Poster Abstract: A Multimodal Data Set for Evaluating Continuous Authentication Performance in Smartphones

Qing Yang[†], Ge Peng[†], David T. Nguyen[†], Xin Qi[†], Gang Zhou[†], Zdeňka Sitová[‡§], Paolo Gasti[‡], and Kiran S. Balagani[‡]

[†]Department of Computer Science, College of William and Mary, USA
[‡]School of Engineering and Computing Sciences, New York Institute of Technology, USA
[§]Faculty of Informatics, Masaryk University, Czech Republic

{qyang, gpeng, dnguyen, xqi, gzhou}@cs.wm.edu, sitovaz@mail.muni.cz, {pgasti, kbalagan}@nyit.edu

Abstract

Continuous authentication modalities allow a device to authenticate users transparently without interrupting them or requiring their attention. This is especially important on smartphones, which are more prone to be lost or stolen than regular computers, and carry plenty of sensitive information. There is a multitude of signals that can be harnessed for continuous authentication on mobile devices, such as touch input, accelerometer, and gyroscope, etc. However, existing public datasets include only a handful of them, limiting the ability to do experiments that involve multiple modalities. To fill this gap, we performed a large-scale user study to collect a wide spectrum of signals on smartphones. Our dataset combines more modalities than existing datasets, including movement, orientation, touch, gestures, and pausality. This dataset has been used to evaluate our new behavioral modality named Hand Movement, Orientation, and Grasp (H-MOG). This poster reports on the data collection process and outcomes, as well as preliminary authentication results.

Categories and Subject Descriptors

K.6.5 [**Security and Protection**]: Authentication

General Terms

Measurement, Experimentation

Keywords

Data Set, Continuous Authentication, Smartphone, Behavioral Modality

---

1 Introduction

As smartphones are loaded with an increasing amount of sensitive information, it is critical to prevent unauthorized parties from accessing this data. Traditional authentication mechanisms on smartphones are based on passwords or some specific biometrics (such as fingerprints), which are designed to authenticate the user only at the beginning of a session. Continuous authentication of smartphone users is a promising authentication technique, because it provides non-interruptive identity verification and can therefore be performed during user activity. For most commodity smartphones, one feasible way to implement continuous authentication is using a behavioral modality to capture user's interaction characteristics, which could be formalized as a set of behavioral features. To quantify and evaluate the availability and discriminability of each feature, touch and sensor data invoked by user's interaction on smartphones should be collected by researchers for baseline analysis.

In this project, we collected fine-grained behavior data on smartphones from 120 volunteers, which encompass multiple modalities: movement, orientation, touch, gesture, and pausality. The data were collected under three task scenarios (reading, writing, and map navigation) and two body motion conditions (sitting and walking). This dataset has more modalities and larger scale than any exiting public datasets regarding user's interaction on smartphones. It has been applied to evaluate features in our new behavioral modality named Hand Movement, Orientation, and Grasp (H-MOG). Preliminary results show that H-MOG features have the potential to reduce error rates of state-of-the-art continuous authentication mechanisms that only use touch features or phone movement features, such as [1] .

2 Data Collection Tool and Process

We developed a data collection tool for Android phones to record real-time touch, sensor and key press data invoked by user's interaction with the phone. The system architecture of this tool is illustrated in Figure 1. Three usage scenarios on smartphones are provided: (1) document reading; (2) text production; (3) navigation on a map to locate a destination. User interfaces of these scenarios are shown in Figure 2.

Due to security concerns, the default input method service (IME) in Android OS forbids third-party applications to
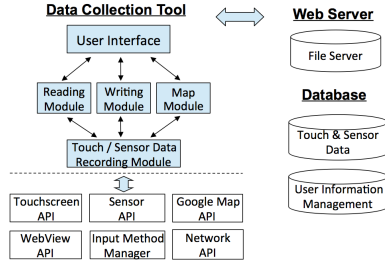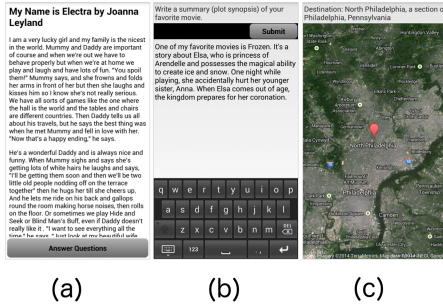
Figure 1. Architecture of Data Collection Tool

Figure 2. User Interface of Data Collection Tool: (a) Reading Task; (b) Typing Task; (c) Map Navigation Task

access touch and key press data from the software keyboard. Thus we developed a customized IME that allows recording these data in the text production scenario.

We recruited 20 volunteers for a pilot study and 100 volunteers for a large-scale data collection. When a volunteer logs into the data collection tool, she is randomly assigned a reading, writing, or map navigation session. One session lasts about 15 minutes, and each volunteer is expected to perform 24 sessions (8 reading sessions, 8 writing sessions, and 8 map navigation sessions). In total, each volunteer contributes about 6 hours of behavior traits.

The collected data are stored in CSV files on the phone as well as uploaded to a server through wireless network. All data are also imported into a MySQL database for subsequent analysis.

3   Data Set Contents

The following 9 categories of data are recorded:

(1) Accelerometer: timestamp, acceleration force along X/Y/Z-axis.

(2) Gyroscope: timestamp, rotation rate along X/Y/Z-axis.

(3) Magnetometer: timestamp, ambient magnetic field along X/Y/Z-axis.

(4) Raw touch event: timestamp, finger count, finger ID, raw touch type, X/Y coordinate, contact size, screen orientation.

(5) Tap gesture: timestamp, tap type, raw touch type, X/Y coordinate, contact size, screen orientation.

(6) Scale gesture: timestamp, pinch type, time delta, X/Y focus, X/Y span, scale factor, screen orientation.

(7) Scroll gesture: starting and current timestamp, X/Y coordinate, and contact size; speed along X/Y coordinate; screen orientation.

(8) Fling gesture: starting and ending timestamp, X/Y coordinate, and contact size; speed along X/Y coordinate; screen orientation.

(9) Key press on virtual keyboard: timestamp, press type, key ID, screen orientation.

At present the total collected data points are: 6×10^7 inertial sensor readings, 4×10^6 raw touch events, 10^6 gestures, and 2×10^5 key press events.

4   Evaluation of H-MOG Modality

We are developing a new behavioral modality named Hand Movement, Orientation, and Grasp (H-MOG), which captures fine-grained spatial-temporal hand movements and oscillations during a user's interaction with the touch screen of smartphone. We formulated about 400 H-MOG behavioral features, which can be categorized into: (1) hand stability features; (2) hand resistance features; (3) touch/gesture features; (4) input pausality features. Each feature is either in the time-domain or frequency-domain.

We used the collected data to preliminarily evaluate the availability and discriminability of H-MOG features. In one instance, we compared the equal error rates (EER) of H-MOG features with touch-based features proposed in [1] by M.Frank, et al. We picked a random subset from the collected data representing the volunteers while performing a reading task. Data from each volunteer was divided into half and half: half for training and half for testing. The results of seven selected users are shown in Figure 3. As observed, H-MOG features are promising to reduce the error rates of continuous authentication over touch-only features. However, more extensive evaluation needs to be done, which should involve data from all volunteers and compare with other state-of-the-art authentication methods.
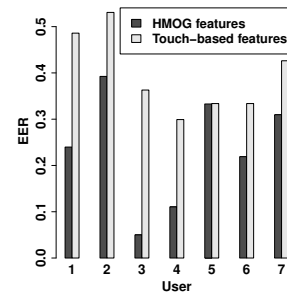

Figure 3. Evaluation of H-MOG Features

5   Work in Process

Based on this dataset, all H-MOG features are being evaluated and compared with other continuous authentication mechanisms. We are also exploring if this dataset could be utilized in other research fields. For example, because it contains user's motion modes (sitting and walking), it might be useful for the evaluation of context recognition models.

6   References

[1] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *Information Forensics and Security, IEEE Transactions on*, 8(1):136–148, Jan 2013.