IET Biometrics

Special Issue: Mobile Biometrics

Journals The Institution of Engineering and Technology

Authentic mobile-biometric signature verification system

ISSN 2047-4938
Received on 31st March 2015
Revised on 2nd November 2015
Accepted on 14th November 2015
doi: 10.1049/iet-bmt.2015.0017
www.ietdl.org

Farhana Javed Zareen ✉, *Suraiya Jabin*

Department of Computer Science, Jamia Millia Islamia, Central University, New Delhi 110 025, India
✉ *E-mail: farhanazareen@yahoo.com*

Abstract: This is an undeniable fact that in the coming years a considerable percentage of organisations are drifting toward mobile devices for authentication. Banking sector as an additional offshoot has shifted to mobile devices with their applications for e-banking and mobile-banking, giving rise to an emergent requirement of a foolproof and authentic mobile-biometric system. This study presents an authentic mobile-biometric signature verification system and a comparative analysis of the performance of the proposed system for the two datasets; one using the standard device that is used for capturing biometric signatures and the other one is a mobile database taken from a smart phone for biometric signature authentication. The results presented demonstrate that the proposed system outperforms existing mobile-biometric signature verification systems based on dynamic time warping and hidden Markov model. Moreover, this study presents a comprehensive survey of mobile-biometric systems, different devices and hardware needed to support mobile biometrics along with open issues and challenges faced by the mobile-biometric systems. The experiments presented establish that the performance of mobile devices is low as compared with normal biometric signature capturing devices and the major reason the authors found is the absence of pen-tilt angle information in the mobile device datasets.

1 Introduction

Unmanned access of people to different types of services has become an important aspect of information era [1]. Biometric authentication system is being used extensively in many organisations, banking sectors and financial organisations across the globe [2]. The next step is to convert the stationary biometric authentication system to a mobile-biometric authentication system. The technological environment of these days is equally favourable due to the ubiquitous implementation of multimedia-enabled portable devices such as tablets, laptops, smart phones, personal digital assistants, palm tops [3] etc. Finger print [1, 4], face [5], voice [1] etc. have been used in the implementation of mobile-biometric authentication system because of the available and cheap hardware requirements for recording of these features. Camera, voice recorder and fingerprints reader are nowadays available with most of the mobile devices. Some of the mobile-biometric technologies that have been used in this literature [6–9] are listed in Table 1.

Nowadays, a variety of software products are available to capture these biometric features through hand-held devices. For example, M2SYS RapidCheckTM10-29 is a multi-modal biometric system that captures fingerprint, iris and face (Fig. 1). It can be used with smart phones or tablets and are mostly used for law enforcement, terror control, border control, military applications etc. As an improvement to static passwords, many laptops and tablets of Hewlett Packard and Fujitsu are coming embedded with fingerprint scanners.

However, these different biometrics also suffer from various drawbacks: e.g. in face recognition, the light quality, age of the person, a person is wearing any accessory (for example, glasses or cap) affects the recognition rate. Voice recognition can be affected due to illness such as flu or cough, iris recognition requires expensive hardware and it is not generally available in all mobile devices. In fingerprint recognition, the quality of the fingerprint image degrades if there is dirt on the finger or on the device. Another drawback of mobile-biometric system is that since these devices are used by people on a daily basis with rare or no maintenance, it gradually tends to wear out, hence giving undesired or wrong results. Nevertheless, mobile-biometric authentication is the need of the hour. '*Mobility is the driving force that will unleash the long awaited biometric revolution!*' as quoted by Aquity Market Intelligence confirms this quote by the estimate that by the end of the year 2020, the global market revenues in mobile applications will be reaching $33.3 billion annually [10].

One feature that is still extensively used and has been socially accepted for authentication is *handwritten signature*. Unconventionally, a digitising tablet is used for acquiring the dynamic features of a signature such as pressure, velocity, pen-tilt angles, pen-ups, pen-downs, x, y coordinates etc. These digitising tablets are pressure sensitive and can acquire such biometric traits of a signature during the process of signing. These tablets can be connected with any mobile device to record the biometric features. Recently, some smart phone and tablet vendors have also incorporated this feature into their devices, e.g. Samsung Galaxy Note has an in-built signature dynamics capturing system. Since handwritten signature is an established means of individual authentication and is socially accepted; therefore, combining these two into one system would produce a foolproof and efficient biometric authentication system on the go. In this era of Bring Your Own Device, it becomes unavoidable and essential aspect for organisations to provide data security. Personal identification numbers (PINs) and passwords are typically used to ensure privacy and security but these are prone to human factors such as bad memory or information theft.

In general, a biometric system operates on these two modes:

- *Identification*: The given template (i.e. test signature with all its dynamic features extracted) is compared with all of the stored templates in the database in order to establish an identity.
- *Verification*: The given template is compared with the stored template of a particular individual in order to verify whether that

Table 1 Mobile-biometric technologies

Biometric technology	Source
fingerprint	Khan *et al.* [4], Bigun *et al.* [1]
gait	Derawi *et al.* 2010, Gafurov *et al.* [11], Ailisto *et al.* [12]
face	Tao and Veldhuis [5], Bigun *et al.* [1]
voice	Marcel *et al.* [6], Bigun *et al.* [1]
gesture	Trewin *et al.* [7], Meng *et al.* [8]
iris	Sieger *et al.* [9]
typing pattern	Sieger *et al.* [9]
signature	Martinez-Diaz *et al.* [13]

person is really the one who he is claiming to be. The present paper describes a mobile-biometric system for *verification only*.

Therefore, it can be concluded there is a pressing need of an authentic mobile-biometric signature verification system which is capable of automatically recording a user's signature as well as verifying it at the time of online mobile transaction. The leading edge additions to the touch sensitive technologies are providing a feasible environment to biometric signature authentication in the mobile setup [14].

An authentic artificial neural network (ANN)-based mobile-biometric signature authentication system is presented and its performance is compared with other state-of-the-art systems based on hidden Markov model (HMM) and dynamic time warping (DTW). The experimental results demonstrate that the proposed system outperforms the other approaches for the same datasets (Samsung Galaxy Note). The outperformance achieved by the proposed system is the result of experimentations with different accelerated versions of backpropagation methods, e.g. resilient backpropagation algorithm (trainrp), scaled conjugate gradient backpropagation (trainscg) and Levenberg–Marquardt backpropagation (trainlm). Moreover, this paper presents a comprehensive survey of different aspects of mobile-biometric systems in order to suggest the improvement in existing mobile-biometric verification system.

2 Mobile devices used for capturing biometric signature

This section describes briefly different devices used for mobile-biometric signature capture and verification and the principle behind the two most important parts of mobile devices gyroscope and accelerometer (Fig. 2).

2.1 Mobile devices

There are a variety of mobile devices that can be used to capture the biometric features of a signature. Nowadays, many smart phones and tablets are including provisions for capture of biometric features in their newer versions. The mobile devices that have been used in this literature [14–16] for signature verification are listed in Table 2.

There are numerous applications that can be used along with different mobile devices to capture the dynamic features of a handwritten signature. Table 3 enlists some of the applications used along with the url of the websites from where these applications can be downloaded.

Table 2 Mobile devices used to capture signature in this literature

Brand name	References
iPhone (Apple)	Bailador *et al.* [17]
Samsung Galaxy Note	Krish *et al.* [14]
Hewlett-Packard TC 1100	Fernandez *et al.* [15]
Toshiba Portege M200	Fernandez *et al.* [15]
WACOM Pen tablet	Kholmatov and Yanikoglu [16]
XGT Serial Digitising tablet	McCabe *et al.* [18]

Table 3 Applications used along with mobile devices to capture dynamic signature

Application name	Supported devices/ platform	Source
SutiDSignature	IPhone 4.0, Android 2.3 and BlackBerry 6 SmartPhones and IPad	http://www.sutisoft.com/sutidsignature/features-smartphones-support.htm
OSIGUARD	Android	http://www.prnewswire.com/news-releases/new-android-osiguard-app-tackles-smartphone-thefts-with-patented-biometric-authentication-283088921.html
Grabba	Blackberry, IPhone, Samsung	http://www.grabba.com/en/technologies/signature-capture
Signosign2	Windows and IOS	http://www.en.signotec.com/products/signature-software/

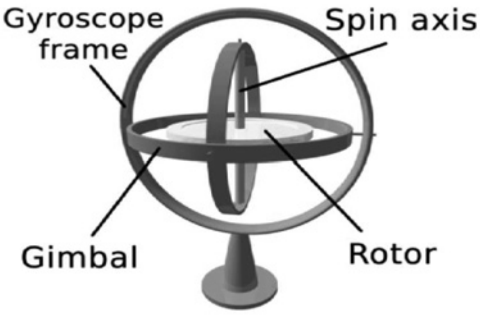

Fig. 2 *Typical gyroscope: image source – Wikipedia*

2.2 Gyroscope and accelerometer

The basic principle behind a Gyroscope is conservation of angular momentum; it contains a rotor that spins and keeps maintaining its orientation [19]. It is used in various applications such as compasses, spacecraft, aircraft and stabilisers for measuring and maintaining the orientation. An accelerometer is a device which is designed to measure the vibrations associated with any movement that takes place. It contains microscopic crystals that undergo stress when any vibration occurs; as a result, a voltage is produced that creates a reading on any acceleration [20]. Accelerometer in mobile devices is used to find out the orientation of the phone. Gyroscope estimates the angular rotational velocity [20]. These devices can be used to measure the pen-tilt angles, the movement of the hands, the direction of the tablet etc. Electronic pens that

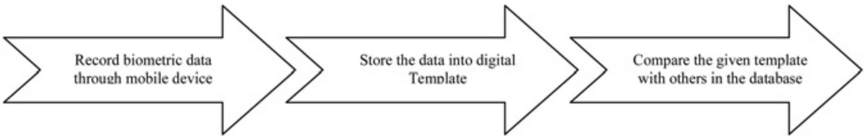
Record biometric data through mobile device
Store the data into digital Template
Compare the given template with others in the database

Fig. 1 *Major steps in the working of a biometric system*

are used to sign are also used to extract some features of the signature such as position coordinates, velocity, pen pressure, pen angles etc. It uses laser diodes, resonance frequency, magneto elastic sensors and strain gauges [21] etc.

Though these above-mentioned mobile devices facilitate functioning of a mobile-biometric signature verification system on the go but they also suffer from a number of drawbacks such as smart phones generally do not provide with large display areas which affects the intra-class variability (intra-class variability is the variation in different signature samples signed by the same individual), another challenge faced is that some important features that are pen-tilt angle information is not being captured using smart phones, other than that security of the signature templates that are stored in smart phones are also a matter of concern [14]. In biometric signature, the system becomes inefficient for people who are not used to perform signing operation on a daily basis. Another problem with mobile devices is that the user may need to sign using their fingertip which is considered to be difficult and uncomfortable for users [22]. In spite of these demerits, the interest in the usage of mobile devices for biometric authentication is on the rise. For signature-based authentication, one advantage of using mobile devices is that it does not require any special hardware. Almost all the smart phones nowadays are capable of capturing high-quality handwritten signature features and therefore there is a growing interest in its usage for individual authentication [14].

3 Architecture of the proposed mobile-biometric system

In this section, we propose architecture of the mobile-biometric system. It is divided into two phases: the registration phase and the authentication phase:

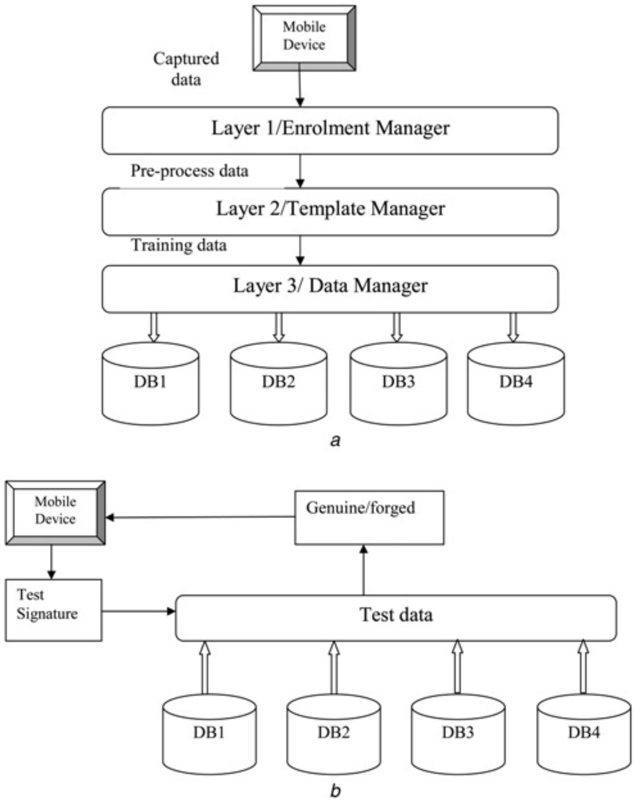

Fig. 3 *Registration phase*

a Registration phase
b Authentication phase

- *Registration phase*: In this phase as depicted in Fig. 3*a*, a set of sample signatures are captured from a user and sent to enrolment manager which pre-processes the data and further forwards the data to template manager, which stores the data as a template with all its dynamic features extracted from sample signature and associates a user id with each signature. The next step, i.e. data manager is responsible for fitting the input training data to a model using a machine learning technique (backpropagation method for the proposed system) and the trained model stored in the database. The registration process is complete.
- *Authentication phase*: In this phase as depicted in Fig. 3*b*, a user provides a test signature sample which is tested against the authentication model, and it gives back the result that whether the signature is genuine or forged.

4 Implementation of the proposed system

We have applied accelerated backpropagation [23] neural network algorithm to train the network for a dataset which is taken from Samsung Galaxy Note [13] and compared the performance of same system on the signature verification competition (SVC) 2004 database [24]. Backpropagation method starts with random initial weight vector and tries to determine a weight vector that minimises mean squared error (MSE) for a fully connected feed-forward multilayer ANN. It basically does hill climbing by gradient descent along the error (MSE) surface drawn for a possible weight vector space in order to minimise the error. Hill climbing tries each possible step to choose a step that does the most good at every step and gradient descent tries moving in the direction of most rapid performance improvement. The default performance function for feed-forward network is minimising MSE which is computed by averaging the difference of squared error between the output vectors and target vectors of the network. At each step, it alters the weight vector in the direction in order to produce the steepest descent along the error surface. Experimental results are presented to demonstrate the performance of the proposed authentic mobile-biometric system and the results are compared for conventional dataset used in this literature. Training stops for the following conditions: it increases the validation performance more than max_fail times or the maximum number of epochs (repetitions) is reached [25]. As this condition ensures that the error over the validation set (separate from training data) of examples typically decreases; otherwise, it may later increase due to overfitting of the training examples. The MSE over only the training examples may result in overfitting. Experiments were performed with different training functions while implementing accelerated backpropagation algorithm and the following training functions demonstrated the best performance of the proposed system [25]: trainrp, trainscg and trainlm.

The resilient backpropagation algorithm (trainrp) is based on the conventional backpropagation algorithms that compute the errors of the network and tries to minimise it by modifying the weights of the network. In scaled conjugate gradient backpropagation algorithm (trainscg), the weights are adjusted in conjugate directions that mostly converge more rapidly than steepest descent method. In most of the conjugate gradient methods searching starts in the steepest descent direction at first and then search is continued in the conjugate direction to determine the step size, and then the step size is adjusted in the next iteration [26]. The Levenberg–Marquardt backpropagation (trainlm) algorithm finds the minimum of a multivariate function. This training algorithm has the fastest performance for moderate sized networks [26].

4.1 Datasets used

Two databases were used; one is taken from Samsung Galaxy Note [13], and the other is taken from WACOM Intuos tablet [24]. The first database SG_NOTE contains 500 signature samples. These signatures have been taken in two sessions: total number of users

Table 4 Parameters for creating network

Training function	Adaption learning function	Performance function	transfer function
Trainrp	Learngdm	MSE	Tansig
Trainlm	Learngdm	MSE	Tansig
Trainscg	Learngdm	sum squared error	Logsig

Table 5 Chosen training parameters

Parameter	Experimental value	Description with default value
net.trainParam.epochs	10, 000	maximum number of epochs to train; default value 1000
net.trainParam.goal	0	performance goal (to minimise error)
net.trainParam.max_fail	600	maximum validation failures; default value = 6
net.trainParam.min_grad	1×10^{-7}	minimum performance gradient
net.trainParam.mu	0.001	initial mu (the learning rate)
net.trainParam.mu_dec	0.1	mu decrease factor
net.trainParam.mu_inc	10	mu increase factor
net.trainParam.mu_max	1×10^{10}	maximum mu
net.trainParam.show	25	epochs between displays (NaN for no displays)
net.trainParam. showCommandLine	0	generate command-line output
net.trainParam. showWindow	1	show training graphical user interface (GUI)
net.trainParam.time	Inf	maximum time to train in seconds

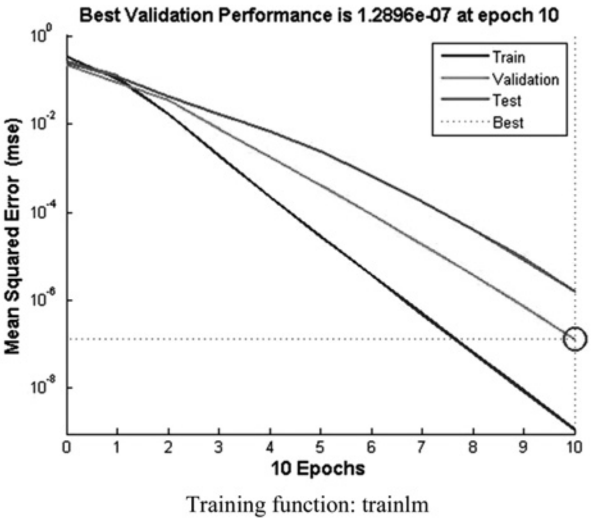

Fig. 4 *Validation curves for SG_NOTE (mobile) data*

being 25 and 10 signature samples were taken at each session. There was a gap of 5 days between the two sessions. This database does not provide any skilled forgery. Each signature sample represents four features: *x*-coordinate, *y*-coordinate, timestamp and pen pressure.

The second database SVC consists of 100 sets of signature samples. For each user, there are 20 genuine signature samples from the user, and 20 skilled forgeries from five other users. Total number of users are five. The samples were taken in two different sessions with a gap of at least 7 days. Each signature sample represents seven features: *x*-coordinate, *y*-coordinate, time stamp, button status, azimuth angle, altitude and pressure.

Furthermore, we need to pre-process the data because the data is inconsistent; we have used curve fitting technique, based on non-linear least-square method to make the data consistent.

4.2 Parameters for checking the accuracy of the system

A biometric signature authentication system is generally checked for accuracy using the following parameters [2, 27]:

- *False acceptance rate (FAR)*: FAR is a parameter that can be used in checking the accuracy of a biometric system. The probability that a biometric system will accept a forged signature considering it to be genuine is represented using FAR. It can be represented in terms of false positive (FP) and true negative (TN) values as given by (1)

$$\mathrm{FAR} = \frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \tag{1}$$

- *False rejection rate (FRR)*: The probability that a biometric system will incorrectly reject a genuine signature sample considering it to be forged is represented by FRR. It can be represented in terms of false negative (FN) and true positive (TP) values as given by (2)

$$\mathrm{FRR} = \frac{\mathrm{FN}}{\mathrm{FN}+\mathrm{TP}} \tag{2}$$

- *Sensitivity*: The likelihood that the system correctly accepts a genuine signature as genuine is represented by the sensitivity of the biometric system. It can be represented as given by (3)

$$\text{sensitivity} = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{3}$$

- *Specificity*: The likelihood that the system will correctly classify a forged signature as forged is known as the specificity of the

Table 6 Features used in both the databases for Experiments 1, 2 and 3

Features	SVC database	SG_NOTE database	SVC database without forgery samples	SVC database pen-ups and pen angle features excluded, without forgery samples
	Experiment 1	Experiment1	Experiment 2	Experiment 3
x-coordinate	√	√	√	√
y-coordinate	√	√	√	√
timestamp	√	√	√	√
pen-ups and pen-down	√	X	√	X
azimuth angle	√	X	√	X
Altitude	√	X	√	X
Pressure	√	√	√	√
random forgery samples	X	X	X	X
skilled forgery samples	√	X	X	X

Table 7 Results of experiments

Parameters	SVC database (full dataset with all features and all forged/ genuine training samples)	SG_NOTE database (full dataset)	SVC database without forgery samples	SVC database pen-ups and pen angle features excluded, without forgery samples
	Experiment 1		Experiment 2	Experiment 3
Sensitivity	0.9900	0.9976	0.9900	0.9800
Specificity	0.9800	0.8900	0.9220	0.8800
FRR	0.00492	0.02526	0.00494	0.03000
FAR	0.01818	0.2302	0.01820	0.2500

biometric system. It can be represented as given by (4)

$$\text{specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}} \tag{4}$$

All of the above-mentioned parameters were used along with receiver operating characteristic (ROC) curve which is a trade-off between the FP rate (FPR) and TP rate (TPR) to validate the performance of the proposed mobile-biometric verification system.

5 Experiments and results

5.1 Experiments

The experiments are structured as follows: three experiments were performed, in the *first experiment* we compare the performance of the proposed system over *SVC* dataset and the mobile dataset to validate which dataset provides the better results.

In the *second experiment*, we again compare the performance of the proposed system over both the datasets but after excluding the forged signature samples of the SVC dataset, since the mobile dataset does not contain any forged samples; therefore, from this experiment we can analyse the effect of training our system without any forged samples and observe whether training the system with forged samples provides any significant improvement to the performance of the system.

In the *third experiment*, only the four features that are available in both the datasets, i.e. x and y coordinates, pressure information of the signature samples and the timestamp were considered for both SVC and mobile database (SG_NOTE) and also the training samples of forged signature were excluded. Therefore, from the SVC database, the three features excluded were, i.e. pen-ups and pen-downs, azimuth angle and altitude, and therefore we are left with just four features in the SVC database that are the same as the mobile database (SG_NOTE). From this experiment, we can analyse two things; first, when working with exactly same features, which database gives better results, the conventional database or the mobile database and second whether including pen-tilt angle information (azimuth angle, altitude, pen-ups and pen-downs) plays any significant role in enhancing the performance of the system and if yes then to what extent.

Experiment 1: In Experiment 1, we apply backpropagation algorithm on a feed-forward neural network, on both the datasets (SVC and SG_NOTE) for the assessment of the performance of the proposed system over both datasets. We have used the parameters listed in Table 4 for creating our network and Table 5 enlists the chosen parameters for our experiment. Furthermore, Table 6 shows the features that we have taken for both the datasets in all of the three experiments.

Experiment 2: In Experiment 2, we apply the same algorithm with the same parameters on both the datasets but we use only the genuine signature samples of SVC database and try to analyse the effects of training the authentication system with skilled forgeries by comparing the results of Experiment 1 and Experiment 2. Table 6 enlists the features that we have used in both the datasets for our experiment.

Experiment 3: In Experiment 3, we extract the features x-coordinate, y-coordinate and pressure thus dropping the azimuth angle and altitude information from SVC database and apply the same algorithm to this extracted database and compare the results with that of Experiment 2 in order to assess the significance of pen-tilt angle information in the database. Table 6 enlists the set of features used in the datasets in this experiment. Moreover, the training samples of forged signatures for SVC dataset were excluded.

5.2 Results and discussion

We have used the standard ten-fold cross-validation [28] method, in which the dataset is partitioned into ten approximately equal parts where nine parts are used for training and remaining one part is reserved for testing and this step is repeated till every part gets used for both training and testing sets in the proportion of 9:1. Fig. 4 represents the plot of train, validation and test curves achieved after training the data.

Experiment 1: From Table 7, we can see that SVC database performs better than mobile data (SG_NOTE). Though the sensitivity of the mobile data is slightly higher than the SVC database but its specificity is recorded to be lesser than SVC dataset. From Fig. 5*a* and *b*, we can see that, SVC database produces better trade-offs of TPR and FPR.

Experiment 2: We can see from Table 7, there are no significant changes in the results of Experiment 2 as compared with Experiment 1. However, the performance of SVC database has lowered a bit. Thus, we conclude that presence of forgery samples is slightly affecting the performance of the proposed authentication system.

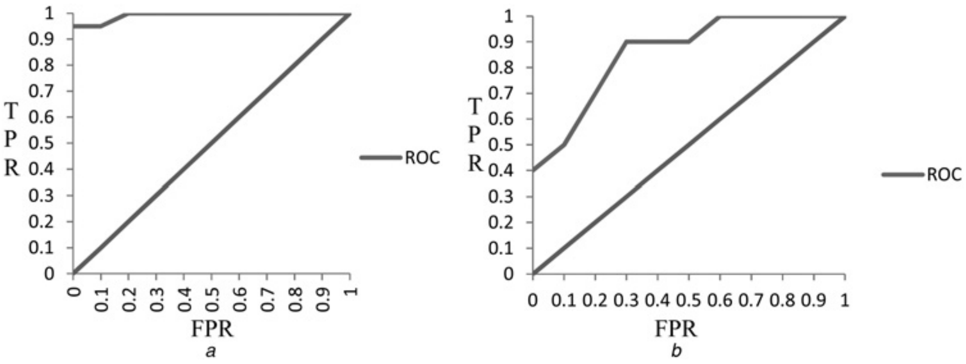

Fig. 5 *SVC database produces better trade-offs of TPR and FPR*

a ROC for SVC database for Experiment 1
b ROC for mobile database for Experiment 1

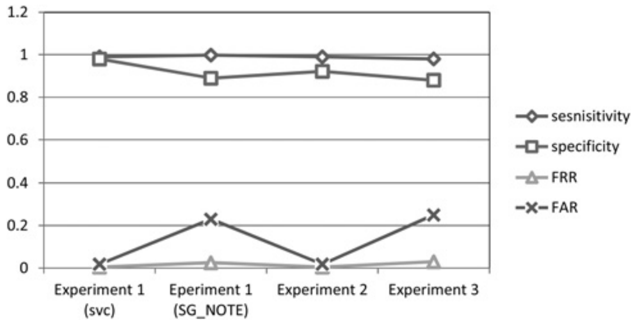

Fig. 6 *Comparison of the result of three experiments performed*

Table 8 Comparison of results

Approach	Device used	Database used	Performance
DTW [7]	Samsung Galaxy Note	25 users, 500 signatures	EER = 0.525%
DTW [11]	Apple iPad2	43 users, 2580 signatures	EER = 0.19%
HMM [13]	Samsung Galaxy Note	25 users, 500 signatures	EER = 6.2%
backpropagation method (the proposed approach)	Samsung Galaxy Note	25 users, 500 signatures	EER = 0.127%

Experiment 3: From Table 7, we can see that when we applied the same algorithm to both the databases with exactly same attributes, i.e. both the datasets do not contain forgery samples and have the same features, *x*-coordinate, *y*-coordinate, timestamp and pressure, we get better results from mobile database than the SVC database for which we recorded better performance till Experiment 2. As we removed the pen-tilt angle information, the performance of SVC database degraded significantly.

Fig. 6 depicts the summary of the experiments performed. From the results we can see that the system performs better for SVC database as compared with the SG_NOTE database. However, as we exclude the pen-tilt angle and pen-ups and pen-down information from the SVC database, its performance becomes poorer than that of mobile data. Thus we can conclude that the pressure information of the mobile data is more accurate and precise than that of the SVC database. Moreover, we conclude that pen-tilt angle information contribute largely for the authentication of the system.

Performance evaluation: Most of the work on biometric signature authentication has been done using a digitiser tablet as compared with hand-held mobile devices [13]. Table 8 shows the performance of the different approaches that have been used in this literature in the field of mobile biometric for handwritten signatures. DTW is a technique that is very popular in dynamic signature verification, and has been used in [14, 22] for mobile biometrics. Samsung Galaxy Note and Apple iPad2 are the devices that have been used to capture signature dynamics and the results are 0.525 and 0.19% in terms of equal error rate (EER), respectively, whereas HMM has been used in [13] that yields an EER of 6.2%, our approach is slightly better than the DTW approach yielding an EER of 0.127%.

6 Conclusions

Mobile devices overcome the difficulties of physical presence of individual at the time or place of authentication. Biometric signature authentication provides security in numerous ways than we can imagine, from mobile commerce to military application, from banking transactions to simple private document protection, mobile-biometric signature authentication is handling them all without the hassles of forgetting passwords, token theft or drawbacks of other physical biometrics. Mobile-biometric authentication belongs to the technology of now and future. The effects of the different features of the captured signatures and the significance of training the system with or without forgeries have been studied. The FAR of the system, when SVC database was used along with all the features (listed in Table 6) as well as forged samples, is 0.01818, as soon as we remove the forged samples from the database, it increases to 0.01820, and when we remove the pen-tilt angle information from the database, FAR further increases to 0.2500 and thus making the performance of the system even worst than that of the mobile database which yielded an FAR of 0.2302. We noted that our proposed approach is yielding an EER of 0.127% which is better than the other state-of-the-art methods present in this literature for the same mobile dataset (Samsung Galaxy Note).

From the experiments, we conclude that the lack of pen-tilt information is penalising the performance of the biometric authentication system in mobile environment, and therefore if we capture and add pen-tilt angle information in the mobile database, then it can be used more effectively for biometric signature authentication systems. One of the future works would be to design a mobile-biometric authentication system/app by capturing datasets for mobile devices with pen-tilt angle information; with the aim that more accurate mobile signature authentication can be performed.

7 References

1 Bigun, J., Fiérrez-Aguilar, J., Ortega-Garcia, J., *et al.*: ‘Multimodal biometric authentication using quality signals in mobile communications’. Proc. Int. Conf. on in Image Analysis and Processing IEEE Computer Society, September 2003, pp. 2–12

2 Jabin, S., Zareen, F.J.: ‘Biometric signature verification’, *Int. J. Biometrics*, 2015, **7**, (2), pp. 97–118

3 Zareen, F.J., Jabin, S.: ‘A comparative study of the recent trends in biometric signature verification’. 2013 Sixth Int. Conf. on Contemporary Computing (IC3), August 2013, pp. 354–358

4 Khan, M.K., Zhang, J., Wang, X.: ‘Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices’, *Chaos Solitons Fractals*, 2008, **35**, (3), pp. 519–524

5 Tao, Q., Veldhuis, R.: ‘Biometric authentication for a mobile personal device’. Proc. Third Annual Int. Conf. on Mobile and Ubiquitous Systems-Workshops IEEE, July 2006, pp. 1–3

6 Marcel, S., McCool, C., Atanasoaei, C., *et al.*: ‘MOBIO: mobile biometric face and speaker authentication’. Idiap, No. EPFL-REPORT-70604, 2010

7 Trewin, S., Swart, C., Koved, L., *et al.*: ‘Biometric authentication on a mobile device: a study of user effort, error and task disruption’. Proc. 28th Annual Computer Security Applications Conf., December. ACM, 2012, December 2012, pp. 79–168

8 Meng, Y., Wong, D.S., Schlegel, R.: ‘Touch gestures based biometric authentication scheme for touchscreen mobile phones’. Information Security and Cryptology, Berlin, Heidelberg, January 2013, pp. 331–350

9 Sieger, H., Kirschnick, N., Möller, S.: ‘User preferences for biometric authentication methods and graded security on mobile phones’. Proc. Symp. on Usability, Privacy, and Security (SOUPS), 2010

10 ‘The global biometrics and mobility report: the convergence of commerce and privacy’. Available at http://www.acuity-mi.com/GBMR_Report.php#sthash.d75xo10B.dpuf, accessed March 2015

11 Gafurov, D., Helkala, K., Søndrol, T.: ‘Biometric gait authentication using accelerometer sensor’, *J. Comput.*, 2006, **1**, (7), pp. 51–59

12 Ailisto, H.J., Lindholm, M., Mantyjarvi, J., *et al.*: ‘Identifying people from gait pattern with accelerometers’. Proc. SPIE, March 2005, pp. 7–14

13 Martinez-Diaz, M., Fierrez, J., Krish, R.P., *et al.*: ‘Mobile signature verification: feature robustness and performance comparison’, *IET Biometrics*, 2014, **3**, (4), pp. 267–277

14 Krish, R.P., Fierrez, J., Galbally, J., *et al.*: ‘Dynamic signature verification on smart phones’. Proc. Highlights on Practical Applications of Agents and Multi-Agent Systems, Berlin, Heidelberg, 2013, pp. 213–222

15 Alonso-Fernandez, F., Fierrez-Aguilar, J., Ortega-Garcia, J.: ‘Sensor interoperability and fusion in signature verification: A case study using tablet pc’, in ‘Advances in biometric person authentication’ (Springer, Berlin, Heidelberg, 2005), pp. 180–187

16 Kholmatov, A., Yanikoglu, B.: ‘Identity authentication using improved online signature verification method’, *Patt. Recognit. Lett.*, 2005, **26**, (15), pp. 2400–2408

17 Bailador, G., Sanchez-Avila, C., Guerra-Casanova, J., *et al.*: ‘Analysis of pattern recognition techniques for in-air signature biometrics’, *Pattern Recognit.*, 2011, **44**, (10), pp. 2468–2478

18 McCabe, A., Trevathan, J., Read, W.: ‘Neural network-based handwritten signature verification’, *J. Comput.*, 2008, **3**, (8), pp. 9–22

19 Kabai, S.: ‘Gyroscope’. Available at http://www.demonstrations.wolfram.com/Gyroscope/, Wolfram Demonstrations Project Published, 28 September 2007

20 Goodrich, R.: ‘Accelerometer vs. gyroscope: what’s the difference?’, LiveScience Contributor

21 Impedovo, D., Pirlo, G.: ‘Automatic signature verification: the state of the art’, *IEEE Trans. Syst. Man Cybern. C, Appl. Rev.*, 2008, **38**, (5), pp. 609–635

22 Blanco-Gonzalo, R., Sanchez-Reillo, R., Miguel-Hurtado, O., *et al.*: ‘Performance evaluation of handwritten signature recognition in mobile environments’, *IET Biometrics*, 2013, **3**, (3), pp. 139–146

23 Mitchell, T.M.: ‘Machine learning. 1997’ (McGraw-Hill, Burr Ridge, IL, 1997), vol. 45

24 SVC 2004 database. Available at https://www.aut.bme.hu/Pages/Research/Signature/Resources

25 Jabin, S.: ‘Stock market prediction using feed-forward artificial neural network’, *Int. J. Comput. Appl. (IJCA)*, 2014, **99**, (9), pp. 4–8

26 Kisi, Ö., Uncuoglu, E.: ‘Comparison of three back-propagation training algorithms for two case studies’, *Indian J. Eng. Mater. Sci.*, 2005, **12**, (5), pp. 434–442

27 Coughlin, S.S., Trock, B., Criqui, M.H., *et al.*: ‘The logistic modeling of sensitivity, specificity, and predictive value of a diagnostic test’, *J. Clin. Epidemiol.*, 1992, **45**, (1), pp. 1–7

28 Refaeilzadeh, P., Tang, L., Liu, H.: ‘Cross-validation’, in Liu, L., Özsu, M.T. (Eds.): ‘Encyclopedia of database systems’ (Springer, US, 2009), pp. 532–538

29 Das, R.: ‘An introduction to biometrics’, *Mil. Technol.*, 2005, **29**, (7), pp. 20–27

30 Gençay, R., Qi, M.: ‘Pricing and hedging derivative securities with neural networks: Bayesian regularization, early stopping, and bagging’, *IEEE Trans. Neural Netw.*, 2001, **12**, (4), pp. 726–734