Pattern Recognition Letters 56 (2015) 7–13

Contents lists available at ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

# Information revealed from scrolling interactions on mobile devices ☆

Margit Antal*, Zsolt Bokor, László Zsolt Szabó

*Sapientia Hungarian University of Transylvania, Tirgu Mures, Soseaua Sighisoarei 1C, Tirgu Mures and 540485, Romania*

ARTICLE INFO

*Article history:*
Received 5 April 2014
Available online 2 February 2015

*Keywords:*
Biometrics
User classification
Gestures
Touchscreen

ABSTRACT

The aim of this study is to analyze information that can be revealed from simple touch gestures such as horizontal and vertical scrolling. Touch gestures contain identity information, they can reflect the user's experience using touchscreen and they can infer the gender of the user. The statements are based on measurements on a large touch dataset collected from 71 users using 8 different mobile devices, both tablets and phones. Touch data were divided in strokes and classification measurements were investigated based on single and multiple strokes. Classification results based on single stroke are inaccurate, which can be improved by using multiple strokes. Measurements prove that identity, gender and user's touchscreen experience level can be accurately predicted from a sequence of 10 strokes. In addition to the different classification results we present statistical analysis of the collected data in order to reveal basic differences between male and female users as well as for less and more experienced touchscreen users.



## 1. Introduction

Each user's interaction with a touchscreen is unique. This unique behavior has been investigated by several researchers proposing authentication schemes based on user's touchscreen dynamics. However, further information may be obtained from touch dynamics. Thus in this paper we propose to study gender and touchscreen usage experience information contained in touchscreen gestures besides identity information. Advertising applications could use gender information in presenting personalized information and games may use touchscreen usage experience to adapt game difficulty for the user.

In order to study the information contained in touchscreen gestures, we designed and developed a client-server application for collecting touchscreen usage patterns from mobile devices. We were interested in the information content of horizontal and vertical strokes, therefore we designed the client application accordingly. In order to collect vertical strokes, users had to read a long text and answer some questions related to it. When collecting horizontal strokes an image gallery was used from which the users had to select their favorite one. The client application was implemented as an Android application, which always starts synchronizing with the server, downloading new texts and images. After the user solves the problems, the generated touch data are sent to the server. The server part of the application permits addition of new texts, images and provides statistics of the collected data.

Although our study is not the only one in this field, its novelty consists in collecting data regarding personal information such as gender, age and touch experience level besides touch information. Consequently, we could perform gender and touchscreen experience level related classifications. Our dataset is also unique in containing data collected from devices with different screen sizes.

The contribution of this work is twofold. We present a dataset containing data from 71 users and 8 mobile devices. Second, we show that beside user identity further pieces of information are contained in touch data, which might be used in applications by adapting the contents to the user. As for the user identity classification results, we can state that using sequences of strokes raises the accuracy of classification. Gender information classification accuracy using only one stroke is quite high, around 88%, which slowly increases using more than one stroke. We noticed that men tend to make shorter and less straight strokes than women. Regarding the users touchscreen experience level we observed that less experienced users tend to make longer strokes with higher velocity.

In Section 2 we present a comprehensive review of the state-of-the-art in touch-based biometrics. Section 3 presents the research aims of our study. In Section 4 our dataset is presented beginning from data acquisition to feature extraction. Section 5 is dedicated to experimental evaluation. User identity, gender and touch experience level classifications are presented using multiple strokes. Beside classification results we present statistical analysis of the collected data in order to reveal main differences between male and female users. The two final sections contain discussions and conclusions.

☆ This paper has been recommended for acceptance by S. Sarkar.

* Corresponding author. Tel.: +40 265 250 620; fax: +40 265 206 211.
*E-mail address:* manyi@ms.sapientia.ro, margitantal68@gmail.com (M. Antal).

http://dx.doi.org/10.1016/j.patrec.2015.01.011
0167-8655/

## 2. Related work

Most desktop computers and mobile devices offer only entry-point based authentication schemes, which usually require a username/password combination. In many institutions people share their authentication data in order to transfer work to other employees. If software was able to continuously track the identity of the user, this abnormal usage pattern would be impossible. Keystroke dynamics [1] is a proposal to solve such usage anomalies. On the one hand it may be used in the username/password typing phase, allowing verification of the user's identity not only by a proper password, but also by typing rhythm, whereas on the other hand continuous authentication would be possible in applications requiring users' typing. Killourhy and Maxion [2] compared several anomaly detectors for keystroke dynamics and identified the best ones. Bours [3] went one step further and proposed continuous, dynamic authentication.

Due to mobile device usage patterns, typing rhythm based continuous authentication schemes are not suitable for smartphones. However, compared to desktop computers, mobile devices are more vulnerable concerning their security. Hence recent studies propose touch-based biometrics instead of keystroke dynamics.

### 2.1. Touch usage based user profiling

Seo et al. [4] conducted two studies for biometric identification based on touchscreen data. In their first experiment only simple touch data were used, such as touch duration, pressure level and the area covered by finger. In their second experiment scroll wheel touch data (strokes) were used in addition to basic touch data. From each stroke start and stop position, speed and stroke length were used. Neither input pattern classification features nor collecting data methods are very clear. However, the paper reports 100% identification accuracy using 12 features and a Back Propagation Neural network (BPN).

A large scale study to observe the users' touchscreen behavior on standard UI elements was conducted by [5]. Hold time characteristics and pressure dynamics of 14000 users through a dedicated game were studied.

Meng et al. [6] present another exploration of touch dynamics for user authentication. The implemented system generates authentication signatures for each session containing 21 features. Users had to complete 6 sessions within 3 days, each lasting for 10 min. The paper reports best error rates using particle swarm optimization (PSO) combined with radial basis function (RBF) network: 2.5% false acceptance rate (FAR), 3.34% false rejection rate (FRR). However, the 10 min session length is a serious limitation of this authentication scheme, as a phone should detect an intruder in a much shorter time.

Damopoulos et al. [7] implemented a touchlogger for iOS based smartphones to demonstrate the ability of touch data for user identification. This paper presents touch data collected through natural usage of smartphones. Participants used their own devices for 24 h, while the touchlogger application running in the background was constantly logging their touch data, which was retrieved from the devices at the end of the experiment. The feature vector contained the $x$ and $y$ coordinates and the timestamp corresponding to the touch event. After feature extraction different supervised machine learning algorithms were tested using Weka. The best error rate was obtained by Random forests: 0.205% equal error rate (EER).

### 2.2. Touch gestures for unlocking devices

De Luca et al. [8] present two experiments using touch strokes for unlocking mobile devices. The aim of the study was to investigate whether it was possible to recognize users based on the way they perform unlocks. The users had to unlock the device using 4 unlock types: horizontal, vertical, diagonal and two-finger vertical strokes. Both experiments were conducted using Android devices and touch data obtained through standard Android API were collected during two sessions. Strokes were compared using dynamic time warping (DTW) algorithm. The best reported accuracy was 57% for diagonal strokes. They concluded that longer time series lead to better results, therefore a second study was designed in order to allow the collection of longer time series. The participants had to unlock their phones once per day for 21 days using password patterns having different levels of difficulties. The best result was 77% accuracy using feature vectors containing pressure, finger area and speed.

Angulo and Wastlund [9] also investigated graphical lock patterns biometrics. Features similar to keystroke dynamics were employed, measuring drawing pattern speed. Neither pressure nor finger area size was employed. A number of 32 users participated in this experiment using an Android application for data collection. A total of 3 graphical patterns were used, each consisting of 6 dots. Fifty trials of each pattern were collected from each user, resulting in 150 trials per user. The paper reports 10.39% EER using Random forests [10] classifier.

Authentication using a set of gestures involving multiple fingers was studied by [11]. A 90% accuracy was reported on a dataset containing data from 34 users by using a single gesture, which can be improved by taking the authentication decision based on multiple gestures. These results are considered to be very promising however, the applicability is still reduced to tablets with large screens due to the special five-finger gestures.

### 2.3. Touch based continuous user authentication

Feng et al. [12] examined gesture based continuous user authentication for the first time. Horizontal, vertical and zooming gestures were involved, reporting classification accuracies separately for each type of gesture. Random forests, Bayes Net and C4.5 (Weka J48) were applied as classifiers. They used 7 consecutive strokes in the authentication measurements, accepting a sequence as valid only if 3 or more strokes are recognized as inputs from the authorized user. Using this setting FAR = 4.66% and FRR = 0.13% were achieved.

Li et al. [13] presented a study related to continuous authentication in which tap, sliding left, right, up and down gestures were collected from 75 users. Data collection was performed in an unsupervised manner, participants were allowed to use the phone without restrictions. The lowest FAR ($\approx$3%) and FRR ($\approx$3%) error rates were obtained when feature vector was computed from a sequence of 14 gestures.

One of the deepest touch data analysis for continuous user authentication is presented by [14]. This thorough paper presents an experiment in which touch data are collected during text comprehension and image comparison tasks. In order to complete these tasks, users had to make several vertical and horizontal strokes using the touchscreen. Forty one users participated in this study in which data were collected in multiple sessions. The authors propose 30 touch features which were evaluated using the k-NN and the SVM (with Gaussian RBF kernel) classifiers. EER less than 4% was achieved using 11 strokes in the long-term authentication scenario.

Micro-movement characteristics of the device were added to the users' touch behaviors by [15] in their SilentSense system. Touchscreen usage actions were classified as tap, scroll (vertical scroll) and fling (horizontal scroll). After 10 user actions, the system identified users with FAR and FRR below 1% using SVM classifier on a dataset containing data from 100 users.

A novel graphic touch gesture feature (GTGF) to extract the identity features from touch strokes was proposed by [16]. A 2.62% EER was achieved on a dataset from 30 subjects using 6 gestures.

Serwadda et al. [17] collected horizontal and vertical strokes from 190 users in 2 sessions. Testing was performed using a sliding window, in which 10 strokes were used to compute a single feature vector. Measurement results are reported based on eight machine learning algorithms and two others using distance metrics. They reported that