Mobile Biometric Security Systems for Today and Future

N. Yildirim1 and A. Varol2

1Fırat University, Elazig/Turkey, nilyildirim87@gmail.com
2Fırat University, Elazig/Turkey, varol.asaf@gmail.com

Abstract—Mobile devices are providing facility to human life in many areas such as online shopping, mobile banking and online messaging etc. Therefore, it has become an essential part of daily life. This scenario has directed people and institutions to seek more new ways regarding the security of mobile because all of the major transactions get done on mobile devices. Passwords (one-time passwords, complex character passwords, etc.) and login screen drawings of devices cannot ensure the safety of mobile devices, their applications and users therefore the hacking is becoming common. Biometric identification which is specific and distinguishing feature it is considered more secure than passwords because it is difficult to copy and alter. Biometric security systems are new as application for mobile systems and they need advancement and development in hardware and application fields. In this paper, we will discuss existing biometric systems for mobile device, operating systems and applications developed for biometrics security.

Keywords—Mobile, Security, Biometric Systems, Mobile Biometric Security, HCI

I. INTRODUCTION

Mobile devices have become a part of human life with the privilege of portability and the daily life is not complete without these devices. Hardware manufacturers, operating system and application developers take a variety of security measures due to personal, private and sensitive information in mobile devices. To ensure the security passwords, PINs or patterns are used to unlock the screen. Processing with password, unlocking mobile phone screens with PIN or pattern drawing, entering the card information for payment every time it is both time-consuming and challenging for users. However, the distinguishing human biometric features can be used as distinctive instead of all these passwords. This can offer a more secure and practical solution for the user. It is under consideration nowadays to use biometric as solution for security protection of mobile devices.

Face, fingerprint, palm, vein, voice and signature recognition features are often used as biometric identification. New generation smart phones and mobile operating systems allows developers to create biometric recognition and security applications using the camera, sound and touching features. Recently, mobile devices with biometric fingerprint sensor have given a different dimension to biometric identifications. In this paper, biometric security, the importance of biometric security for mobile devices, developed biometric applications for mobile, future of biometrics in mobile and applications in terms of human-computer interaction (HCI) are discussed.

II. BIOMETRIC SECURITY SYSTEMS

Biometric technologies are described as automated authentication and verifying the identity of a living person based on the physiological and behavioral characteristic [1]. In all of biometric systems, the samples (fingerprint, voice, retina, etc.) taken from people are stored in a storage device after translated into a numerical expression and encryption, afterwards, when users want to log in to the system again compatibility of records is checked via matching previously existing reference points with the stored reference point [2].

Figure 1: Operating mode of biometric security systems [3].

Biometric recognition systems can be listed as iris, retina, face, fingerprint, vein, palm for physiological biometrics and voice, signature, keystroke for behavioral biometrics. Physiological biometrics is based on the measurements of a part of the living human body and behavioural biometrics means measurements that are provided from an action implemented by the user [3].

In a survey of 188 people about the use of biometrics, it is measured that 71.8 percent of users use fingerprint recognition it is a big majority and 6 percent of users use hand geometry and signature recognition while face recognition is measured as only 1 percent [4]. So it is clear that the most applied biometric method is fingerprint. A fingerprint consists of the ridges on a person’s finger and a fingerprint distinguishes from others by the unique pattern of those ridges [5]. Face recognition is the simplest and natural way to identify biometric authentication of living human and also face recognition has three types; single image, multiple image and frame by frame video [3]. According to Javelin Strategy & Research [6], 35 percent of consumers use fingerprint matching method as biometric as seen in Figure 2.
While collecting data with biometric devices, data accuracy, and detecting that the data which is gathered from living user are important [7]. Liveness detection is important for biometric systems because spoof biometric data can be gathered from a living user and can be used in illegal operations [7]. Nowadays, motion pictures, determination of a person’s vein structure and use with fingerprint or palm recognition (with infrared rays), heartbeat and telling desired sentence with person’s own voice are used for liveness detection due to biometric identification copying such as fingerprint, face is also possible. Two methods are applied together is defined as bi-modal authentication as described. Bi-modal authentication is important to identify the real person. Using only one way authentication is less secure than bi-modal authentication due to the risk of copying and capturing biometric information.

III. MOBILE BIOMETRIC SECURITY SYSTEMS

Considering the security measures on mobile devices, followed security measures emerge:

- SIM card security with the PIN code
- Drawing shapes on the screen or pin number input for security of access to smart mobile phones.
- E-mail and password authentication for accessing some applications.
- Various applications for ensuring the safety and validity of mobile phones.

All of these security measures are not sufficient for the case of stolen or illegally access. It is likely to be stolen PIN number of mobile SIM card and screen pattern password or screen PIN number by shoulder surfers or to be seized e-mails and passwords by malicious people. When the credit card is saved to Google Play Store or Apple App Store, a person who knows the phone password can shop from markets. Considering all this negativity, biometric features of user have been starting to use to protect the mobile device and therefore user.

In Karnan and Krishnaraj’s study [1], durations, times, typing errors and force of keystrokes have been used as behavioral biometric characteristic for accessing to mobile devices. But it is understood that to evaluate the keystrokes as biometric characteristic and compare results too hard.

In Tsai et al.’s study [8], they have proposed the use of biometric identification with one-time password (OTP) for mobile banking transactions. With the increase of the techniques for seizing one-time passwords, this has been a threat to mobile users. In the proposed system, it is recommended for banks to store the user’s fingerprint, iris and face captured records to avoid this situation and to improve the security of mobile banking. When the user enters the correct OTP, biometric verification is required via real-time biometric capture from user. Thus the user will be able to enter the mobile banking system [8].

In the study [9] about mobile payment system via fingerprint, at first, user enters credit card and fingerprint templates and templates are saved. After obtaining a public key with an SSL connection, hash template of the fingerprint are created. The verification process is done after fingerprint hash and credit card information are sent to the server by public key.

In Omri et al.’s paper [10], a handwriting authentication system has been proposed and covered. User's handwriting templates are saved to the database. The biometric recognition system runs on a server which is on the cloud virtual machine. The password that is entered by handwriting to mobile device with touch screen is compared with the password which is in the database and provided to enter to system.

A. Biometric Security Applications for Smart Mobile Devices

Mobile Smart Phones enable the user to develop applications by using some telephone features as camera, microphone, and stylus (in some smart mobile devices like iPad and Galaxy Note). By the advantages of these features, users develop applications about biometric security systems for mobile devices. Face, fingerprint and iris recognition applications being developed using the camera of mobile device also the applications have been developed for voice recognition using a microphone and signature recognition using a stylus. In addition to all of these hardware features, Google has developed “face unlocks” for Android 4.0 (Ice Cream Sandwich) [11]. Camera.Face class on Android helps developer to identify a face. When face detection is used with a camera, the Camera.FaceDetectionListener lists the face objects (left eye, right eye, mouth, and cheekbone) to use in focusing and measurement [12].

As well as Android, iOS has brought AVCaptureStillImageOutput class with “SquareCam” [13] for camera settings and has created CIFaceFeature class for face recognition. The following features are defined by the facial recognition objects of iOS: left eye, right eye, mouth, smiling, left and right eye closed positions [14]. Android and iOS systems also include speech recognizer classes as well as face recognition classes.

Some of known Android applications about biometric recognition and biometric security systems and its area of use have been described in Table 1.
Table 1. Biometric applications and their functions.

<table>
<thead>
<tr>
<th>Application Name and Platform</th>
<th>Biometrics</th>
<th>How it works</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visidom AppLock [16] Android</td>
<td>Face Recognition</td>
<td>It protects any application (i.e. SMS, Gallery, E-Mail, Facebook, etc.) on the user’s phone using face recognition</td>
</tr>
<tr>
<td>Mobbeel [17] Android and iOS</td>
<td>Face, Iris, Voice, Signature Recognition</td>
<td>This API uses these biometric for recognitions. Signature recognition needs iPads and it comes with digital certificate. User can use multi biometrics for security.</td>
</tr>
<tr>
<td>RecognizeMe [18] iOS</td>
<td>Facial Detection</td>
<td>It locks iPhone using face detection with front camera</td>
</tr>
<tr>
<td>FaceLock [18] iOS</td>
<td>Facial Detection</td>
<td>It scans user’s face and user accesses the iPhone and it only detects the real user’s face.</td>
</tr>
<tr>
<td>FaceVault [18] iOS</td>
<td>Facial Detection</td>
<td>It uses facial Recognition and if it fails, it passes to pattern-based unlocking. It detects user’s face even if wearing glasses or make up.</td>
</tr>
<tr>
<td>Signedoc [19] Android and iOS</td>
<td>Signature Recognition</td>
<td>With this API user signs documents with legal validity on mobile or tablet. It recognizes user’s signature</td>
</tr>
<tr>
<td>XyzmoSIGNificant [20] Android and iOS</td>
<td>Signature Recognition</td>
<td>This app processes signing documents, mailing of paper originals, and long-term storage of documents. User can sign documents electronically with a tablet or smartphone.</td>
</tr>
<tr>
<td>Start Voice Recognition [21] Android</td>
<td>Voice Recognition</td>
<td>This application uses voice recognition system on Android and is used for to lock the screen of user's phone. It is only used on devices which support the Quick Start.</td>
</tr>
<tr>
<td>BioLock v1.0 [22] Android</td>
<td>Face and Iris and PIN Combined Recognition</td>
<td>It uses two forms of biometrics (face or iris) with a PIN and creates a encrypted key and it is used to lock or open the phone or user data.</td>
</tr>
<tr>
<td>SESTEK Voice Signature (Vocal passphrase) [23]</td>
<td>Voice Recognition</td>
<td>It is a biometric voice recognition application which verifies the identity of the person who calls.</td>
</tr>
<tr>
<td>HoyosID [24] Android and iOS</td>
<td>Face Recognition</td>
<td>This application performs face recognition with the front camera of the mobile device and all accounts, user names and passwords are required to save in this application. When the application recognizes the face, it enters the passwords instead of the user. In addition, the passwords are stored in telephone, not on the internet.</td>
</tr>
</tbody>
</table>

Besides these applications, mobile smart phone manufacturers create face recognition applications for user to open unlocked phone screen as well as Samsung Galaxy Nexus [25].

B. Biometric Security Solutions as Hardware for Smart Mobile Devices in Today

The use of biometric recognition on mobile devices has started with cameras and microphones as hardware features and the operating systems which allow using them with programming. According to Gartner's report, 30 percent of organizations will use biometric authentication on mobile devices by 2016 and this usage may be facial, voice, iris recognition and user password [26]. Goode Intelligence predicts that 3.4 billion users will use biometric systems on their mobile devices by 2018 and mobile device producers will earn 8.3 billion dollars [27].

Mobile device manufacturers have started to carry different biometric sensors on mobile devices due to practical and safer methods of biometric authentication for users. Now fingerprint sensors are able on the latest smart mobile devices. Apple’s Touch ID creates a strong biometric platform on consumer mobile devices by 2018 and fingerprint sensors will be standard on mobile devices until 2015 [27].

In Goode's mobile biometric market report 2013-2018, the factors in realization of mobile biometric market growth are discussed in the following [27]:

- Biometrics is presented to end-users and consumers like Apple iPhone 5s and Touch ID technology.
- Biometrics that can be used easily brings practical mobile device protection due to mobile device authentication methods (PIN or password) are cumbersome and unpractical.
- The use of biometric authentication system for mobile commerce is a convenient and safe way for payment methods.
- Many authentication companies as FIDO Alliance are making plans to support biometrics and this support will also be provided on mobile devices.
- Fingerprint templates are kept in a secure area called “secure vault” by Apple’s Touch ID fingerprint solution and all the security measures makes mobile devices safer for biometrics.
a. iPhone 5s as iOS Device and Touch ID

Touch ID for iPhone was developed as a fingerprint identification technology. Fingerprint sensor is located under the main screen button as seen in Figure 3.

![Figure 3: iPhone fingerprint sensor [28]](image)

When touching (without pressing) the home button of iPhone 5s, Touch ID sensor reads fingerprints and unlocks the phone's lock automatically [28]. One of the features in this system, as users use fingerprint sensor, the system learns the types of the fingerprint. The system allows five fingers identification and 50,000 different fingers should be tested for random matching of fingerprints [29]. Also Touch ID has reading fingerprint in 360 degrees feature, which means the system can read fingerprints in any direction of phone. Also fingerprint data is encrypted and protected with the safe containment within the A7 chip and none of applications can access fingerprint information [29].

Touch ID is used for:
- Shopping from Tunes Store, App Store and iBooks Store,
- Unlocking iPhone.

iOS does not allow to use Touch ID features for developers in terms of security. This hampers developing applications using fingerprint sensor.

b. HTC One Max and Samsung Galaxy S5 as Android Device

HTC One Max is the first Android mobile device which includes fingerprint sensor. Fingerprint scanner is located below the camera lens at the back of the phone. The system allows identification of three fingers and fingerprint identification is used for unlocking phone (Figure 4) [30]. It also has A7 chip security as iPhone.

![Figure 4: Fingerprint recognition of HTC One Max [30]](image)

Fingerprint sensor that is integrated into Galaxy S5 home button is used for unlock device and pay. Samsung Galaxy S5 differs from other fingerprint features because it allows third party application developers to create applications using fingerprint sensor API (Pass API) [31]. It is associated with PayPal and Samsung Galaxy S5 users can shop via Paypall using fingerprint biometric.

C. HCI for Biometric Systems on Smart Mobile Devices

Human Computer Interaction can be explained as interaction between users of computer and technology and computer hardware and software. Human Computer Interaction (HCI) has become more important in human lives because technology and technological devices have become a part of human life.

Blanco-Gonzalo et al. [32] have investigated the usability evaluation of biometrics in mobile devices. Handwriting signature recognition is used for usability evaluation. IPad is used as a mobile device. The effects of usability of biometric signature with different styluses were measured with different parameters. The results have been different with each stylus [32]. This illustrates the importance of mobile device usability of biometric recognition. It can be interpreted that the errors arise from usability can cause not confirmed entries in the biometric recognition process.

When biometric technologies on mobile devices are analyzed by usability branch of HCI, some points are discovered that may prevent safety and practicality for users.

- Using the rear camera for face recognition on mobile devices affect the usability. Because the user cannot take his/her picture accurately from back camera.
- When using the styluses for signature recognition, signature pairings may not be accurate [32] due to the type of styluses or touch screen. Appropriate hardware affects usability.
- The location of the fingerprint sensor on a mobile device is very important for usability. While HTC places the fingerprint sensor below the rear camera, Samsung and iPhone have positioned it under home screen button. Be present of the sensor on the display side of the mobile phone can positively affect usability. When iPhone reads fingerprint from 360 degrees by touching, Samsung and HTC needs to scroll up and down of the finger in one direction. This may not be very practical and may not be easy to find the correct position of the finger for the user.
- Biometric identification applications should not exhibit an inverse approach to the user's habits. Speed and simplicity of applications affect the usability.
IV. CONCLUSION

Today with technology advent, information security has become more important. It is seen that passwords or PINs are insufficient for ensuring and protecting the security of information. The importance of mobile device technologies in human life and all kinds of personal information carried on these devices was also necessary to take different security measures. Unique biometric features of human are used as the password with existing technology. Image, voice and signature of the person have been used as biometrics with the help of camera, microphone and touchscreen features of the mobile device. Phone protection, application access, e-signature transactions are provided via these characteristics.

Mobile device manufacturers install the fingerprint sensor in the devices for identification of fingerprint which is frequently used biometrics. In this way user security is protected and operations which require password can be performed only by one touch. In addition, usability of biometric recognition systems for HCI will increase use of mobile biometric systems by everyday users.

It is concluded that with the popularization of mobile devices which include fingerprint sensor, mobile biometric recognition will be used in the following ways:

- Biometric recognition, especially fingerprint, for mobile payment transactions will bring mobile payments in a safer and easier position.
- Using the fingerprint as the screen lock of device will be easier and safer for users.
- Mobile banking will provide fingerprint along with one-time-password and mobile applications will be updated in this way.
- Through allowing developers of using fingerprint sensor for creating applications, different ideas will be born for mobile biometrics and a new page will be opened in mobile security.

REFERENCES

[18] Techfat.com, «Top 5 Face Recognition Apps For iPhone


