CHAPTER 13

Biometric Signature for Mobile Devices

Maria Villa and Abhishek Verma

CONTENTS

13.1 BIOMETRIC SIGNATURE RECOGNITION

This chapter talks about the most recent mechanisms for biometric signature in mobile devices. The structure of this chapter is as follows: Section 13.2 introduces a general background and definitions of biometric signature on mobile methods. Section 13.3 presents some public databases for biometric signature. Next, Section 13.4 discusses different approaches for liveness detection on biometric signature and presents four case studies. Finally, the conclusions are drawn in Section 13.5.

13.2 INTRODUCTION

The expression signature originates from Latin *signare* (to sign) and is typically a handwritten representation of a person's name [1]. The individual that signs is known as signer. Some signatures require a witness and a notary public for further legal strength such as the event of a marriage, purchase of a property, and more. A signature gives indication of both identity (proves identity) and will (informed consent) [1]. The verification of a signature can be divided into two categories [1]:

1. *Offline signature verification* takes as input the image of a signature and is used in banks and on documents.
2. *Online signature verification* uses signatures, captures by pressure-sensitive surfaces.

In the last 5 years a variety of devices with touch screens have emerged. This headed to the idea of using a touch screen as the capture device, dropping the cost and at the same time reaching the final user in point of service terminals, smartphones, tablets, and more [2].

13.2.1 How Biometric Signature Works

Signature is considered to be a behavioral biometric trait. A behavioral feature studies the motions of an individual [3] and it is based on interactive characteristics. Some approaches use the image of the signature [4]. Figure 13.1 shows the signature of John Hancock which became synonym for "signature" in the United States [1]. John Hancock's signature is the most outstanding on the United States Declaration of Independence [1].

Biometric signature recognition measures and analyzes the physical motion of signing including speed, the stroke order, and applied pressure

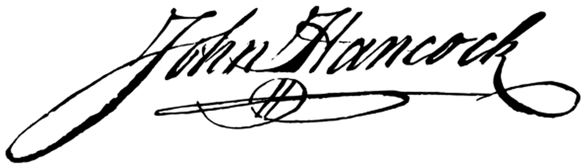

FIGURE 13.1 Signature of John Hancock. (From https://en.wikipedia.org/wiki/Signature#/media/File:JohnHancocksSignature.svg)

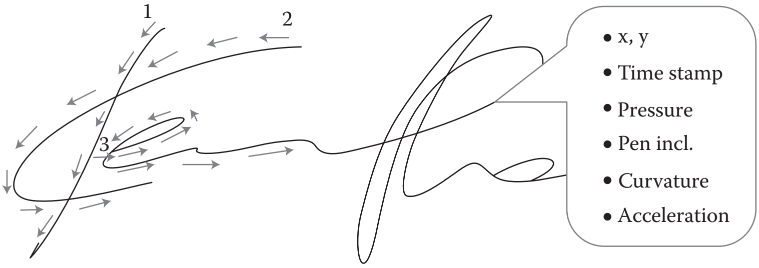

FIGURE 13.2 Biometric signature analysis. (From Biometrics Research Group.)

as illustrated in Figure 13.2 [4]. Some systems could also match graphic images of signatures, but the core of a signature biometric system is interactive or behavioral (how it is signed rather than visual).

Handwritten signature is used worldwide in different situations [2]:

1. As an agreement to the content of the signed document
2. As legal background
3. Used in forensic analysis
4. Links the document with the signer's identity

13.2.2 Benefits of Biometric Signature Biometric Systems

In our culture, handwritten signature is used in everyday life to gain access to documents, contract and agreement execution, acknowledgement of goods or services received, and banking services [6]. After electronic documents emerged, an electronic signature system using cryptographic algorithms was designed and it has been implemented in several countries.

Some biometric signature benefits are as follows [6]:

- The image of a signature is easy to falsify, however, the behavior of signing is exceptionally difficult [6]
- Low false acceptance rates (FAR) [6]
- Signature is perceived as not invasive since people are used to sign documents in daily basis [6]
- Remove the use of handling and storage of paper dl at shops and parcel delivery [2]

A weakness of signature biometric systems is that individuals may not always sign in a consistent manner.

13.3 PUBLIC DATABASES FOR BIOMETRIC SIGNATURE

13.3.1 Biometric Ideal Test

A distinguished database for biometric signature is biometrics ideal test (BIT). BIT is a website for biometric database supply and algorithm valuation. Among the databases available through BIT are iris, face, fingerprint, palm print, multispectral palm, and handwriting databases [7]. Researchers can download the public databases and submit algorithms online to be tested by third parties and also provides certification free of charge [7]. Figure 13.3 shows biometric signature workflow.

With respect to biometric signature, BIT is supported and certified by the following organizations [7]:

- International Association of Pattern Recognition (IAPR)
- Technical Committee on Biometrics (IAPR TC4)
- Asian Biometrics Consortium (ABC)
- Committee on Testing and Standards (ACTS)
- Testing results of algorithms are certified by IAPR TC4 and ACTS

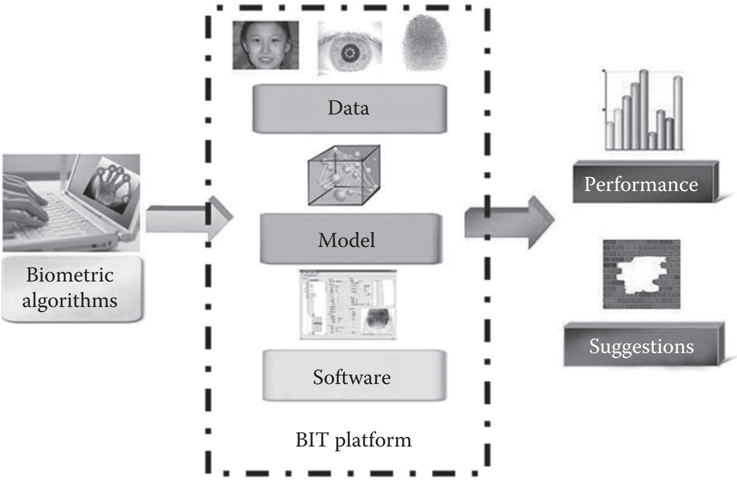

FIGURE 13.3 BIT biometric signature workflow. (From http://www.idealtest.org/images/idea_17.jpg)

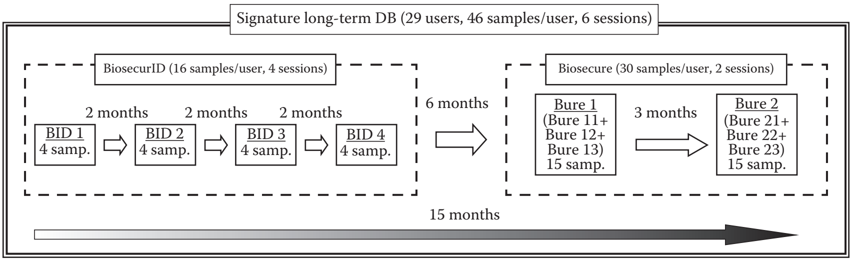
Signature long-term DB (29 users, 46 samples/user, 6 sessions)
BiosecurID (16 samples/user, 4 sessions)
2 months
2 months
2 months
BID 1 4 samp.
BID 2 4 samp.
BID 3 4 samp.
BID 4 4 samp.
6 months
Biosecure (30 samples/user, 2 sessions)
Bure 1 (Bure 11+ Bure 12+ Bure 13) 15 samp.
3 months
Bure 2 (Bure 21+ Bure 22+ Bure 23) 15 samp.
15 months

FIGURE 13.4 Time diagram of the different acquisition sessions that confirm the ATVS online signature long-term DB. (From ATVS—Biometric Recognition Group » Databases » ATVS-FFp.)

- BIT diagnoses algorithms are based on performance metrics and suggest improvements

13.3.2 Biometric Recognition Group-ATVS-SLT DB

Biometric Recognition Group—ATVS from the Autonomous University of Madrid has numerous biometric databases, all available for research at no charge [8]. The database available for biometric signature is ATVS-SLT DB. This dataset contains the online signature data of the 29 users to the BiosecurID and the Biosecure databases. The two signature subsets were developed within 15 months and they present some unique features that make them especially appropriate for aging evaluation of online signature recognition systems [PONE2013]. The general time distribution of the different sessions of the database is presented in Figure 13.4.

13.4 LIVENESS DETECTION ON BIOMETRIC SIGNATURE

Biometric signature recognition systems measure and study the physical motion of signing. Dynamic signature recognition has been accomplished using a pen stylus [9]. The applications using smartphones with a small touch screen are questionable since only a small touch display is used and the signature is performed with the finger [9].

The following case studies introduce different approaches for liveness detection of biometric signature systems.

13.4.1 Biometric Signature Commercial Applications

13.4.1.1 BioSign-ID

Among commercial applications for liveness detection for biometric signature is biometric signature ID (BSI). BSI designed BioSig-ID™ to secure a wide array of transactions in banking, health care, education and research, financing services, online purchases, retail, and government. The purpose of BioSig-ID is to diminish fraud, maintain security, and keep compliance. BioSig-ID has been implemented in about 70 countries [10].

BioSig-ID uses a gesture biometric password. The login is designed with a four unique digit password that is drawn by users as seen in Figure 13.5. It does not require tokens, keys, fobs, or passwords and no sensitive biometric data is required [10]. It offers two options to use as a layer or to replace the security method used. BioSig-ID system captures the user's unique movements when drawing four digit password including:

- Direction
- Speed
- Length
- Angle
- Pressure
- Height

Biometric signature is not considered threatening to people since they are used to signing paper documents (i.e., checks, contracts, and

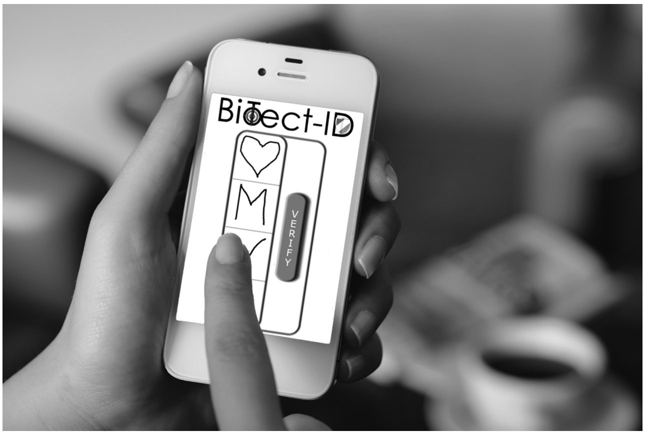

FIGURE 13.5 BioSign technology on mobile. (From Blog—Biometric Signature ID.)

applications) and electronic surfaces (i.e., credit card transactions and mail receipt electronic surfaces). Therefore, the system of BioSign-ID is very user friendly.

Not only BioSig-ID is user friendly but also is effective at keeping imposters out with 99.98% accuracy as reported by independent auditor Tolly Group [11].

13.4.2 Evaluation of Strengths and Weaknesses of Dynamic Handwritten Signature

The evaluation of strength and weaknesses of dynamic handwritten signature study presents a toolbox, Windows-based program with a Wacom STU 500 connected, which stores data from a signing pad connected to a computer and a touch screen device located in a smartphone or a tablet. This study introduces a DTW-based algorithm and uses a database of genuine signatures obtained with a STU-500 pad as input. This approach presents some strengths and weaknesses of biometric signature modality [2].

This study considers the following features for a signature biometric system [2]:

- Altitude
- Positioning of the capture device
- Enrollment process
- Policies for accepting acquired signatures
- Capture device
- Impact of stress in the act of signing

In the acquisition tool box step, when a counterfeit signature is recognized in the system, it is requested to choose a genuine signature identifier from the ones that have not been forged beforehand. Once the genuine signature is designated, the different levels start sequentially, with no possibility of toing to a previous level and with the option to cancel the attempt as soon as the forged signature is recognized.

- The error rates obtained when using the STU-500 are mentioned below:

1.59% (level 1)

6.77%

12.86%

23.35% (level 4)

17.73%

19.51%

33.43% (level 7)

19.27%, 18.27%

16.93%, 18.21%

(level 11)

- Results when using mobile devices are mentioned below:

  APCERs of (in all cases for levels 8, 9, 10, and 11) 19.98%

  20.43%

  18.73% and 19.02%

  Note4-S; 18.4%, 18.45%, 16.73%, and 17.25%

  Note4-F; 15.32%, 14.72%, 15.06%, and 14.7% for iPad

13.4.3 Usability Analysis of a Handwritten Signature Recognition System Applied to Mobile Scenarios

With the growth of the use of smartphones and mobile devices in general, the sensitive data stored in them creates the need to protect it. This defense of delicate data started to be covered by biometrics [13]. The work of this case study is primarily focused on online signature. The method to obtain the biometric signature is by using the fingertip instead of a stylus. In addition, the system in this case uses a DTW-based handwritten signature recognition algorithm in mobile scenarios. The trials use a state evaluation and the users sign in four different devices, in five different positions, and three sessions separated by 1 week each. The results also display satisfaction and efficiency as shown in Figures 13.6 and 13.7.

The satisfaction results of this case study indicate that users scored 3.85 over 5. The preferred factor was the easiness (3.9) and the less favorite the

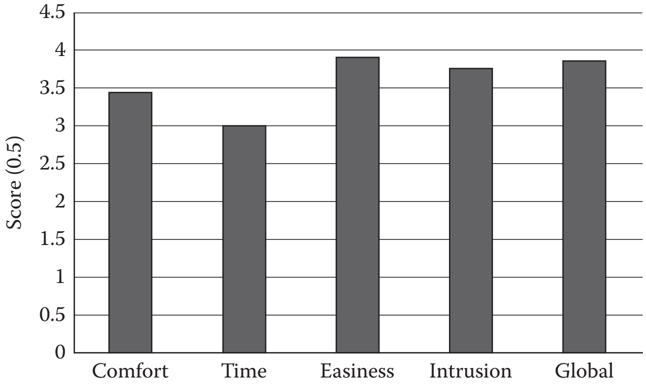

FIGURE 13.6 Satisfaction factors.

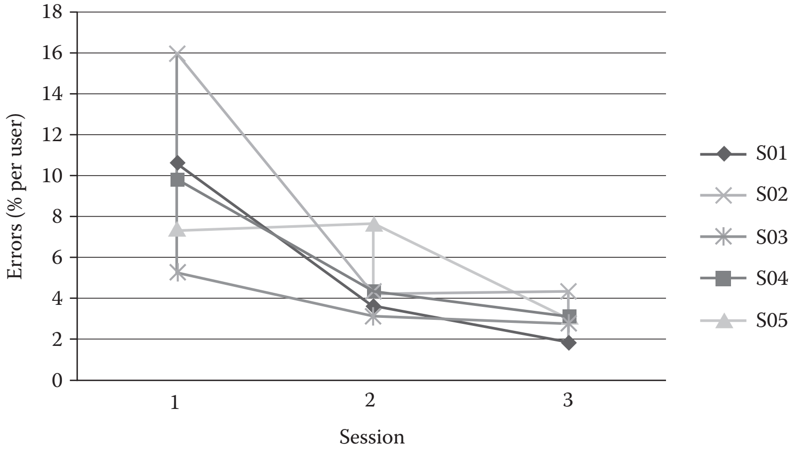

FIGURE 13.7 Efficiency.

time (3). 80% of the operators would use handwritten signature recognition on mobiles again in the future with the exception of one of them that chose stylus. The favorite devices were the STU using the stylus and the iPad using the fingertip. The preferred scenarios were arranged as follows: S01 > S03 > S04 > S02 > S05. Refer to Figure 13.6 [13].

Figure 13.7 indicates the efficiency results. The STU is the scheme that offers the most constant performance in the assessment, as anticipated it is the reference device. However, the iPad in scenario 2 shows the best results. The iPad also obtained an equal error rate (EER) over 7% in the reference scenario. Figure 13.7 demonstrates the high importance or the order of scenarios and the devices in the performance [13].

The method introduced in this section has the potential for future work. The first approach is to improve the liveness detection and usability in handwritten signature recognition. One of the proposals is to conduct a similar evaluation with different methods such as the human-biometric sensor interaction (HBSI). A second option is to design a scenario with more comfort for the user by training the users to familiarize with the biometric system [13].

13.5 CONCLUSION

Smartphones and in general mobile devices are becoming more and more sophisticated. Thus, people's daily life opened the doors for many building blocks for applications. This chapter presented two databases for biometric signature and three liveness detection approaches for biometric signature in mobile devices.

When the three approaches are compared, BioSign-ID is at the top vanguard of the other two discussed methods of biometric signature systems. BioSign-ID is revolutionary and it has been used among highest officials. BioSign-ID has been used as the first authentication step to ensure the highest level of identity in a network [12].

Particularly, the case "DTW-based handwritten signature recognition algorithm in mobile scenarios" proposes to enhance their services to conduct a similar evaluation with different methods such as the HBSI. Another option available to improve is to design a scenario with more comfort for the user by training the users to familiarize with the biometric system [13].

With respect to Section 13.4.2, it is important that mobile devices present the same level of vulnerability with trained forgers when comparing with the biometric reference obtained with the same device, no matter whether the forger uses a stylus or a finger. However, the results obtained in this study can be used as reference for further studies dealing with other algorithm and in particular, for those incorporating PAD mechanisms.

REFERENCES

1. Biometrics Research Group. n.d. http://biometrics.sabanciuniv.edu/signature.html (retrieved February 28, 2016).
2. Sanchez-Reillo, R., Quiros-Sandoval, H. C., Liu-Jimenez, J., Goicoechea-Telleria, I. 2015, September. Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries. In *Security Technology (ICCST), 2015 International Carnahan Conference on*, Taipei, Taiwan, pp. 373–378. IEEE.

3. Welcome to the Technology Executives Club. n.d. http://www.technology-executivesclub.com/Articles/security/artBiometricsSignatureRecognition.php (retrieved April 17, 2016).
4. Signature Biometrics. n.d. http://www.biometricnewsportal.com/signature_biometrics.asp (retrieved February 28, 2016).
5. Signature. n.d. https://en.wikipedia.org/wiki/Signature (retrieved April 17, 2016).
6. Signature Biometrics. n.d. http://www.biometricnewsportal.com/signature_biometrics.asp (retrieved April 17, 2016).
7. http://biometrics.idealtest.org/dbDetailForUser.do?id=12
8. ATVS—Biometric Recognition Group » Databases » ATVS-FFp. n.d. http://atvs.ii.uam.es/slt_db.html (retrieved April 17, 2016).
9. Vera-Rodriguez, R., Tolosana, R., Ortega-Garcia, J., Fierrez, J. 2015, March. e-BioSign: Stylus-and finger-input multi-device database for dynamic signature recognition. In *Biometrics and Forensics (IWBF), 2015 International Workshop on*, Gjøvik, Norway, pp. 1–6. IEEE.
10. The World's First Biometric Password. n.d. https://www.biosig-id.com/ (retrieved April 17, 2016).
11. Tolly Enterprises, LLC. January 19, 2011. Biometric Signature ID—BioSig-ID 2.0 User Authentication Solution. Test Report Tolly #211104, no. January 2011, pp. 1–7. http://biosig-id.com/images/docs/Tolly_BioSigID_Accuracy.pdf (retrieved April 16, 2016).
12. Blog—Biometric Signature ID. n.d. https://www.biosig-id.com/resources/blog (retrieved April 18, 2016).
13. Blanco-Gonzalo, R., Miguel-Hurtado, O., Sanchez-Reillo, R., Gonzalez-Ramirez, A. 2013, October. Usability analysis of a handwritten signature recognition system applied to mobile scenarios. In *Security Technology (ICCST), 2013 47th International Carnahan Conference on*, Medellin, Colombia, pp. 1–6. IEEE.