Continuous Mobile Authentication using Touchscreen Gestures

Tao Feng*, Ziyi Liu*, Kyeong-An Kwon*, Weidong Shi*, Bogdan Carbunar†, Yifei Jiang‡ and Nhung Nguyen*
*Computer Science Department, University of Houston, Email: tfeng3@cs.uh.edu
†School of Computing and Information Sciences, Florida International University, Email: carbunar@cs.fiu.edu
‡Computer Science Department, University of Colorado Boulder, Email: yifei.jiang@Colorado.EDU

***Abstract*—Securing the sensitive data stored and accessed from mobile devices makes user authentication a problem of paramount importance. The tension between security and usability renders however the task of user authentication on mobile devices a challenging task. This paper introduces FAST (Finger-gestures Authentication System using Touchscreen), a novel touchscreen based authentication approach on mobile devices. Besides extracting touch data from touchscreen equipped smartphones, FAST complements and validates this data using a digital sensor glove that we have built using off-the-shelf components. FAST leverages state-of-the-art classification algorithms to provide transparent and continuous mobile system protection. A notable feature is FAST 's continuous, user transparent post-login authentication.**

We use touch data collected from 40 users to show that FAST achieves a False Accept Rate (FAR) of 4.66% and False Reject Rate of 0.13% for the continuous post-login user authentication. The low FAR and FRR values indicate that FAST provides excellent post-login access security, without disturbing the honest mobile users.

***Index Terms*—Hand-held device, touch-screen, user-authentication**

I. Introduction

Technological advances in computing and I/O capabilities as well as network connectivity are shifting the focus from PCs to mobile devices. Market analysis predicts that in 2015 there will be 1.5 billion smartphones and 640 million tablets in use worldwide [3], [12]. Moreover, companies, universities, and government agencies are increasingly handing out mobile computing systems and applications that allow their employees to work remotely while continuously staying connected to the organization's infrastructure.

The popularity of mobile devices makes them a frequent storage medium for sensitive information (e.g., confidential documents, trade secrets, credentials). As mobile devices are easily lost or stolen, the problem of securing the user access to this data becomes one of paramount importance. As a first defense step, user authentication is quintessential to protecting a system. However, mobile devices introduce a tradeoff between the security and usability of most existing authentication solutions: one-shot authentication solutions are vulnerable to theft and loss [5], while periodic authentication or automatic logouts following periods of inactivity are likely to be counterproductive.

The need for strong authentication is countered by the still clumsy input methodology of such devices and the different user expectations for interaction models, especially when compared to the standard authentication solutions. As shown in a study of over 6,000,000 passwords, 91% of all user passwords belong to a list of just 1,000 common passwords [4] (e.g., 8.5% users use either "password" or "123456" as their passwords). Moreover, the additional hardware cost makes standard biometric authentication techniques to be still unpopular on mobile devices.

To address the pressing demand for a more secure *and* user friendly mobile authentication solution, we design FAST , a touch based seamless user authentication mechanism that supports both passive and continuous authentication for mobile users based on user's touch gestures. FAST takes advantage of the fact that during their interaction with mobile devices, users reveal their unique touch features, such as finger pressure and trajectory, the speed and acceleration of movement.

An essential advantage of our approach is its transparency to the user: the touch data is captured by sensors without disrupting normal user-device interactions. During the post-login stage, the traditional explicit authentication process is triggered only when FAST detects that the current user is likely different from the smartphone owner (i.e., loss or theft of the device).

Furthermore, we have built a a digital sensor glove with IMU digital combo boards ITG3200/ADXL345. The glove provides 6 degrees of freedom and allows us to collect fine-grained biometric information of finger movements. We have used the digital glove to complement and validate touch gesture data. Thus, the main contributions of our work are the following:

- The design of a multi-touch gesture based mobile authentication solution to provide additional enhanced protection of mobile devices.
- Research into using digital sensor gloves, consisting of multiple 6-degrees of freedom IMU sensors, to cross validate and complement the touch gesture based user authentication process.
- An empirical study and evaluation of the applicability of using multi-touch gesture inputs for implicit and continuous user identification, that studies the trade-off between false reject and false accept rates.

The rest of this paper is organized as follows. Section II describes metrics and machine learning classifiers on which we build our solution. Section III describes the overall design of FAST . Details of the equipment we have used and build as well as of the data collection process are described in Section IV. The analysis of our experimental results are explained in Section V. The related work is discussed in Section VI and the final conclusions are presented in Section VII.

II. Background

A. Security vs. Usability Metrics

We use the following two metrics to model the the trade-off between usability and security achieved by an authentication solution.

Definition 1: (FAR) The False Accept Rate (FAR) is the percentage of authentication decisions that allow access to an unauthorized user.

Definition 2: (FRR) The False Reject Rate (FRR) is the percentage of authentication decisions where an authorized user is denied access.

A solution exhibiting a low FAR and a high FRR is more secure but not user friendly. A solution with a low FRR and

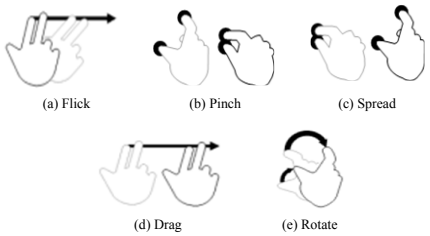


Fig. 1. Example Multi-touch Gestures

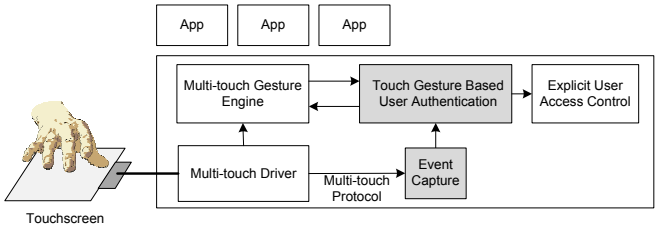


Fig. 2. FAST Design

a high FAR is more user friendly but less secure. Our goal is to minimize both metrics.

B. Classifiers

Our approach relies on classification algorithms for authentication purposes. We have evaluated the use of three classification algorithms, (i) Decision tree, (ii) Random Forest and (iii) Bayes net classifier. We describe each in the following.

Decision Trees.: Decision tree is a popular machine learning approach that can be used to discover patterns in the data and classify data based on the learned patterns. The basic idea of constructing a good decision tree is to build it with high precision and small-scale. It should have the smallest leaf nodes and the depth of the leaf nodes should all be the smallest. Hence a normal decision tree algorithm uses some evaluation method, such as information entropy, to choose an attribute that can best differentiate the data sets, and use it as a decision node and split the data sets in every step.

Random Forest.: Random Forest is an ensemble classifier that consists of many decision trees and outputs the class that is the mode (most frequently occurring) of the class's output by individual trees [1]. It has been widely used in many real-life classification problems, such as image classification [6], object class segmentation [10] and many other applications [9]. Random forest normally selects attributes in the same purpose as decision tree; however, it creates a set of trees. A Random Forest normally selects attributes in a similar manner to decision trees; however, it creates a set of trees.

Bayes Net Classifier.: Bayes net is a probabilistic graphical model algorithm that has been widely applied because of its easy to use and good performance. Formally, Bayesian networks are directed acyclic graphs whose nodes represent random variables in the Bayesian sense. The nodes may be observable quantities, latent variables, unknown parameters or hypotheses. Edges represent conditional dependencies; nodes which are not connected representing variables which are conditionally independent of each other. Each node is associated with a probability function that takes as input a particular set of values for the node's parent variables and gives the probability of the variable represented by the node [2].

III. The FAST Framework and Design

Previous work has explored the feasibility of applying keystroke dynamics and typing patterns for user identification for personal computers – keystrokes can be continually sampled by intercepting output from a keyboard. A study [7] on user's perceptions of authentication on mobile devices shows that users prefer a system that can implicitly and continuously perform user authentication without disrupting the normal user-mobile device interaction. Furthermore, Jakobsson et al [14] proposed an implicit user authentication framework and studied using recorded phone call history and location for continuous user authentication.

Unlike PCs, touchscreen is the primary input medium on smartphones and tablets. Multi-touch inputs embed behavior characteristics that are user specific and can be used for detecting mobile users. We classify touch input into three categories: touch gestures (e.g., flick, spread, pinch, drag, and tap) see Figure 1; virtual typing (e.g, typing using a touchscreen based keyboard, entering a phone number using touch); and touch based drawing (e.g., drawing shapes using fingers). For each category, user specific features can be extracted from traces collected from a device touchscreen.

We propose a touch gesture based user authentication system, FAST (Fingergestures Authentication System using Touchscreen), that focuses on post-login user authentication. Figure 2 shows a high level diagram of the design. As long as the smartphone is used, FAST authenticates the user continuously. After user login, FAST continues to authenticate the mobile user in the background using intercepted touch data from normal user-smartphone interactions. To achieve the objective, FAST relies on gesture based smartphone owner detection. The detection approach is invoked on-demand whenever touch inputs are received and is transparent to the smartphone user. Only when there is sufficient evidence that the current user is not the smartphone owner, traditional user authentication is activated.

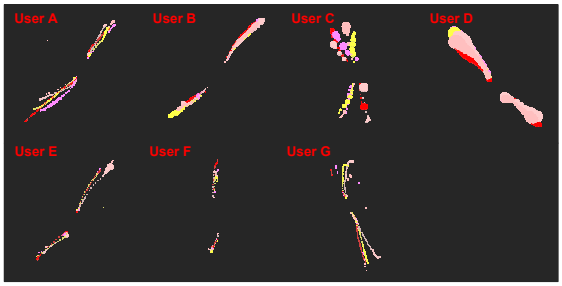
A. Touch Gestures

FAST collects selected touch gesture information including gesture type, X and Y coordinates, directions of the finger motion, finger motion speed, pressure at each sampled touch point and the distance between multi-touch points. In total, there are 53 features for each touch gesture. We consider only the six most frequent and useful gestures: down to up swipe, up to down swipe, left to right swipe, right to left swipe, zoom-in, and zoom-out. Since a smartphone user may apply different levels of touch pressure at different stages of a touch gesture FAST also divides each gesture into three segments, (i) the beginning of a touch motion, (ii) the main touch motion, which is the longest segment and (iii) the end of a touch motion.

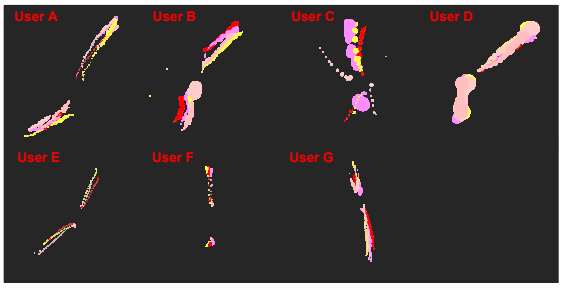
We have implemented an Android application that collects touch information from touchscreen equipped smartphones. In a preliminary user study, we have collected the touch inputs of 7 users (three females and four males). Each user was asked to perform a set of touch related tasks, including controlling the smartphone UI using flick touch gesture (left-to-right flick, right-to-left flick), mobile web browsing using pinch and spread touch gestures, dragging icons and drawing simple shapes using finger touch. Each task was repeated multiple times by the same user.

Figure 3(a) shows sample spread touch traces of the seven tested users. Each subfigure cell contains plotted traces of one user. In each subfigure, traces from different test trials are plotted using different colors. For each touch trace, the size of trace dots increases with the level of touch pressure.

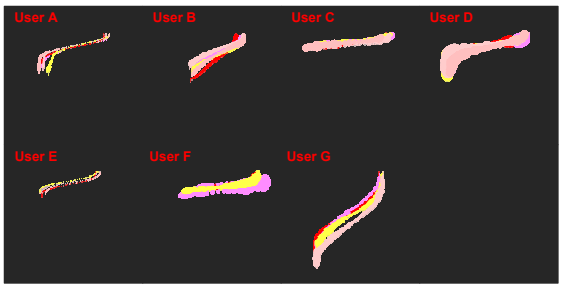
Figure 3(b) contains pinch touch traces of the same seven tested users. Similar to the plotted spread traces, each subfigure cell shows plotted traces of one user. As indicated by Figure 3(a) and (b), each user has his/her own distinctive spread



(a) Sample Spread Profiles of Seven Users



(b) Sample Pinch Profiles of Seven Users



(c) Sample Flick Profiles of Seven Users

Fig. 3. Sample Multi-touch Traces from Users

touch style. No two of the seven users share the exact same spread touch style. For the same user, there is high degree of consistency that the same user exhibits similar spread and pinch touch style. Though collected from different trials, some of the spread touch trace patterns of the same user match with one another almost perfectly.

Figure 3(c) shows sample flick touch traces of the seven tested users. Different from spread and pinch, a flick is a single finger gesture. Each subfigure cell contains plotted traces of one user. In each subfigure cell, the horizontal-axis denotes screen location translation and the vertical-axis denotes time. Each cell of figure 3(c) shows traces from different test trials using different colors. For each trace, the size of the trace dots increases with level of touch pressure. By observing the traces, one can find that for each trace, there was a finger acceleration stage, a steady movement stage (middle section of each flick trace), and a deceleration stage. FAST extracts steady touch pressure, minor/major ratio, steady finger moving speed, and acceleration/de-acceleration speed as features.

Furthermore, FAST complements touchscreen gesture information with information collected from a digital sensor glove. The glove provides X, Y, and Z axis angular rate information, the yaw, pitch and roll of finger movements, for a total of 36 additional features. We use these features to validate and complement touch gesture extracted features, for the user authentication process that occurs during normal smartphone interactions. Our intuition is that additional insight can be obtained by examining touchscreen traces and finger motion sensor data together.

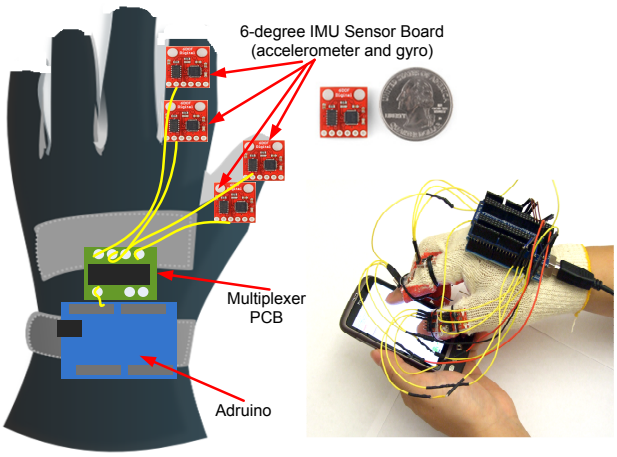


Fig. 4. The Sensor Glove with 6-degree IMU Boards

B. FAST : Putting It All Together

FAST collects, separates and stores the above three types of data, into two databases. One database is used for training classifiers and the other for testing the trained classifiers. Collected touch inputs are split between the two databases to avoid over-fitting.

FAST uses the classifiers described in Section II to classify a mobile phone user based on her touch behavior. FAST uses the results of the classification to improve smartphone security in the following scenario. In the post-login stage, FAST extracts touch gesture and digital sensor glove features and uses them to authenticate the user.

Care must be taken to achieve the proper balance of the FAR and FRR values. During the post-login stage, due to the constant user monitoring and frequent transparent authentication based on touch gestures and sensor glove inputs, a low FRR is the primary objective – during normal user-smartphone interactions, usability is more important. This is because the frequency of the authentication operations ensures a rapid detection of intruders even for larger FAR values.

Touch Sequence Length and Authentication Threshold.: During the post-login phase, FAST continuously monitors the authenticity of the mobile user in a user transparent fashion. FAST achieves this by intercepting touch gestures and virtual typing inputs, and strives to achieve a low FRR. However, a user's touch gestures and corresponding sensor glove inputs may vary in time. Thus, a user authentication solution that relies on just single input instances of touch gestures is unlikely to be reliable and accurate.

Instead, FAST adopts an aggregated authentication approach where results from a sequence of touch instances are combined. To control the quality of the aggregated user verification performance, FAST uses two metrics: the *Touch Sequence Length*(TSL), the length of touch input sequences and (ii) the *Authentication Threshold*(AT), for aggregating results. The AT metric is used to provide the lower bound on the touch sequence length: If the number of accepted touch inputs during one sequence is below the threshold, FAST considers that the current user is unauthorized and invokes an explicit authentication process.

IV. Experiment Setup

A. The Equipment

To evaluate the ability of FAST to authenticate users, we have used the following equippment.

Sensor glove.: We have created a digital sensor glove with IMU digital combo boards ITG3200/ADXL345. The glove provides 6 degrees of freedom and allows us to collect fine-grained biometric information of finger movements. This includes the three angle information: yaw, pitch, and roll, which is computed from the output of the three accelerometers on the digital combo board. The ITG-3200 is a single-chip, digital-output, 3-axis MEMS gyro IC. It outputs X-, Y-, and Z-Axis angular rates with a sensitivity of 14.375 LSBs per /sec and a full-scale range of 2000/sec. The ITG-3200 has three internal 16-bit analog-to-digital converters. The ADXL345 is a small 3-axis accelerometer with high resolution (13-bit) measurement at up to 16 g.

Smartphone.: We used several HTC Android smartphones (Sensation model) for data collection. The model features a 4.3 inch capacitive S-LCD Gorilla glass touch screen with qHD (540960) resolution at 256.15 PPI. We have developed an Android program for collecting touch gesture data from the HTC smartphones.

B. Glove Data Collection

We have divided the participants in a user study into two groups: the users in one group were equipped with a digital sensor glove, the users in the other group were not. All the participating users were asked to perform smartphone functionalities using common touch gestures (i.e., zoom-in, zoom-out, spread). The participant's touch gesture data were collected and stored.

40 subjects participated in the study. 11 users first joined the experiment with digital glove. However, for comparison, we have also collected their data without wearing the digital glove. Furthermore, because in the common case, people using mobile phone were not wearing a digital glove, we collected the 40 subjects' touch gesture data without digital glove and stored in another database.

We have worked with the IRB at University of Houston, where the experiment was conducted, to ensure an ethical design of the experiment. Participants were provided with a written consent form, including sections that describe the purpose of the study, its duration, the right to withdraw from participation and to refuse participation, the confidentiality of the information obtained and the use of research results. Participants were required to sign the form before participating in the experiment.

V. Experimental Results

All the results shown in this section are discussed in comparison with a baseline mobile authentication solution that does not apply user specific touch behavior for authentication and does not perform continuous user verification using touch inputs after login. We denote this solution by BASE.

The security of BASE fails if the attacker has physical access to the mobile device that is in a post-login state. That is, BASE achieves a FAR of 100%: it does not authenticate the user following the login procedure. The FRR value of BASE is 0%.

In contrast, FAST exploits user specific touch gesture behaviors to improve mobile device security. We quantitatively evaluate the security improvements of FAST by comparing its FAR value with the FAR of 100% of BASE. We measure FAST 's usability in terms of its achieved FRR, where a smaller FRR means higher usability.

A. Touch Gestures With Sensors

For multi-touch gestures involving two fingers, the set of touch related features include, gesture types, sampled locations of the two fingers, directions of the touch motion of the two fingers, time and pressure history of touch points, and the distances of the two touch points. Furthermore, with the help of the digital sensor glove, some more user specified biometric features can be acquired and applied for user classification such as the X-, Y-, and Z-Axis angular rates of fingers when performing touch gesture inputs. We applied the three algorithms, Random Forest, J48 Decision Tree, and the Bayes Net on the collected touchscreen and sensor glove data. The performance results achieved are shown in Figure 5.

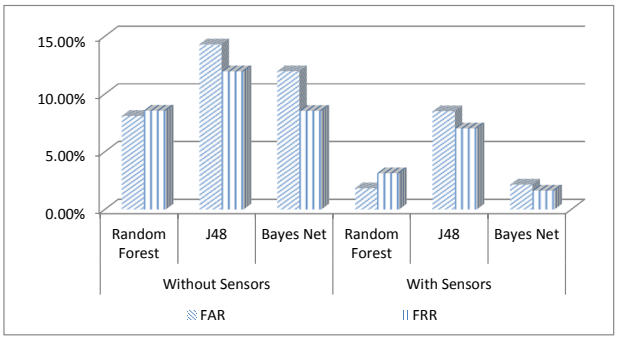


Fig. 5. The Comparison of Data with Sensor Features and Data without Sensor Features

As indicated by Figure 5, for both data with additional sensor glove information and data without sensor glove information, the Random Forest Classifier always outperforms the other two classification algorithms in terms of FAR value. However, the Bayes Net classifier always outperforms the other two in terms of the FRR metric. Since during the post-login stage, it is critical not to annoy the user and interrupt normal smartphone interaction with explicit access control activated by false rejection, we choose the Bayes Net classifier.

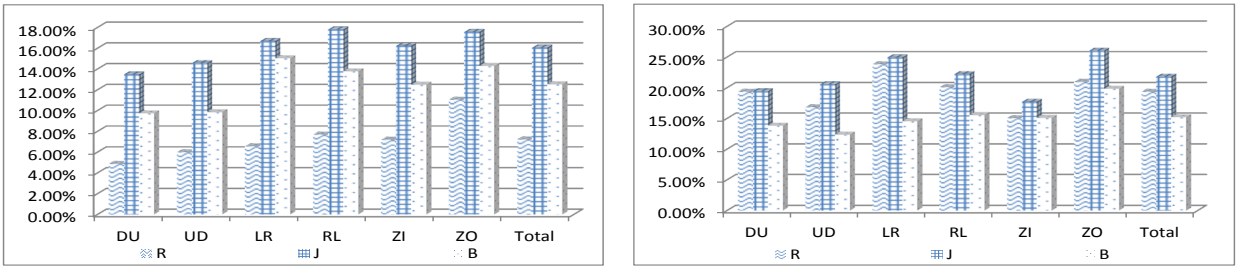
Furthermore, for all the three tested classifiers, the results achieved with the sensor glove information significantly exceed the results achieved without it. FAST achieves a FAR of 11.96% and a FRR of 8.53% without external sensor information, when applying the Bayes Net classifier for single touch gestures. When additional sensor glove information is present, FAST achieves a FAR of 2.15% and a FRR of 1.63%. This suggests that touch gestures of different people and smartphone touch gestures can be used as a source of information for user authentication. Furthermore, this also indicates that the biometric information acquired from the digital sensor glove is helpful in authenticating the users when combined with the touchscreen inputs.

B. Touch Gestures Without Sensors

We further continued the user study using the touch gesture data of the 40 participants when no additional sensor glove information is available. We performed this in order to simulate the normal user-to-smartphone interaction conditions.

We applied the same three algorithms, Random Forest, J48, and Bayes Net as the classifiers. The results are shown in Figure 6. R, J, and B respectively stand for Random Forest, J48 Decision Tree, and Bayes Net. The data sets are divided according to the gesture types: DU, UD, LR, Rl, ZI, ZO and Total respectively stand for, swipe from down to up (DU), swipe from up to down (UD), swipe from left to right (LR), swipe from right to left (RL), zoom-in (ZI), zoom-out (ZO) and the overall performance of all the combined gesture types (Total).

Figure 6 shows that the Random Forest classifier always performs better than the other two classifiers in terms of



(a) FAR (False Accept Rate)

(b) FRR (False Reject Rate)

Fig. 6. The FAR and FRR of Different Algorithms and Gesture Types

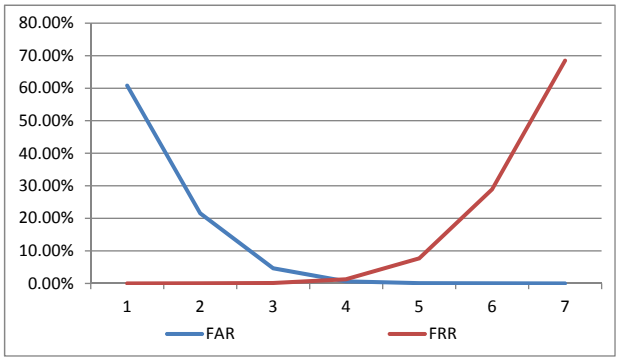


Fig. 8. FAR and FRR of different sequence-based threshold values.

FAR. However, in terms of FRR, it performs worse than the Bayes Net. Although FAST can achieve, on average, a 14.02% FAR and a 18.92% FRR using the Bayes Net classifier using limited data provided by a single touch gesture, it is still not good enough for meeting the design requirement of low FRR. Consequently, we proposed a sequence-based authenticate mechanism. It is described below.

Gesture Sequence Based Authentication.: Figure 7 shows the FAR and FRR values achieved by FAST as a function of the Touch Sequence Length (TSL) metric introduced in Section III. The x-axis shows the TSL value of an authentication cycle and the y-axis shows the best FAR and FRR values that can be achieved under the TSL. It shows that the best FAR/FRR combination is achieved when the TSL is 7. Thus, we set TSL to 7.

Furthermore, Figure 8 shows the FAR and FRR values under an AT of 2 (FAR=21.54% and FRR=0.01%) and an AT of 3 (FAR=4.66% and FRR=0.13%). Thus, both values are applicable for authentication purposes. Since the FAR of AT=3 is significantly smaller than for AT=2, we choose AT=3. This means that for every 7 valid touch gestures, if 3 or more gesture inputs are recognized as inputs from the authorized user, then this input sequence is accepted as being valid – the user is authenticated. Otherwise, the input sequence is considered as an unauthorized sequence.

An FRR of 0.13% is equivalent to one wrong user logout every 800 touches or about 1 hour of continuous system use. A FAR of 4.66% means that after 3 attempts, an unauthorized user will be still authorized with a probability of 0.01%. Thus, FAST's gesture sequence-based authentication mechanism provides strong post-login security protection while significantly reducing user interruptions.

Furthermore, FAST uses a time threshold of sixty seconds to limit the valid time window size of an unfinished gesture input sequence. This means that if a gesture sequence is incomplete and there are no more gesture inputs for more than sixty seconds, a new sequence will be created upon receipt of the next touch gesture input with the unaccepted touch number of the previously incomplete sequence. This time threshold is set to protect the system in the case where an attacker continues to use the device left off by an authorized user who has already completed several gesture inputs.

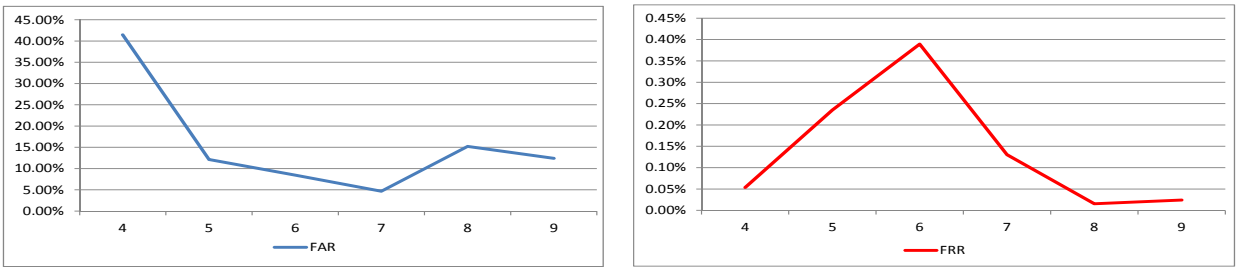
VI. Related Work

In general, there are three kinds of user authentication approaches: "what you have", "what you know", and "who you are". The approach of "what you have" relies on a smartcard, a USB thumb drive, or some other types of objects which users must have. Smartcards and USB drives must be physically inserted into the computer in order to authenticate user. However, a mobile phone itself can be considered as a token of "what you have", and the challenges are associated with lost control of the smartphone token itself.

The arts of the approach "who you are" can be categorized into two groups including implicit user identification and multi-modality pattern classification, especially, multi-modality biometrics.

For desktops, researchers in the past explored the feasibility of applying keystroke dynamics and typing patterns for user identification. Keystrokes can be continually sampled by intercepting output from a keyboard. Ailisto et al. [17] used accelerometers in television remote controls to identify individuals. Cuntoor et al. [8] and Gafurov et al. [11] experimented user identification using gait analysis and recognition. Koreman and Morris et al. [16] proposed a continuous multi-modal based approach for user identification. In [14], Jakobsson et al proposed an implicit user authentication framework and studied using recorded phone call history and location for continuous user authentication.

Some research efforts were conducted on graphical authentication method that uses the implicit drawing features to authenticate users. Jermyn, et al. [15] proposed a technique – "Draw a secret (DAS)". Users will draw a graph on a 2D-grid, and the information about which a grid is occupied, and in which orders will be recorded. When trying to login, users will repeat the drawing. According to Jermyn et al., a relatively small grid is in fact secure enough. But according to Thorpe et al.'s study [19], DAS's security perhaps is not so good as once believed. In the real world, people usually use signature to prove their identities. So it is natural that Syukri et al. [18] proposed similar method in the cyber world. In their scheme, users need to draw their signatures with mouse, and system will normalize the data and record them into a database. During authentication, the system will extract the characteristics from the newly entered signature, and compare them with the pre-stored version. Furthermore, Varenhorst, et al. [20] proposed a method of drawing doodles rather than signatures. They used several methods to analyze the data,



(a) FAR (False Accept Rate)

(b) FRR (False Reject Rate)

Fig. 7. The FAR and FRR under different sequence length values.

including grid, speed, doodle variance and a combination of all the above and achieved very high accuracy based on their evaluation.

There has been a body of literature on combining multiple biometric inputs to produce aggregated user identification results. In [13], Indovina et al. identified that biometric integration can occur on the feature level, or the score level. In feature level integration, all of the initial features from measurements are grouped together into a single feature vector for classification. Although the most information is available at this point, feature-level integration suffers from the so-called curse of dimensionality. Additionally, the features of some measurements may not always be available.

VII. Conclusion

This paper presents a novel touch-screen based user authentication approach for mobile devices, named FAST . FAST provides enhanced security for mobile systems by using touch gestures as input. Furthermore, FAST relies on a digital sensor glove that we have built, that enables the collection of additional gesture information. This information is used in conjunction with the touch gesture data. Following login, FAST authenticates the mobile user in the background using touch gestures intercepted from the normal user-smartphone interactions and from the sensor glove.

FAST achieves a good balance between security and usability during the continuous user verification stage by maintaining low false reject rates (FRR). FAST improves the security protection provided by solutions that do not use post-login authentication protection mechanisms. Specifically, quantitative evaluations using touch gestures collected from 40 users, show that when using state of the art machine learning based classifiers, FAST achieves a FAR of 4.66% with a FRR of 0.13% . The low FRR indicates that FAST is usable: an honest user can perform 800 touch gestures (the equivalent of using the device for an continuous hour) without being interrupted to perform an explicit authentication.

References

[1] http://en.wikipedia.org/wiki/Random_forest.

[2] http://en.wikipedia.org/wiki/Bayesian_network.

[3] Worldwide smartphone markets: 2011 to 2015 - analysis, data, insight and forecasts. http://www.researchandmarkets.com/research/7a1189/worldwide_smartpho.

[4] More top worst passwords. http://xato.net/passwords/more-top-worst-passwords#more-269, 2010.

[5] Altinok, A., and Turk, M. Temporal integration for continuous multimodal biometrics. In *Multimodal User Authentication '03* (Santa Barbara, CA, 2003), pp. 11–12.

[6] Bosch A, Z. A., and X, M. mage classification using random forests and ferns," in computer vision. *ICCV 2007* (Oct 2007), 1–8.

[7] Clarke, N. L., and Furnell, S. M. Authenticating mobile phone users using keystroke analysis. *Int. J. Inf. Secur. 6* (December 2006), 1–14.

[8] Cuntoor, K. R., Kale, A., Rajagopalan, A. N., Cuntoor, N., and Krger, V. Gait-based recognition of humans using continuous hmms. In *Fifth IEEE International Conference on Automatic Face and Gesture Recognition* (2002), pp. 321–326.

[9] D Richard C, Thomas E Jr, K. B. A. C. K. H. J. G., and L, J. Random forests for classification in ecology. *Ecology 88* (Nov 2007), 2783–2792.

[10] Florian S, A. C., and Z, A. Object class segmentation using random forests,. *British Machine Vision Conference (BMVC)* (Sep 2008), 1–4.

[11] Gafurov, D., Helkala, K., and Soendrol, T. Biometric gait authentication using accelerometer sensor. *Int. J. Inf. Secur. 1* (2006), 51–59.

[12] Huberty, K., Lipacis, M., Holt, A., Gelblum, E., Devitt, S., Swinburne, B., Meunier, F., Han, K., Wang, F. A., Lu, J., Chen, G., Lu, B., Ono, M., Nagasaka, M., Yoshikawa, K., and Schneider, M. Tablet demand and disruption: Mobile users come of age, 2011.

[13] Indovina, M., Uludag, U., Snelick, R., Mink, A., and Jain, A. Multimodal biometric authentication methods: A cots approach. In *Proc. MMUA 2003, Workshop on Multimodal User Authentication* (2003), pp. 99–106.

[14] Jakobsson, M., Shi, E., and Chow, R. Implicit authentication for mobile devices. In *4th USENIX Workshop on Hot Topics in Security (HotSec '09)* (Montreal, Canada, August 2009).

[15] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D. The design and analysis of graphical passwords. In *Proceedings of the 8th conference on USENIX Security Symposium - Volume 8* (Berkeley, CA, USA, 1999), USENIX Association, pp. 1–1.

[16] Koreman, J., Morris, A. C., Wu, D., Jassim, S., Sellahewa, H., Ehlers, J., Chollet, G., Aversano, G., Bredin, H., Garcia-salicetti, S., Allano, L., Van, B. L., and Dorizzi, B. Multi-modal biometric authentication on the securephone pda. In *Proc. MMUA Workshop on Mult-Modal User Authentication* (Toulouse, France, May 2006).

[17] Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., marja Makela, S., and Ailisto, H. Identifying users of portable devices from gait pattern with accelerometers. In *IEEE International Conference on Acoustics, Speech, and Signal Processing* (2005).

[18] Syukri, A. F., Okamoto, E., and Mambo, M. A user identification system using signature written with mouse. In *Proceedings of the Third Australasian Conference on Information Security and Privacy* (London, UK, 1998), ACISP '98, Springer-Verlag, pp. 403–414.

[19] Thorpe, J., and van Oorschot, P. C. Graphical dictionaries and the memorable space of graphical passwords. In *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13* (Berkeley, CA, USA, 2004), SSYM'04, USENIX Association, pp. 10–10.

[20] Varenhorst, C. Passdoodles; a lightweight authentication method. In *Proceedings of the 9th international conference on Multimodal interfaces* (2007), ICMI '07, pp. 236–239.