Implicit Authentication System for Smartphones Users Based on Touch Data

Reham Amin, Tarek Gaber and Ghada ElTaweel

Abstract Currently smartphone' users run many crucial applications (such as banking and emails) which contains a very confidential information. To secure this information, the built in sensors equipped with smartphone devices can be utilized. In this paper, based on these sensors, an implicit authentication system for smartphone's users is proposed. A mobile App is developed to collect the data source of users' biometrics and then features (pressure, position, size, and time) are extracted. classifiers were then applied to decide whether a user is the true owner of device or an impostor. The experimental results showed that our implicit authentication system achieved accuracy of 96.5 % which is better than a related work.

1 Introduction

Mobile computing devices (such as Smartphones and tablets) are worldwide commodities that combine phones and desktop computers characteristics [1]. Market analysis predicts that it will be 640 million tablets and 1.5 billion smartphones in use worldwide by the end of 2015 [2]. Inside these devices sensitive information (such as business secrets and even credit card numbers) is stored. Therefore, it's a nightmare for the owner to lose smartphone [1]. Not only theft but also device share with a guest user (e.g. coworkers, partners or family members) is also considered a disaster [3].

To safeguard this information against unintended usage, such as an impostor accessing the bank account [4], user authentication has been proposed. The two common types of authentication are knowledge based and biometric based [2, 5].

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

T. Gaber
e-mail: tmgaber@gmail.com

T. Gaber
IT4Innovations, VSB - Techincal University of Ostrava, Ostrava, Czech Republic
e-mail: ghada_eltawel@ci.suez.edu.eg

A. Abraham et al. (eds.), *Intelligent Data Analysis and Applications*,
Advances in Intelligent Systems and Computing 370,
DOI 10.1007/978-3-319-21206-7_22

The knowledge based one depends on a secret such as password, PIN [6] and unlock pattern (i.e. match several points on the screen using one move) [1]. Although this type is simple, cheap and quick enough for frequent logins (e.g. unlock patterns) [6], it is more vulnerable to various attacks such as Smudge attack or shoulder surfing attach.

In the other hand, the biometric one depends on unique human characteristics such as keystroke, face unlock, or finger print. This type is much safe and effective to accommodate some of the above attacks. Biometric can't be forged, stolen or borrowed [7, 8]. However, it's limited on accuracy and usability during unlocked state [2, 9]. In general, biometric authentication is divided into physiological and behavioral biometrics [9]. Physiological biometrics depends on what a user already owns. Such as face, fingerprint, voice, iris and hand geometry. This biometrics can't be stolen or imitated in contrast to the knowledge based one [9]. However, this approach is costly (e.g. requires sensors), and requires user interaction (e.g. frequent logins), not to mention the extra load required to authenticate users on smartphones. [10]. Apart from that, behavioral biometrics depends on how the user behaves. Such as gait, location and keystroke patterns. It provides active authentication by using the built-in smartphone sensors [11].

In this paper, we propose an authentication method which depends on the behavioral biometric of the smartphone's users. This method works in the background while user using the phone's keyboard typing phone numbers. It utilizes the various sensors equipped with the smartphone device, thus there is no need for password/PIN (i.e. avoiding password remembering problem and surf attack). Also there is no need for external hardware like the case of physiological based methods. Not to mention ease of use and user intrusive manner in gathering data among other behavioral biometrics (e.g. Gait recognition).

The main contributions of this paper are threefold. Firstly, this paper presenting a touch behavior based authentication system by using only touch data available in most smartphones without using any external hardware. Secondly, developing a mobile App to collect our own dataset from different type of smartphone's users. Thirdly, proposing an implicit authentication approach using our collected dataset and based on SVM and KNN classifier.

The rest of the paper is organized as follows. Section 2 presents a background about authentication system based on touch data and Sect. 3 discusses the related work. Section 4 introduces the proposed system, Sect. 6 concludes and gives some open points for further search.

2 Tapping Background

There are many reasons motivate this work. First of all, data provided by the touchscreen sensors of mobile devices is considerably richer data than that available from personal computer hardware keyboards. The capabilities of such screens could be utilized as input devices of keystroke biometric which is considered as means of authentication on touchscreen devices. Secondly, this biometrics is unique to an

individual and difficult to imitate [12]. Thirdly, even if imposter sees what user input, he couldn't reproduce the user's behavior through shoulder surfing or smudge attacks [1]. This is because of the non-visual cues for tapping behavior. Last but not the least, such mechanism require no extra hardware and done in user intrusive manner as person typed information [10].

2.1 Tapping Types

Types of touch operations include stroke, slide, pinch and handwriting [3, 10].

- Keystroke(Tap): is a finger press on some point of the screen to click item, text, type PIN for example. This type differs when inputting different words.
- Slide: is a finger move (i.e. curve) on the screen to navigate mails, photos, messages or contacts. This type differs on any of 4 directions.
- Pinch: is a two-finger gesture on the screen to read EBook, zoom in/out photo or webpage. This type differs based on case: open or close.
- Handwriting: is a free form gesture for entering characters. This type differs on different letters.

In practice, people interaction with mobile is not limited to these principle gestures, and they may use double touch, open pinch or long press to deal with phone. Such gestures are achieved for daily usage of a fraction less than 5 % [5]. As a result, we neglect other gestures in this paper and focus on the tap gesture.

2.2 Main Modules of an Authentication System Based on Touch Data

To authenticate a user based on touch operations, a user model has to be built for identifying him/her. Building such a model for a legitimate user requires a training phase in which touch data of a labeled user is collected. Then a feature extraction module define what features should be extracted from touch data. Finally, classifier should recognize users based on these features. Again to decide if a user is owner or impostor during authentication phase, feature extraction and classification modules are required. So the main key steps needed to be addressed are what and how. What features to extract (feature extraction's mission during enrollment phase) and how features can be used to recognize user (classifier's mission during verification phase). These modules are shown at Fig. 1.

3 Related Work

There are a number of efforts done to support solutions for implicit authentication for mobile's users. This section discusses a number of these solutions. Latent Gesture [4] collected a suite of behavioral features associated with a user interaction (i.e. touch

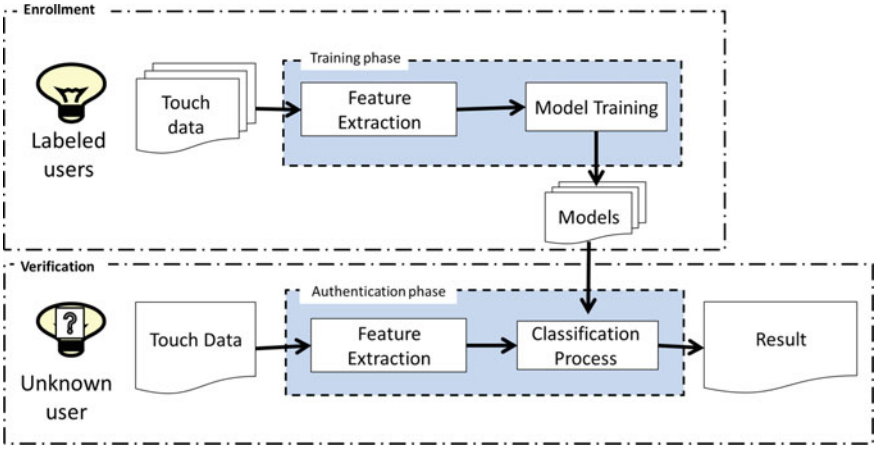

Fig. 1 User authentication typical system [10]

pressure, locations) on common user interface. This method used the common user interface to gather tapping behavior without any user interaction or any external hardware. It also makes usage of Support Vector Machine (SVM) and Random Forests classifiers to achieve the owner's identification which was 96.87 % TPR. However, almost of time the imposter uses this common user interface. This consumes much energy to analyze users interaction continuously.

Jain et al. [12] compared the Equal Error Rates(EER) obtained from the touch screen sensor with the rates of keystrokes in hardware keyboard. A developed keyboard application replaces the system keyboard to capture features in any application that uses a keyboard. The features are then stored in a SQLite database and classified by a one-class SVM. This method achieved EER of 10.5 % for keystroke data, 3.5 % for touch data and 2.8 % for all data (touch and keystroke). However, Additional sensors on the devices, such as gyroscopic and rotational sensors, are ignored in this study. These sensors could differentiate accurately touch data from the keyboard timing data.

Alariki et al. [2] has suggested a framework to be implemented later for authentication using touch biometrics. They review methods and features used for this field. Then, they proposed an approach in which a user has to enter gesture in any direction to build user's model to be matched later through a score computation. However, no implementation is done to show accuracy achieved by the proposed framework.

Table 1 summarizes the related work based on: # of input : needed training samples to build a model for owner, Classifier : classifier used to classify user and give a decision, Performance: performance achieved from the experiment, and Users: Number of users participated in the experiment.

Table 1 Tapping paper summary

Ref.	# of Inputs	Classifier	Performance
[4]	9 per user	Naive Bayes, Random Forests	TPR of 96.87 %
[13]	25 samples per PIN	Z score	EER of 3.65 %
[12]	A single passcode	1 class SVM	EER: 10.5 % Touch, 3.5 % All Data, 2.8 % keystroke
[1]	15009 samples	SVDE libSVM with RBF	EER of 0.5 %
[2]	6 trials per direction	SVM classifier	No implementation
[3]	min 15 samples	SVM classifier	FAR: 18 % for tap, 22 % for fling, 8 % for scroll
[5]	Thousands of actions	SVM classifier	EER of 20 %
[10]	Different inputs	SVM with RBF	EER of 10 %
[14]	Roughly 10 times	Protractor recognition algorithm	EER of 3.34 to 13.16 %

4 Proposed Solution

Our proposed solution consists of three phases: *Data collection, feature extraction and user's classification*. In the data collection phase, we have developed our own mobile App and used it for gathering touch data from different users, students and employees. In the feature extraction phase, from the data collected, the features of the pressure, position, size, and time of pressing were extracted for each user. The classifiers, e.g. SVM, were used in the classification phase to differentiate between the Mobile's owner and the impostor.

4.1 Data Collection

Touch data was gathered from the entered subscriber's code of Egyptian mobile operators (i.e., 0106 for Vodafone, 0128 for Mobinil, 0114 for Etisalat) and from the national landline telecommunication with 0643 code for a local phone code. These codes are chosen because it spans the keyboard: 6 for the leftmost side, 4 for the rightmost, 8 for the downside, 1 and 2 for the upside. While a device's owner uses his smartphone to contact any unsaved number which started with the subscriber's code. A mobile app was developed using Android OS. It was then run on a smartphone of Samsung Galagxy Note N7000.

The touch data was collected by two different modes: Captcha and free entry. For the Captcha mode as seen in Fig. 2, the developed touchscreen number board prompts

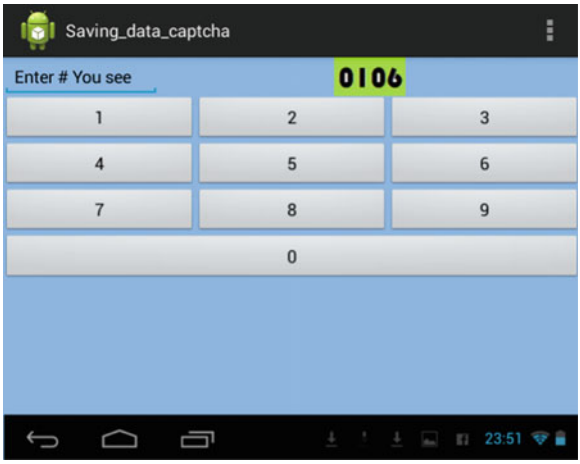

Fig. 2 Screenshot of data collection App: captcha mode

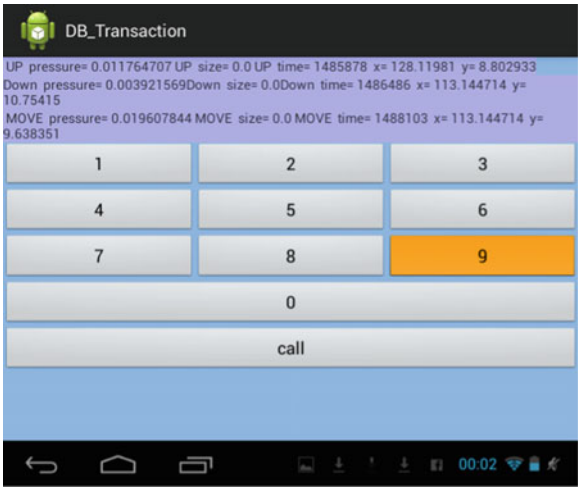

Fig. 3 Screenshot of data acquistion App for free entry

the captcha at the top right of the screen where a user can type in the text field. In our system, Captcha could be any subscription code of the Egyptian mobile operators (e.g. 0106 for vodafone, 0128 for Mobinil, 0114 for Etisalat and 0643 for local land-line phone code). For the **Free Entry mode** , a user could enter any free sequence of numbers, e.g. the full mobile number to complete the code entered through Capcha. Figure 3 shows the layout of free entry Android application for the data collection.

Participants Twelve participants were recruited for collecting touch data. Participants were with age range(20–50) and jobs ranging from faculty students to corporate employees. Also they were mixed between male and female. More details about the participants can be seen in Table 2.

Table 2 Type of participants

Participants	Age	Gender	Job	Used hand
4	22	Female	Undergraduate students	Right handed
2	20	Male	Undergraduate students	Right handed
1	20	Female	Undergraduate students	Right handed
1	23	Female	Employees	Left handed
1	25	Female	Employees	Right handed
1	50	Female	Employees	Right handed
1	28	Male	Employees	Right handed
1	50	Male	Employees	Right handed
12	**Total users**			

All participants followed the detailed procedure described below. They were free to use the mobile with any hand of their hand. One was left-handed and the others was right-hand for typing.

Data Collection Procedure The data collection procedure is described as follows. First of all, each participant has to sign in/up with any chosen username and password. During this process, ID is assigned to each participant to allow anonymous data collection. Secondly, he/she was asked to enter a network operator code for Captcha mode and other numbers for *Free Mode*. In this step, (1) the session lasted for about 20 min where participants sat on a chair and were reminded to enter Captcha code and any chosen number, (2) the phone was held in portrait orientation, (3) the participants were asked to touch screen naturally as they usually do while using their smartphone, and each participant typed 7 taps on the numbers keyboard: 4 in the same order as requested by Captcha and 3 in random order.

Data was submitted with the call key appeared in Fig. 3. Data are stored in Android DB inside mobile device and then exported into Excel file. The number of attempts was unlimited to get as much samples as possible for building the user model. However, the data, from 7 taps from each user's data, was used during the training and testing the system.

4.2 Feature Extraction

From the database collected in the above phase, as shown in Table 3, features of size, pressure, time, and position are recorded when touching any key during the raw touch events(Up, Down and Move). The *Up* action happens when a pressed gesture has finished while the *Down* action takes place when a pressed gesture has started. The *Move* action occurs when a change has happened during a press gesture (between ACTION_DOWN and ACTION_UP) while the *Time* action is the time taken during the pressing action. Table 3 shows the data which gathered from *one single user* using the data acquisition tool when touching some number.

Table 3 Tapping raw data sample

Tap	Pressure			Size			Time in milliseconds			Position					
	UP	DOWN	MOVE	UP	DOWN	MOVE	UP	DOWN	MOVE	UP		DOWN		MOVE	
										X	Y	X	Y	X	Y
1	0.5	0.5	0	0.234	0.234	0	67905343	67905242	0	50	32	50	32	50	32
1	0.45	0.45	0.45	0.2	0.17	0.2	68492904	68488901	68492854	49	42	49	68	49	42
1	0.65	0.65	0.55	0.134	0.134	0.1	69187800	69187686	69187201	94	86	94	86	213	75
2	0.3	0.83	0.3	0.034	0.167	0.04	69373956	69371134	69373906	188	63	169	52	188	63
2	0.99	0.99	0.99	0.2	0.2	0.2	69511770	69511673	69511684	214	57	214	57	214	57
2	1.15	1.15	1.15	0.3	0.5	0.3	69636591	69636421	69636541	237	82	237	82	237	82

These features are collected while tapping "1" and "2" on the developed soft keyboard. In this example, each tap "1" and "2" are repeated for three times. These values are used to build a feature vector for each user. Thus a feature vector for each tap on the screen consists of the shown 15 features for each user. These features can be described as followed:

1. Pressure: the finger's pressure when touching up/down on a soft key. This includes 3 features: pressure at touchup, pressure at touchdown and pressure at touchmove.
2. Size/Orientation: length and orientation of major and minor axes of finger-press. This includes 3 features: size up, size down and size move.
3. Tap timing: times of holding and releasing the soft key. This is also available on hardware keyboards. This includes 3 features: time up, time down, time move.
4. Position: the position where finger touches a soft key with x-y coordinates. This includes 6 features: xposition up, yposition up, xposition down, yposition down, xposition move and yposition move.

4.3 User Classification

The aim of the classification phase is to authenticate the legitimate owner of the smartphone. For this purpose, two classifiers, SVM (Support Vector Machine) with its four kernel functions [15], and the KNN (k Nearest Neighbor) [16] were used.

For training each classifier, supervised learning methods were used to build a classifying model on groups of patterns belonging to both the owner and other user's groups. During the training process, each sample was provided with its known class (user). This model was then used in the authentication phase for an unknown user. By this way, it is possible to authenticate the legitimate owner of the smartphone using his/her touch data.

5 Results and Analysis

A number of experiments were conducting to evaluate the proposed system, i.e. to decide if a user is the legitimate owner of a smartphone or an impostor. The KNN and the SVM with its kernel functions (linear, polynomial, quadratic,RBF, an MLP) were applied to the extract features The results obtained from the classifiers are shown at Table 4.

Our proposed system was evaluated with two well-known methods: error rates and accuracy (i.e. the number of true identification from the number of all identification attempts). For the error rates, the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) were used [9, 10]. The FAR means the probability of accepting an impostor falsely, while the FRR means the probability of rejecting a rightful owner falsely. The FER and FAR are calculated according to Eqs. (1) and (2) respectively.

Table 4 Classifier performance

Classifier	SVM					KNN
	Quadratic	RBF	Linear	MLP	Polynomial	Euclidean distance
FRR	0.0853	0.1067	0.0587	0.7333	0.1040	0.0053
FAR	0.1040	0.0267	0.0907	0.4601	0.2213	0.1387
Correction Rate	83.20 %	89.33 %	89.87 %	48.55 %	67.73 %	96.80 %

$$FRR = \frac{N_{FR}}{N_{IA}} \tag{1}$$

where N_{FR} is the number of false rejections and N_{IA} is the number of identification attempts

$$FAR = \frac{N_{FA}}{N_{IA}} \tag{2}$$

where N_{FA} is the number of false acceptances and N_{IA} is the number of identification attempts

For a good authentication system, FAR and FRR rates should be as small as possible. As it can be seen from Table 4, the smallest value of FRR(0.0053) was achieved by KNN with the Euclidean Distance while the smallest value of FAR (0.0267) was achieved by the SVM with RBF kernel. From these results, the following remarks can be drawn. Firstly, the KNN classifier with the Euclidean Distance was the best by achieving the highest correction rate and the lowest FRR. Secondly, these features are able to distinguish stroke behavior among users (discriminating users). Last but not least, the seven taping of different numbers provided by collected for a participant is encouraging as it the results that even users although users with few times touching the soft keyboard (i.e. only 7 taps) can still be a rich source of data to distinguish among own and impostor.

6 Conclusion and Future Work

This paper presented a proposed system for authenticating smartphone's users based on their behavior while touching their mobile screen. We built our own dataset by developing a mobile App and recruiting a number of participates from different background and ages. Feature are then extracted from the collected data and then SVM with its 4 kernel functions and KNN classifiers are used to classify the legitimate owner of a mobile and an impostor. Our proposed system was evaluated using FRR and FAR error rates. It was found that the smallest value of FRR(0.0053) was achieved by KNN with the Eculidean Distance while the smallest value of FAR (0.0267) was achieved by the SVM with RBF kernel. Also based on the accuracy

rate, it was found that our system is comparable with related work achieving rate at 96.8 %. For the future work, we plan to collect more data by increasing the number of participates and then try other classifiers, e.g. Random Linear Oracle.

Acknowledgments This paper has been elaborated in the framework of the project New creative teams in priorities of scientific research, reg. no. CZ.1.07/2.3.00/30.0055, supported by Operational Programme Education for Competitiveness and co-financed by the European Social Fund and the state budget of the Czech Republic and supported by the IT4Innovations Centre of Excellence project (CZ.1.05/1.1.00/ 02.0070), funded by the European Regional Development Fund and the national budget of the Czech Republic via the Research and Development for nnovations Operational Programme.

References

1. Muhammad S, Alex XL, Arjmand S (2013) Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it. In: Proceedings of the 19th annual international conference on mobile computing & #38; networking. MobiCom '13, New York, NY, USA, ACM (2013), pp 39–50
2. Ala AA, Azizah AM (2014) Touch gesture authentication framework for touch screen mobile devices. J Theor Appl Inf Technol 62(2)
3. Cheng B, Lan Z, Xiang-Yang L (2013) Silentsense: silent user identification via touch and movement behavioral biometrics. In: Proceedings of the 19th annual international conference on mobile computing & networking. MobiCom '13, New York, NY, USA, ACM, pp 187–190
4. Premkumar S, Samuel C, Duen HPC, Hongyuan Z (2014) Latentgesture: active user authentication through background touch analysis. In: Proceedings of the second international symposium of Chinese CHI. Chinese CHI '14, New York, NY, USA, ACM, pp 110–113
5. Cheng B, Lan Z, Xiang-Yang L (2013) Silentsense: silent user identification via dynamics of touch and movement behavioral biometrics. arXiv preprint arXiv:1309.0073
6. Vibha KR (2011) Integration of biometric authentication procedure in customer oriented payment system in trusted mobile devices. Int J Inf Technol Conver Serv 1(6):15–25
7. Kresimir D, Mislav G (2004) A survey of biometric recognition methods. In: 46th International symposium on electronics in Marine. Proceedings Elmar 2004. IEEE pp 184–193
8. Tharwat A, Ibrahim A, Ali H (2012) Personal identification using ear images based on fast and accurate principal component analysis. In: 8th international conference on informatics and systems (INFOS), IEEE MM-56
9. Reham A, Tarek G, Ghada E, Aboul Ella H (2014) Biometric and traditional mobile authentication techniques: Overviews and open issues. In: Hassanien AE, Kim TH, Kacprzyk J, Awad AI (eds) Bio-inspiring cyber security and cloud services: trends and innovations, vol 70. Intelligent Systems Reference LibrarySpringer, Berlin Heidelberg, pp 423–446
10. Hui X, Yangfan Z, Michael RL (2014) Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. In: Symposium on usable privacy and security (SOUPS 2014), Menlo Park, CA, USENIX Association, pp 187–198
11. Hugo G, Sebastian U, Christopher W, Konrad R (2014) Continuous authentication on mobile devices by analysis of typing motion behavior. In: Sicherheit, vol P-228, Gesellschaft fr Informatik, Bonn, pp 1–12
12. Lohit J, John VM, Michael JC, Charles CT (2014) Passcode keystroke biometric performance on smartphone touchscreens is superior to that on hardware keyboards. Int J Res Comput Appl Inf Technol 2:29–33
13. Nan Z, Kun B, Hai H, Haining W (2014) You are how you touch: user verification on smartphones via tapping behaviors. In: IEEE 22nd international conference on network protocols (ICNP), IEEE, pp 221–232

14. Michael S, Gradeigh C, Yulong Y, Shridatt S, Arttu M, Janne L, Antti O, Teemu R (2014) User-generated free-form gestures for authentication: security and memorability. In; Proceedings of the 12th annual international conference on mobile systems, applications, and services, pp 176–189
15. Tharwat A, Gaber T, Hassanien AE, Hassanien HA, Tolba MF (2014) Cattle identification using muzzle print images based on texture features approach. In: Abraham A, Kömer P, Snášel V (eds) Proceedings of the fourth international conference on innovations in bio-inspired computing and application IBICA 2014, vol 303. AISCSpringer, Heidelberg, pp 217–227
16. Tharwat A, Gaber T, Hassanien AE, Shahin M, Refaat B (2015) Sift-based arabic sign language recognition system. In: Afro-european conference for industrial advancement, vol 334. Springer International Publishing, pp 359–370