Applied Mechanics and Materials Vols. 284-287 (2013) pp 3270-3274

doi:10.4028/www.scientific.net/AMM.284-287.3270

A Preliminary Study on Non-Intrusive User Authentication Method using Smartphone Sensors

Chien-Cheng Lin[1,a], Chin-Chun Chang[1,b], Deron Liang[2,c,*], Ching-Han Yang[2,d]

[1]Dept. of Computer Science and Engineering, National Taiwan Ocean University, Keelung, 20224, Taiwan

[2]Dept. of Computer Science and Information Engineering, National Central University, Taoyuan, 32001, Taiwan

[a]hammerlin@hotmail.com, [b]cvml@mail.ntou.edu.tw, [c]drliang@csie.ncu.edu.tw, [d]yang.chinghan@gmail.com

Keywords: Non-intrusive authentication; Continuous authentication; Orientation sensor

Abstract. This paper proposes a non-intrusive authentication method based on two sensitive apparatus of smartphones, namely, the orientation sensor and the touchscreen. We have found that these two sensors are capable of capturing behavioral biometrics of a user while the user is engaged in relatively stationary activities. The experimental results with respect to two types of flick operating have an equal error rate of about 3.5% and 5%, respectively. To the best of our knowledge, this work is the first publicly reported study that simultaneously adopts the orientation sensor and the touchscreen to build an authentication model for smartphone users. Finally, we show that the proposed approach can be used together with existing intrusive mechanisms, such as password and/or fingerprints, to build a more robust authentication framework for smartphone users.

Introduction

With the advances in nowadays technologies, smartphones are used not only for communicating purposes but also for business applications [9,10,11]. Surveys show that smartphones are used more frequently for various applications other than telecommunication [9,10]. These new applications raise new security issues to smartphone users [6]. The current protection mechanisms of these devices are usually based either on PIN codes, passwords, or biometric-based methods [13,26,17,18]. These mechanisms are intrusive in the sense and not convenient in frequent use; therefore, most users choose to turn them off [14,21,23]. Then, non-intrusive authentication mechanisms are desirable.

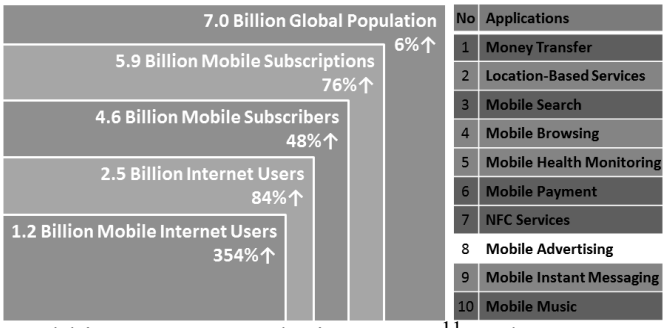


Fig. 1 The Digital World in 2012: Growth since 2007[11] and Top 10 Mobile Applications[10]

Recently, many biometric modalities are proposed as non-intrusive authentication methods for smartphone users. Derawi et al. and Gafurov et al. proposed a gait-based authentication mechanism based on the accelerometer [5,8]. Conti et al. proposed approach by using both accelerometer and orientation sensor to authenticate a smartphone user [4]. Surveys showed that smartphones are used more frequently for touchscreen applications than for telecommunication [9,10]. Shi et al. presented a touchscreen-based authentication system, which was verified via experiments involving 7 users [20]. We observe that people tend to have unique ways of holding and operating their smartphones. Consequently, we found that the two sensitive apparatus of smartphones, namely the orientation

sensor and the touchscreen, are capable of capturing the unique behavioral biometrics while the user is engaged in relatively stationary activities, such as holding the device to perform apps. The readings from the orientation sensor can represent both the holding posture and hand stability; furthermore, the trajectory of the flicking on the touchscreen reveals a user's habits such as finger agility. This type of information can be captured by the touchscreen sensor. In this work, we therefore propose a non-intrusive authentication method based on these two sensors. To the best of our knowledge, this work is the first publicly reported study that simultaneously adopts the orientation sensor and the touchscreen to build an authentication model for smartphone users.

To model this type of user's biometrics, 53 new features based on the readings of the orientation sensor and a feature vector comprised of 57 components based on the touchscreen-based flick gesture are proposed. To evaluate the feasibility of the proposed approach, an app has been implemented to collect the biometrics of 20 participants when they operate the smartphones in their hands. For each smartphone user, an authentication model is constructed based on the 110 combined features. To construct the authentication model, the iterative relief algorithm [22] is used to select and weigh a good feature set for each participant and the weighted k-nearest neighbor (WkNN) is used as the classification algorithm. Finally, the majority vote based on a few of the classification results of the WkNN is employed to improve the authentication accuracy. Our empirical results for twenty participants show that the proposed approach has an equal error rate of about 3.5% to 5%.

At a broad level, authentication mechanisms based on physiological approaches typically show better performance than behavioral models [3,7]. Recent studies, however, show that several behavioral modalities can be combined to provide satisfactory performance, comparing with physiological modalities, such as fingerprints [13,26]. It should be noted that we do not propose the proposed approach as a replacement or sole mechanism of authentication but rather as a complementary mechanism that can be used to improve security in hand-held devices. Users can still use strong biometrics or password explicitly when authenticating for the first time. Then, the proposed biometric can be applied implicitly for re-verification in a continuous authentication manner.

Structural modeling and experiment

The Orientation-sensor-based features. The orientation sensor is a common device of a smartphone. It is used to obtain the orientation of a smartphone with respect to three axes, namely, the *x*-, *y*-, and *z*-axis. The angles around the *x*-axis and the *y*-axis are the pitch angle and the roll angle of a smartphone, and the *z*-axis is referred to the azimuth [16]. In addition to these angles, a combined angle *w* of the pitch and the roll angle is adopted due to the fact that the movement of the wrist and forearm are often physically dependent on each other. After analyzing the metrics of the orientation sensor and the limitation of wrist motions [15,24], we define the range of measurements for wrist motions, such as flexion, supination, and pronation. Accordingly, a total of 53 features are defined for the orientation-sensor-based biometrics.

Touchscreen-based features. In order to represent an effective flick gesture that a user makes on the touchscreen, 57 features are extracted from the touchscreen sensor to comprise the feature vector for authentication. These features can be classified into 10 groups that reflect various aspects of a user's operating behavior. These feature groups include the distance, path, time, velocity, acceleration, curvature, tangential, angle, pressure and size.

Data collection. The touch gesture of smartphone apps can be classified into several types: left-right flick, up-down flick, spread, pinch, etc. We find the first two types are by far the most commonly used gestures in all apps. We therefore design an app on Android™ 2.3 platform to collect user's behavioral biometrics of these flicks. To gather experimental data, participants are required to have a seat. Once a user's finger touches the screen of the smartphone, the app continuously collects the sensor-based features until her/his finger does not touch the screen for a while.

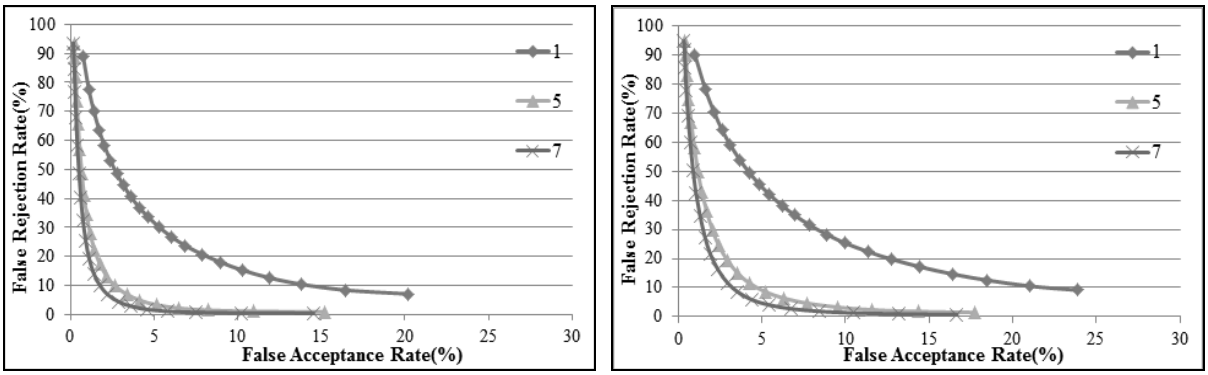
System modeling. To construct the authentication model, we use 110 features which are directly combined with the features of the orientation sensor and the touchscreen. In the learning phase, the iterative relief algorithm [22] is used to select and to weigh a good feature set for each

participant. Then, authentication models are trained by using the selected feature set and the weighted k-nearest neighbor (WkNN) classifier, which classifies a query sample by the k training samples nearest to the query sample. In our experiments, the k nearest training examples around a query sample are defined by the Euclidian distance. Since the experimental results with respect to k = 1, 3, 5, and 7 are similar, we only show the results with respect to k = 5 for simplicity. In the test phase, the majority voting [19] is adopted for improving the accuracy of the WkNN.

Results and discussion

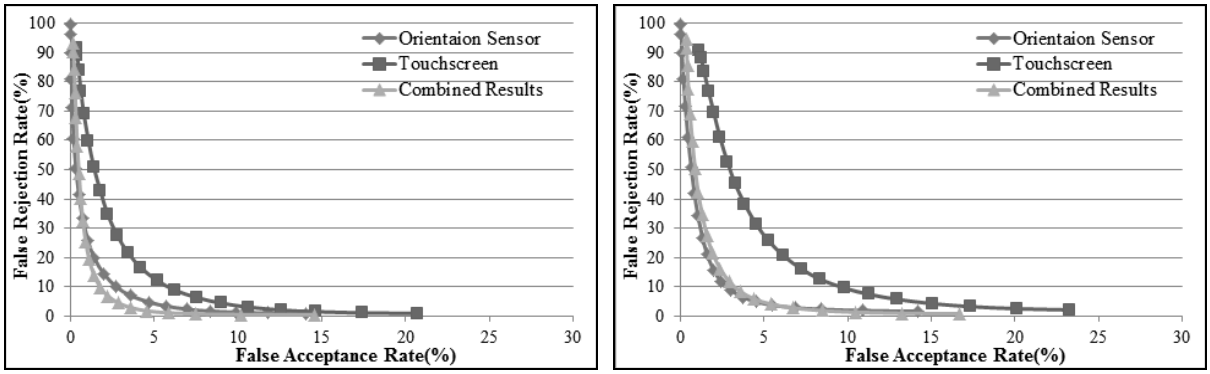
Experimental results. Twenty participants with varying smartphone experiences and ages ranging from 18 to 40 years, joined this experiment to generate two data sets: one is for the up-down flicks and the other is for the left-right flicks. These participants used the same smartphone to produce a total of 78,888 flick samples for the two data sets. Each participant conducted about 2,000 up-down flick samples and 1,800 left-right flick samples. About 3.8 percent of the samples were abandoned due to the operation duration being less than 100 milliseconds. In this experiment, the false acceptance rate (FAR), and the false rejection rate (FRR) were estimated by the leave-one-person-out strategy based on the results of 200 runs. For each run, the training set contained 450 samples, and the test set had 500 samples. In addition, for each sample set, the numbers of the positive sample and the negative sample were equal.

Fig 2 (a) and (b) shows the receiver operating characteristic (ROC) curve of the proposed approach with respect to the both data sets, respectively, where the FAR, and FRR with respect to different threshold limit and the number of classification results for the majority vote are shown. In this study, a test sample is classified into the positive if the positive receives two-thirds of the votes. We have found that the performance rises when the number of votes is increased as the odd numbers 1, 5, and 7. The experimental results have an equal error rate of about 3.5% and 5% when the number of votes is seven.



(a) up-down flicks (b) left-right flicks

Fig. 2 ROC curves showing the variances of FRR and FAR with thresholds and voting numbers



(a) up-down flicks (b) left-right flicks

Fig. 3 The performance comparison between the single-modality and the multi-modalities

To evaluate the effectiveness, we compared the performance of the proposed approach with the single modality approaches. Fig 3 (a) and (b) show the performance comparison among the single modality and the proposed multi-modalities with seven flicks. The experimental results show that the performance of multi-modalities is better than these two single modality approaches.

Discussion. The applications of the hold-and-operate biometric can include authentication and access control. It has been reported that the physiological approaches typically show better performance than behavioral models [3,8]. Table 1 summarizes the performance of existing biometrics including both physiological ones as well as behavioral ones. The accuracy of the proposed biometric is not comparable with the strong biometric modalities such as fingerprints. It should be noted, however, that we do not propose this approach as a replacement or sole mechanism of authentication but rather as a complementary mechanism that can be used to improve security in hand-held devices. Users can still use strong biometrics or password explicitly when authenticating for the first time. Then, the proposed biometric can be applied implicitly for re-verification in a continuous authentication scenario.

Table 1. Performance of various biometrics

	Biometrics	Performance, %	Participants
Physiological	IRIS[17,18]	EER = 0.0259	n/a
	Fingerprint[13,26]	EER = 3.2	n/a
	Palmprint[18,25]	EER = 0.19	n/a
	Face[18]	FRR = 16; FAR = 16	n/a
	Voice[18]	FRR = 7; FAR = 7	n/a
Behavioral	Signature[12]	EER = 0.99-1.07	94
	Keystroke[2,4]	FRR = 4; FAR = 0.01	154, 32
	Mouse[1,19]	FRR = 2.461; FAR = 2.464	22, 15-22
	Gait[5,8]	EER = 5 to 9	21

n/a: not applicable

Conclusions

In this work, we have proposed a novel non-intrusive authentication approach based on the orientation sensor and touchscreen of a smartphone. In this approach, we define 53 new features transformed from the readings of the orientation sensor and summarize 57 features transformed from the readings of the touchscreen. We have implemented an app for collecting both orientation-sensor-based and touchscreen-based features. The experimental results indicate that the proposed approach is feasible since its performance closes to the gait approach. We further have showed that the proposed mechanism can be used together with existing intrusive mechanisms, such as password and/or fingerprints, to build a more robust authentication framework for smartphone users. The current features adopted in this paper are only related to one kind of flick motion of a finger, we shall improve the proposed approach by utilizing the adopted features for multiple types of flick motion and combination algorithm, in the future.

Acknowledgments

This work was partially supported by the National Science Council of R.O.C. under Contract Nos. 100-2218-E-008-003 and 100-2218-E-008-004 and Software Research Center of National Central University.

References

[1] A.A.E. Ahmed and I. Traore: IEEE T DEPEND SECURE. Vol. 4(3) (2007), p. 16

[2] F. Bergadano, D. Guneti and C. Picardi: ACM T INFORM SYST SE Vol. 5(4) (2002), p. 367

[3] R. Bolle, J.H. Connell and N.K. Ratha: Pattern Recognition. Vol. 35 (2002), p. 2727

[4] M. Conti, I.Z. Zlatea and B. Crispo: Proceedings of the 6th ACM Symposium on Information, Computer, and Communications Security, (2011) March 22–24; New York, USA

[5] M.O. Derawi, P. Bours and K. Holien: The Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, (2010) Oct. 15-17; Darmstadt, Germany

[6] M.N. Doja and N. Kumar: INFOCOMP Journal of Computer Science. Vol. 7(4) (2008), p. 38

[7] S. Furnell, N. Clarke and S. Karatzouni: Computer Fraud & Security. Vol. 2008(8) (2008), p. 12

[8] D. Gafurov, K. Helkala and T. Søndrol: Journal of Computers. Vol. 1 (2006), p. 51

[9] Information on http://www.gartner.com/it/page.jsp?id=995812

[10] Information on http://www.gartner.com/it/page.jsp? id=1230413

[11] Information on http://www.slideshare.net/scapecast/accenture-mobility-mwc-2012-bubble-over-barcelona-lars-kamp

[12] A. Kholmatov and B. Yanikoglu: Pattern Recognition Letters. Vol. 26(15) (2005), p. 2400

[13] D. Maio, D. Maltoni, R. Capelli, J.L. Wayman and A.K. Jain: IEEE T PATTERN ANAL. Vol. 24(3) (2002), p. 402

[14] O. Mazhelis, J. Markuula and J. Veijalainen: Info. Manage. & Comp. Secur. Vol. 13(5) (2005), p. 367

[15] Information on http://www.medtrng.com/posturesdirection.htm

[16] R. Meier, in: *Professional Android™ 2 Application Development* (Wiley Publishing Inc., 2010).

[17] D.M. Monro, S. Rakshit and D. Zhang: IEEE T PATTERN ANAL. Vol. 29(4) (2007), p. 586

[18] L. O'Gorman: Proceedings of the IEEE, Vol. 91(12) (2003), p. 2021

[19] K. Revett, H. Jahankhani, S. Magalhães and H. Santos: Communications in Computer and Information Science (Global E-Security). Vol. 12 (2008), p. 210

[20] W. Shi, J. Yang, Y. Jiang, F. Yang and Y. Xiong: 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), (2011) October 10-12; Shanghai, China

[21] Information on http://www.smartcredit.com/blog/2011/09/02/consumer-reports-survey-on-Mobile-phones-and- security/

[22] Y. Sun: IEEE T PATTERN ANAL. Vol. 29 (2007), p. 1035

[23] Information on http://nakedsecurity.sophos.com/2011/08/09/free-sophos-mobile-security-toolkit/

[24] Information on http://www.vistalab.com/commoninjuries.asp

[25] X. Wu, K. Wang and D. Zhang: Proceedings of 2006 International Conference on Computational Intelligence and Security, (2006) November 3-6; Guangzhou, China

[26] Y.L. Zhang, J. Yang and H.T. Wu: Electronics Letters. Vol. 42(4) (2006), p. 204