beyond point-of-entry security. This means that it doesn't depend on only writing password correctly at login time but also at runtime [7].

Table 16.1 Comparison of authentication techniques

Technique	Usability	Cost	Performance	Explicit or implicit technique	Eavesdropping robustness	Circumvention	authentication authentication
PIN or PUK or alpha numeric password	High	Medium	Low	Explicit	No	Yes	Login time
Graphical password	Medium	Low	Medium	Explicit	No	Yes	Login time
Token	Medium	High	Medium	Explicit	No	Yes	Login time
Face recognition	High	Medium	High	Explicit or implicit	Yes	No	Login or runtime
Finger print	High	High	High	Explicit	Yes	Yes	Login time
Iris recognition	Medium	High	High	Explicit or implicit	Yes	No	Login or runtime
Gait recognition	Medium	Medium	High	Implicit	Yes	No	Runtime
Voice recognition	Medium	Low	Medium	Implicit	Yes	Yes	Login or runtime
Keystroke	High	Low	Low	Implicit	Yes	No	Login or runtime
Signature recognition	High	Low	Medium	Implicit	Yes	Yes	Login or runtime

16.7 Open Issues

Authentication based on behavioral biometrics have advantages over physiological ones as the former could be used to support continuous and transparent authentication system. Also, behavioral biometrics do not need any special hardware while collecting behavioral data, thus very cost-effective. Nonetheless, it is very difficult to design behavioral biometric techniques which could suite all users. So, the research should focus on how to propose an authentication system such that providing continuous and transparent authentication while not imposing additional cost for the special hardware. One way to achieve this is by developing multi-modal behavioral biometric authentication systems. In addition, these multi-model systems should be flexible and scalable. For example, a multi-model authentication system could be voice and keystroke or signature based system. Furthermore, this system should have the capability to integrate new biometric techniques while preserving the underling mechanism of the overall system design.

GP must be resistant to shoulder surfing or any eavesdropping while taking less time and effort to login. However, it isn't suitable for blind people or people with weak visions.

16.8 Conclusion

Mobile smart phones are now very important for their users. They aren't only used for communication purposes but also for storing and accessing sensitive data. In the era of cloud computing, the smart phones are a good tool to provide access to data and services on cloud and on the Internet. The first gate to protect the mobile itself and the data stored on it or the services provided by it is the authentication process. Many techniques are being used to support mobile authentications in different environments. This chapter has given an overview on the current mobile authentication mechanisms: traditional and biometric. Based on the user interaction with these mechanisms, a classification has been made. In addition, the chapter has showed the advantages and disadvantages of these mechanisms and it has conducted a comparison between the described techniques. Furthermore, the chapter has highlighted that the behavioral biometric authentication could be promising techniques for mobile authentication as they do not require any special hardware while support a continuous authentication. However, there is no a generic behavioral model to support all users, thus a multi-model (physiological and behavioral) is required to consider for further research in this direction. Before successful deployment of such potential system, great efforts of research and development are still required to investigate all aspects (e.g. power consumption and usability) of the mobile smart phone biometric system.

References

1. Tseng, D., Mudanyali, O., Oztoprak, C., Isikman, S.O., Sencan, I., Yaglidere, O., Ozcan, A.: Lensfree microscopy on a cellphone. Lab Chip **10**(14), 1787–1792 (2010)
2. Wang, H., Liu, J.: Mobile phone based health care technology. Recent Pat. Biomed. Eng. **2**(1), 15–21 (2009)
3. Fudong, L., Nathan, C., Maria, P., Paul, D.: Behaviour profiling on mobile devices. In: International Conference on Emerging Security Technologies (EST), 2010, IEEE (2010), pp. 77–82
4. Vaclav, M.J., Zdenek, R.: Toward reliable user authentication through biometrics. IEEE Secur. Priv. **1**(3), 45–49 (2003)
5. Hanul, S., Niklas, K., Sebastian, M.: Poster: user preferences for biometric authentication methods and graded security on mobile phones. In: Symposium on Usability, Privacy, and Security (SOUPS) (2010)
6. Wazir, Z.K., Mohammed, Y.A., Yang, X.: A graphical password based system for small mobile devices. arXiv preprint arXiv:1110.3844 (2011)
7. Nathan, L.C., Steven, M.F.: Authentication of users on mobile telephones-a survey of attitudes and practices. Comput. Secur. **24**(7), 519–527 (2005)
8. Mohsen, T., Ali, A.B.: Solutions to the gsm security weaknesses. In: The Second International Conference on Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08, IEEE (2008), pp. 576–581 (2008)
9. Qian, T., Raymond, V.: Biometric authentication system on mobile personal devices. IEEE Trans. Instrum. Meas. **59**(4), 763–773 (2010)
10. Andrea, K., Valerie, S., Michael, S.: Using publicly known passwords with haptics and biometrics user verification. In: IEEE Haptics Symposium (HAPTICS) 2012, IEEE (2012), pp. 559–562 (2012)
11. Greg, E.B.: Graphical password (September 24 1996) US Patent 5,559,961
12. Haichang, G., Zhongjie, R., Xiuling, C., Xiyang, L., Uwe, A.: A new graphical password scheme resistant to shoulder-surfing. In: International Conference on Cyberworlds (CW) 2010, IEEE (2010), pp. 194–199 (2010)
13. Lawrence, O.: Comparing passwords, tokens, and biometrics for user authentication. Proc. IEEE **91**(12), 2021–2040 (2003)
14. Fadi, A., Syed, Z., Wassim, E.H.: Two factor authentication using mobile phones. In: IEEE/ACS International Conference on Computer Systems and Applications, 2009 (AICCSA 2009) IEEE (2009), pp. 641–644 (2009)
15. Parekh, T., Gawshinde, S., Sharma, M.K.: Token based authentication using mobile phone. In: International Conference on Communication Systems and Network Technologies (CSNT) 2011, IEEE (2011), pp. 85–88 (2011)
16. Clarke, N.L., Furnell, S.: Advanced user authentication for mobile devices. Comput. Secur. **26**(2), 109–119 (2007)
17. Fred, C.: A secure mobile otp token. In: International Conference on Mobile Wireless Middleware, Operating Systems, and Applications, pp. 3–16. Springer (2010)
18. Mohamed, H.E., Muhammad, K.K., Khaled, A., Tai-Hoon, K., Hassan, E.: Mobile one-time passwords: two-factor authentication using mobile phones. Secur. Commun. Netw. **5**(5), 508–516 (2012)
19. Salil, P., Sharath, P., Anil, K.J.: Biometric recognition: security and privacy concerns. IEEE Secur. Priv. **1**(2), 33–42 (2003)
20. Mohammad, O.D., Claudia, N., Patrick, B., Christoph, B.: Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) 2010, IEEE (2010), pp. 306–311 (2010)
21. Anil, K.J., Arun, R., Salil, P.: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 4–20 (2004)
22. Arun, R., Anil, J.: Biometric sensor interoperability: a case study in fingerprints. In: Proceedings of International ECCV Workshop on Biometric Authentication. Springer, pp. 134–145 (2004)

23. Anil, K.J., Patrick, F., Arun, A.R.: Handbook of Biometrics. Springer, New york (2007)
24. Pim, T., Anton, H.M.A., Tom, A.M.K., Geert-Jan, S., Asker, M.B., Raymond, N.J.V.: Practical biometric authentication with template protection. In: Audio-and Video-Based Biometric Person Authentication, pp. 436–446. Springer (2005)
25. Kresimir, D., Mislav, G.: A survey of biometric recognition methods. In: 46th International Symposium Electronics in Marine, 2004. Proceedings Elmar 2004, IEEE (2004), pp. 184–193
26. Patrick, G., Elham, T.: Performance of biometric quality measures. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 531–543 (2007)
27. Vibha, K.R.: Integration of biometric authentication procedure in customer oriented payment system in trusted mobile devices. Int. J. Inf. Technol. **1**(6), 15–25 (2012). doi:10.5121/ijitcs.2011.1602
28. Jakobsson, M., Shi, E., Golle, P., Chow, R.: Implicit authentication for mobile devices. In: Proceedings of the 4th USENIX conference on Hot topics in security, USENIX Association, pp. 9–9 (2009)
29. Umut, U., Sharath, P., Salil, P., Anil, K.J.: Biometric cryptosystems: issues and challenges. Proc. IEEE **92**(6), 948–960 (2004)
30. Muhammad, K.K., Jiashu, Z., Xiaomin, W.: Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. Chaos Solitons Fractals **35**(3), 519–524 (2008)
31. Jakobsson, M.: Mobile Authentication: Problems and Solutions. Springer Publishing Company, Incorporated, New York (2013)
32. Yooyoung, L., Phillips, P.J., Ross, J.M.: An automated video-based system for iris recognition. In: Tistarelli, M., Nixon, M.S. (eds.) Advances in Biometrics, pp. 1160–1169. Springer, Berlin (2009)
33. Park, K.R., Park, H.A., Kang, B.J., Lee, E.C., Jeong, D.S.: A study on iris localization and recognition on mobile phones. EURASIP J. Adv. Signal Process **2008**, Article ID 281943 (2008). doi:10.1155/2008/281943
34. Hamed, N., Ghada, E.T., Eman, M.: A novel feature extraction scheme for human gait recognition. Int. J. Image Graph. **10**(04), 575–587 (2010)
35. Dacheng, T., Xuelong, L., Xindong, W., Stephen, J.M.: General tensor discriminant analysis and gabor features for gait recognition. IEEE Trans. Pattern Anal. Mach. Intell. **29**(10), 1700–1715 (2007)
36. Oriana, R., Chuan, Q., Karin, S., Dimitrios, L.: Progressive authentication: deciding when to authenticate on mobile phones. In: Proceedings of the 21st USENIX Security Symposium (2012)
37. Shanmugapriya, D., Padmavathi, G.: A survey of biometric keystroke dynamics: approaches, security and challenges. arXiv preprint arXiv:0910.0817 (2009)
38. Carlo, T., Abbas, R., Ilhami, T.: Full-size projection keyboard for handheld devices. Commun. ACM **46**(7), 70–75 (2003)
39. Ting-Yi, C., Cheng-Jung, T., Jyun-Hao, L.: A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. J. Syst. Softw. **85**(5), 1157–1165 (2012)
40. Sevasti, K., Nathan, C.: Keystroke analysis for thumb-based keyboards on mobile devices. In: New Approaches for Security, Privacy and Trust in Complex Environments, pp. 253–263. Springer (2007)
41. Simon, L., Mark, S.: A practical guide to biometric security technology. IT Prof. **3**(1), 27–32 (2001)
42. Marcos, M.D., Julian, F., Javier, G., Javier, O.G.: Towards mobile authentication using dynamic signature verification: useful features and performance evaluation. In: 19th International Conference on Pattern Recognition, 2008. ICPR 2008, IEEE (2008), pp. 1–5
43. Ram, P.K., Julian, F., Javier, G., Marcos, M.D.: Dynamic signature verification on smart phones. In: Highlights on Practical Applications of Agents and Multi-Agent Systems, pp. 213–222. Springer (2013)
44. Anil, K.J., Friederike, D.G., Scott, D.C.: On-line signature verification. Pattern Recognit. **35**(12), 2963–2972 (2002)

45. Roman, V.Y., Venu, G.: Behavioural biometrics: a survey and classification. Int. J. Biometrics **1**(1), 81–113 (2008)
46. Kai, X., Jiankun, H.: Biometric mobile template protection: a composite feature based fingerprint fuzzy vault. In: IEEE International Conference on Communications, 2009. ICC'09, IEEE (2009), pp. 1–5
47. Rene, M., Thomas, K.: Towards usable authentication on mobile phones: an evaluation of speaker and face recognition on off-the-shelf handsets. In: Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK (2012)