PACIS 2020 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-22-2020

What is More Important for Touch Dynamics based Mobile User Authentication?

Kanlun Wang

Lina Zhou

Dongsong Zhang

Zhihui Liu

Jaewan Lim

What is More Important for Touch Dynamics based Mobile User Authentication?

Completed Research Paper

Kanlun Wang
UNC Charlotte, BISOM
Charlotte, USA
kwang17@uncc.edu

Lina Zhou
UNC Charlotte, BISOM
Charlotte, USA
lzhou8@uncc.edu

Dongsong Zhang
UNC Charlotte, BISOM
Charlotte, USA
dzhang15@uncc.edu

Zhihui Liu
UNC Charlotte, CS
Charlotte, USA
zliu15@uncc.edu

Jaewan Lim
UNC Charlotte, BISOM
Charlotte, USA
jlim13@uncc.edu

Abstract

Mobile user authentication (MUA) has become a gatekeeper for securing a wealth of personal and sensitive information residing on mobile devices. Keystrokes and touch gestures are two types of touch behaviors. It is not uncommon for a mobile user to make multiple MUA attempts. Nevertheless, there is a lack of an empirical comparison of different types of touch dynamics based MUA methods across different attempts. In view of the richness of touch dynamics, a large number of features have been extracted from it to build MUA models. However, there is little understanding of what features are important for the performance of such MUA models. Further, the training sample size of template generation is critical for real-world application of MUA models, but there is a lack of such information about touch gesture based methods. This study is aimed to address the above research limitations by conducting experiments using two MUA prototypes. Their empirical results can not only serve as a guide for the design of touch dynamics based MUA methods but also offer suggestions for improving the performance of MUA models.

Keywords: Mobile user authentication, touch dynamics, feature importance, template generation

Introduction

The wide adoption of mobile technologies makes it convenient to access and store information. In particular, a tremendous amount of confidential information and personally sensitive and private data are being stored on mobile devices (Gubernatorov et al. 2020). MUA aims to prevent unauthorized access to mobile devices and protect them from security threats that may compromise the confidentiality, privacy, and integrity of the data stored therein (Kunda and Chishimba 2018). However, traditional MUA methods are insufficient to protect users against malicious activities because emerging technologies continuously change methods, consequently making mobile devices vulnerable to such threats (Khan et al. 2015). Touch dynamics, a process of tracking human touch motion on mobile screens, has attracted increasing attention in MUA research in recent years (Zhang et al. 2019). Touch dynamics based MUA has the potential to make mobile devices resistant to security threats such as smudge trace and shoulder surfing attacks (Abuhamad et al. 2020; Zhao et al. 2014; Zhou et al. 2016). Thus, it can be portrayed as an additional safeguarding mechanism for protecting users' mobile devices.

Touch dynamics can be captured from keystroke based behaviors (Raul et al. 2020; Shekhawat and Bhatt 2019) or touch gesture based behaviors such as swiping and pinching (Zhou et al. 2016). However, previous studies have yet to draw a comparison of these two types of touch dynamics based MUA methods to date. In addition, there is an increasing amount of research that incorporates touch dynamics into the development of MUA methods (e.g., Aviv et al. 2012, Meng et al. 2014). These methods typically rely on classification models to determine whether a mobile user is authenticated or not (e.g., Tse and Hung 2019, Zhou et al. 2016). The focus of the research is on improving the effectiveness of MUA models by exploring a variety of touch behavioral features. Nevertheless, there is a lack of a systematic understanding of what features are more important for MUA and how to categorize different features to better guide the process of feature selection. Another important issue associated with the performance of MUA models is the training sample size. In general, the enrichment of training data is an effective way to improve the quality of the generated model (Polyzotis et al. 2017). In contrast, an intelligent training sample can make a positive contribution to classification (Foody and Mathur 2004). This issue has been overlooked in previous studies.

This study aims to address the above research limitations by answering the following research questions: 1) How do touch gesture based MUA methods compare with keystroke based MUA methods in terms of their authentication performance? 2) What is the minimal size of training samples for a touch gesture based MUA method to achieve its near-optimal performance? 3) What are the most important features for touch gesture based MUA? To answer the research questions, we conducted a user experiment that examines two types of touch dynamics based MUA methods.

Related Work

In this section, we first provide an overview of touch dynamics based MUA methods, followed by a categorization of touch gesture based features. Finally, we summarize the machine learning techniques used in previous MUA studies and their reported performances.

Touch Dynamics Based MUA Methods

Given the innovations of modern technologies especially on touchscreen mobile devices, touch dynamics based MUA has recently drawn increasing attention in the research community (Ferrag et al. 2019). It is a process of performing MUA or recognition by measuring human touch rhythm on touchscreen mobile devices (Teh et al. 2016). Via the lens of user identification, touch dynamics authentication can be dated back to the 1860s when people started using telegraphs. Telegraphers identified one another via the way people tapped on the keys (Bryan and Harter 1897). Owning to the introduction of PC along with keystroke-based keyboards, researchers identified that PC users' typing patterns could be used as a personal identifier (Obaidat and Sadoun 1996). Therefore, a host of research studies have been carried out to investigate keystroke dynamics based authentication (e.g., Crawford 2010, Venugopal 2020). In light of the increasing adoption of touch-screen mobile devices, more and more researchers are shifting their focus to touch dynamics based MUA.

Touch dynamics based authentication offers several unique characteristics and advantages. For instance, distinctiveness is one of the sophisticated features of touch dynamics because its patterns are capable of generating multi-dimensional features (e.g., temporal and spatial features) and are difficult to replicate (Zheng et al. 2014). Touch dynamic based MUA also offers a continuous monitoring mechanism by constantly monitoring a user's touch behavior patterns (Dee et al. 2019; Zhou et al. 2016). As an addition to the usability of MUA methods, revocability (e.g., a new touch dynamic template can be easily generated for template replacement), non-dependency (e.g., the surrounding lighting and background noise would not impact the authentication), and transparency (e.g., the system requires little or no additional interventions from a mobile user) are all associated with touch dynamics based MUA.

There are two general types of touch dynamics used in MUA, including keystroke based and gesture based touch dynamics. Touch dynamics can add another safeguarding dimension to passcode, so that even if someone steals another person's passcode, he or she may not be able to access the latter's device because they have different touch dynamics (Zhang and Tao 2019). Keystroke based MUA authenticates users based on their typing behavior patterns (Raul et al. 2020; Shekhawat and Bhatt 2019). Touch gesture is another type of touch dynamics, which is based on users' touch strokes (Zhang et al. 2019). To name but a few, HATS (Zhou et al. 2016) integrates password, gesture, and keystroke as a whole to authenticate a user. In addition, Balducci et al. (2019) used users' swiping behaviors to classify negative affective states, and Zhang et al. (2019) investigated swipe-based behaviors by capturing users' four different swiping orientations in one-handed gesture, including vertical scroll-up, vertical scroll-down, horizontal scroll-left, and horizontal scroll-right. Touch dynamics can be further integrated into a cloud environment to reduce the workload on local mobile devices (Lin et al. 2020). On the other hand, research on touch dynamics based MUA is still in its early stage and several challenges remain to be addressed (Rashid and Chaturvedi 2019).

Features of Touch Dynamics

Feature extraction has been widely used in improving data representation. In the context of MUA, it is essential to extract distinguishable human behaviors. There are three major categories of features of touch dynamics, namely timing features, spatial features, and motion features (Teh et al. 2016). Timing features refer to two main time events, with one being dwelling time that is the duration of a touch event with the same key/stroke and the other being flight time that is the time interval between two consecutive keys (Yong Sheng et al. 2005). Spatial features refer to the interaction between a fingertip and a touchscreen surface, usually consisting of touch size, touch pressure, and touch position (Meng et al. 2014). Touch size represents an approximation of the area where the screen is being touched (Zheng et al. 2014), while touch pressure is an approximated finger force on a touchscreen (Dee et al. 2019). A touch position is a measurement of a landing location on a touchscreen associated with the two-dimensional matrix feature (Kolly et al. 2012). Motion features are normally captured by an accelerometer or a gyroscope sensor equipped in modern mobile devices. They represent a three-dimensional feature (Aviv et al. 2012). There has been a discussion in selecting different sensors to accurately extract features (Cai and Chen 2012; Giuffrida et al. 2014). Recent research focused on extending features through mathematic or statistic transformation to improve classification accuracy (Frank et al. 2013; Gong et al. 2016; Teh et al. 2019). For instance, features can be extended to the first-order and the second-order features using a transformation of statistics metrics (Teh et al. 2019), or the ramifications of raw data can be extended to movement direction features and operation features (Frank et al. 2013; Gong et al. 2016; Zhou et al. 2016).

Machine Learning Techniques for MUA

The state-of-the-art classification techniques are effective in distinguishing the authenticity and ownership of an authentic user (e.g., Balducci et al. 2019, Zhou et al. 2016). Zhou et al. (2016) showed that touch gesture based MUA outperformed keystroke based MUA using a number of classification models such as Naïve Bayes (NB), K-nearest Neighbor (KNN), Decision Tree (DT), Neural Network (NN), Random Forest (RF), and Support Vector Machine (SVM). Their results suggested that the NN and RF achieved about 75~76% accuracy. Zhang and Tao (2019) examined senor data consisting of two different PINs ("182537" and "111111") and achieved the highest authentication accuracy of 99% with RF classifier. Balducci et al. (2019) used users' swiping behavioral data covering 14 different features, demonstrating that touch dynamics could successfully classify personal negative emotional states. Since one-handed gesture is one of the most commonly used gestures in human interaction with mobile devices (Wang et al. 2019), Zhang et al. (2019) investigated single-handed thumb-based swipes with the implementation of classification models. More interestingly, there is strong evidence showing that the integration of keystroke based and touch gesture based user behavioral data has the potential for more accurate prediction, with Logistic Regression (LR) performed the best (Tse and Hung 2019). A summary of the reviewed studies, the machine learning techniques used, and their best performance is presented in Table 1.

Our review of the related work shows that there has been much recent development in touch dynamics based MUA, which relies on classification techniques that employ a variety of input features extracted from touch dynamics. However, there is a lack of understanding of the importance of various features for the performance of MUA. In view of a large number of input features that have been explored, a categorization schema is also much needed. More importantly, the difference between different types of touch dynamics based MUA is understudied, particularly over multiple attempts.

Studies	LR	NB	KNN	DT	NN	RF	SVM
(Zhou et al. 2016)		✓ (41%)	✓ (70%)	✓ (65%)	✓ (76%)	✓ (75%)	✓ (70%)
(Zhang and Tao 2019)			✓ (95%)			✓ (99%)	✓ (97%)
(Balducci et al. 2019)		✓ (47%)		✓ (65%)	✓ (56%)	✓ (76%)	✓ (43%)
(Zhang et al. 2019)		✓ (95%)		✓ (97%)		✓ (97%)	✓ (97%)
(Tse and Hung 2019)	✓ (91%)	✓ (89%)	✓ (87%)		✓ (90%)		✓ (90%)
Our Study	✓	✓	✓	✓		✓	✓

Table 1. Classification Techniques and their Performance in Touch Dynamics based MUA

Method Design

To address the research limitations, we experimented with two types of touch dynamics based MUA methods and compared them via a user experiment. In this section, we introduce two different MUA methods and feature selection and describe participants, study procedure, and evaluation measures.

Apparatus

We used two different MUA methods, including a keystroke based and a touch gesture based MUA methods. We developed a keystroke based MUA method based on QWERTY, a conventional virtual keyboard, and a touch gesture based MUA method based on Thumbstroke (Lai et al. 2019), which exploits thumb strokes in entering text on a touch-screen mobile device. To support the experiment, we developed a QWERTY prototype and a Thumbstroke prototype (see Figure 1), and a user interface application for password entry using Android APIs. The QWERTY keyboard could align to the right or left, depending on the user's preference, and the Thumbstroke keyboard was initially placed in the middle of the screen by default and the participants were able to move it to anyplace they preferred on the screen. To ensure consistency in the use of the mobile device, we asked all the participants to use an experimental device, Samsung Galaxy S6 with a 5.1 in. screen and 1440x2560 pixels resolution. All the interactions, such as time and locations, were automatically recorded.

(a) Keytroke **(b) Touch Gesture**

Figure 1. Screenshots of the Touch Dynamics based MUA

Feature Selection

Based on our review of related MUA studies, we selected a wide range of touch gesture based features (Frank et al. 2013; Gong et al. 2016; Zhou et al. 2016). We further grouped the features into four categories: spatial, temporal, movement direction, and operation features. A summary of the selected features and their categorization is shown in Table 2.

Spatial Features	**Descriptions**
start x	The starting point of x coordinate on the touchscreen
stop x	The ending point of x coordinate on the touchscreen
start y	The starting point of y coordinate on the touchscreen
stop y	The ending point of y coordinate on the touchscreen
length of trajectory	The length of the trajectory of a stroke
direct end-to-end distance	The direct distance between its endpoints
ratio end-to-end dist and length of trajectory	The ratio between the length of the trajectory of a stroke and the direct distance between its endpoints
Temporal Features	
stroke duration	The duration of a stroke
median velocity at last 3 pts	The median velocity recorded in the last 3 points
median acceleration at first 5 points	The median acceleration recorded in the first 5 points
average velocity	The average velocity of a stroke
20%-perc. pairwise acc	The 20% percentile of acceleration of two consecutive points
50%-perc. pairwise acc	The 50% percentile of acceleration of two consecutive points
80%-perc. pairwise acc	The 80% percentile of acceleration of two consecutive points
20% perc pairwise velocity	The 20% percentile of the velocity of two consecutive points
50%-perc. pairwise velocity	The 50% percentile of the velocity of two consecutive points
80% perc pairwise velocity	The 80% percentile of the velocity of two consecutive points
20%-perc. dev. from end-to-end line	The 20% percentile of deviation between its endpoints
50%-perc. dev. from end-to-end line	The 50% percentile of deviation between its endpoints
80%-perc. dev. from end-to-end line	The 80% percentile of deviation between its endpoints
Movement Direction Features	
average direction	The average direction of all segments of the trajectory
direction of end-to-end line	The direction between its endpoints
largest deviation from end-to-end line	The largest deviation of its endpoints
Operation Features	
letter	The letter entered
input area: x axis	The input area covered by the x-axis
input area: y axis	The input area covered by the y-axis

Table 2. The Selected Features of Touch Gesture based MUA

Participants and Procedure

The participants were recruited from a university campus in the Eastern U.S. To make the participant pool more representative of the diverse users of mobile devices, we leveraged a public event to reach out to local communities. All qualified participants were required to have prior experience with using touch-screen mobile devices and to be 7 years old and above. A total of 14 participants successfully completed the study. Among them, 4 were between 7 and 18 years old and 10 were above 18 years old.

Each of the participants received a reward upon the completion of the study. The study was approved by the Institutional Review Board of the authors' home institute in advance.

The procedure of the study is as follows. After reading and signing the consent form (or forms when the participants were under 18 years old), the participants were asked to go through a training session. During the training session, a researcher first introduced the two MUA prototypes to the participant and then asked the participant to practice with both methods using the prototypes with the provided sample phrases covering all the 26 letters. Upon completion of the training, the participant was asked to play the role of an imposter to enter the authentication information of another participant 5 times with each of the MUA prototypes separately. The order of the MUA method assignment was randomized to avoid sequence effect. The authentication information was collected in advance through a longitudinal study where each participant was asked to create a password that was 8-letter long and entered the password 3 times each time over multiple sessions. Finally, we removed the first two attempts of the role players' data to enhance the ecological validity of the study findings. This is because a real-world imposter is expected to have some level of familiarity with the target victim's authentication information.

Variables and Evaluation Metrics

We measured the performances of the touch dynamics based methods from two perspectives: password entry performance and authentication performance (i.e., discriminating an imposter from an authentic user). The performance of password entry was measured by three variables: password duration, letter duration, and accuracy. To gain insights into the duration of password entry, we measured it at both of the password and letter levels.

- The password duration was measured as the time elapsed between the time when a participant started to enter the authentication information (i.e., password) to the time when he/she completed the entry.
- The letter duration was measured as the time elapsed between when a finger started to touch the screen and when the finger was lifted off from the screen. We did not take the time intervals between different letter entries into consideration in measuring duration at the letter level.
- We measured accuracy as the percentage of correct letter entries to the total number of letters used in password entry. This is because a successful password entry might involve a variety of operations, such as pressing, stroking, deletion, and substitution (Ouyang et al. 2017).

Prior studies demonstrated satisfactory performance of touch dynamics MUA using the traditional classification models (e.g., Balducci et al. 2019, Zhou et al. 2016). Thus, we adopted a similar set of classifiers, including LR, NB, KNN, DT, RF, and SVM. We selected the most commonly used metrics for measuring the authentication performance, including accuracy, true positive rate (TPR), and true negative rate (TNR).

- Accuracy is defined as the percentage of correct authentication decisions made to accept or deny user access.
- True positive rate is defined as the percentage of correct authentication decisions that allow access by an authentic user.
- True negative rate is defined as the percentage of correct authentication decision that denies access by a role player.

We split the data into training and testing sets. To shed light on the effect of training sample size on the MUA performance, we varied the training sample size from 1 to 21 for both the role players and the authentic user, separately. The training samples were randomly drawn from the collected data for each setting. We repeated each sample size setting multiple times and reported the average performance.

Results

We report the password entry performances and MUA classification performance separately.

Password Entry Performance

The descriptive statistics of password entry performances of keystroke based and touch gesture based methods are reported in Table 3. The analysis results of one-way ANOVA between the authentic user and the role players for each of the three attempts are reported in Table 4. The results show that the password duration of the keystroke based MUA is shorter for the authentic user than that of role players for the first attempt ($p<.01$). Surprisingly, there is no difference in letter duration between the authentic user and the role players except for the third attempt when the role players perform significantly faster than the authentic user ($p<.01$). This is particularly concerning because the role players were able to quickly become familiarized with the target's authentication information and even outperformed the targets given some practice. The analysis did not yield any difference in accuracy between the authentic user and the role players across any of the three attempts ($p>.05$). This finding is counterintuitive and suggests that the keystroke based MUA method may subject to simulation attacks.

For the touch gesture based MUA, the analyses of password duration and letter duration both yield significant differences between the two types of users across all the three attempts ($p<.001$). Specifically, the duration of the authentic user is shorter than those of the role players. The results provide supporting evidence for developing touch gesture based MUA methods. Nevertheless, there is no significant difference in the accuracy of password entries except for the first attempt ($p< 0.05$). We performed repeated analyses of the participants' performance over the three attempts, which did not yield any significant difference. The result suggests that it requires extensive practice for users to perform touch dynamics based MUA effectively.

Touch Dynamics MUA Methods		**Keystroke based MUA**			**Touch Gesture based MUA**		
Attempt		**1**	**2**	**3**	**1**	**2**	**3**
Password Duration	**Authentic User**	3425.43 (905.44)	4147.36 (2156.37)	3782.29 (1229.24)	8365.14 (2934.59)	8209.14 (2425.44)	9244.43 (3515.90)
	Role Players	6185.93 (3062.07)	4599.57 (885.10)	4649.14 (1987.51)	26123.64 (9942.98)	19891.29 (8267.16)	20417.50 (7252.05)
Letter Duration	**Authentic User**	120.63 (22.62)	122.84 (14.65)	127.22 (17.56)	371.56 (22.14)	387.74 (32.10)	394.36 (34.83)
	Role Players	110.81 (21.26)	127.67 (73.50)	105.12 (22.65)	618.44 (235.03)	605.58 (186.65)	583.91 (182.24)
Accuracy	**Authentic User**	1.00 (0.00)	0.98 (0.09)	0.99 (0.05)	0.85 (0.16)	0.89 (0.17)	0.85 (0.22)
	Role Players	0.92 (0.19)	0.91 (0.15)	0.91 (0.20)	0.67 (0.24)	0.77 (0.21)	0.73 (0.21)

Note: *Durations are reported in milliseconds; accuracies are reported in percentile; standard deviations in parentheses.*

Table 3. Descriptive Statistics of Password Entry Performance

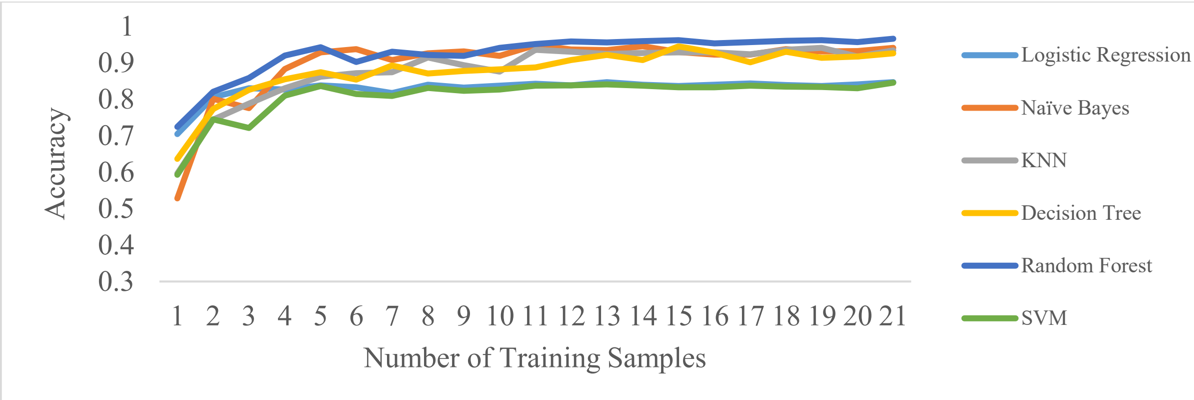
Touch Dynamics MUA Methods	**Keystroke based MUA**			**Touch Gesture based MUA**		
Attempt	**1**	**2**	**3**	**1**	**2**	**3**
Password Duration	0.003**	0.474	0.177	0.000***	0.000***	0.000***
Letter Duration	0.248	0.811	0.008**	0.001***	0.000***	0.001***
Accuracy	0.108	0.149	0.199	0.026*	0.116	0.154

$^{***}p< 0.001$; $^{**}p< 0.01$; $^{*}p< 0.05$

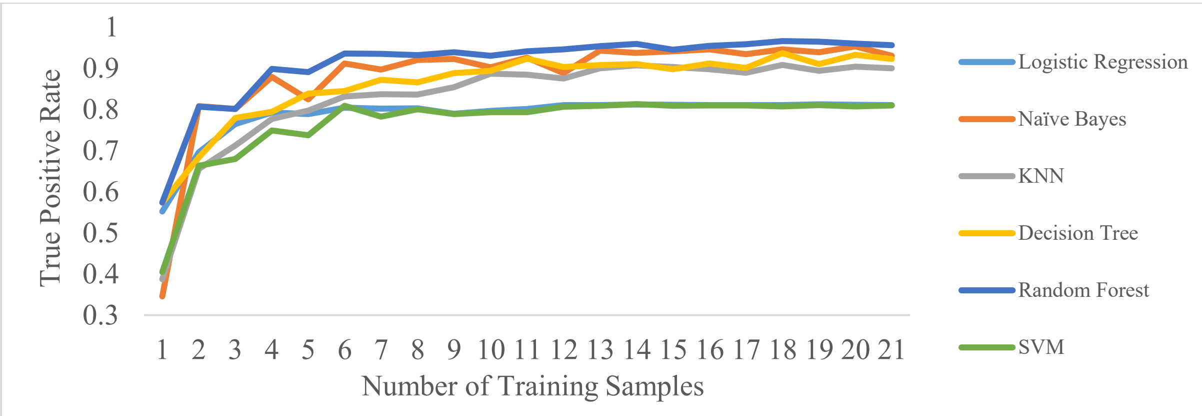
Table 4. Comparison Results between the Authentic User and the Role Players

MUA Classification Performance

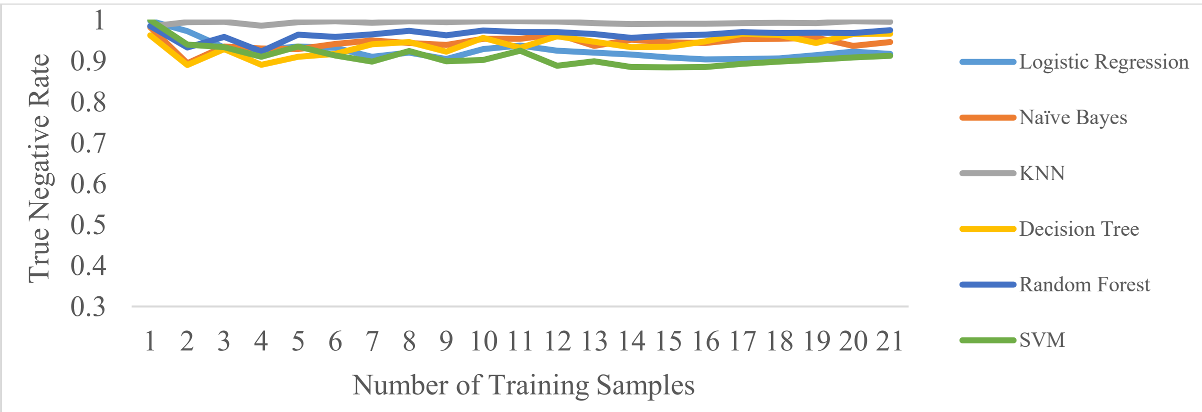
We report the MUA performance of the touch gesture based MUA methods with varying sizes of training samples in Figure 2. The results show that there are generally increasing trends of accuracy and TPR as the sample size increases. The trend starts to level off as the sample size is increased to 4, which achieved an accuracy ranging from 81% by SVM to 97% by RF. Besides, the RF model achieved a TPR of 97% at a TNR of 98% in MUA. The results are consistent with the findings of other studies that RF outperformed other traditional classification methods in MUA (Balducci et al. 2019; Zhang et al. 2019; Zhang and Tao 2019; Zhou et al. 2016).



(a) Accuracy



(b) True Positive Rate

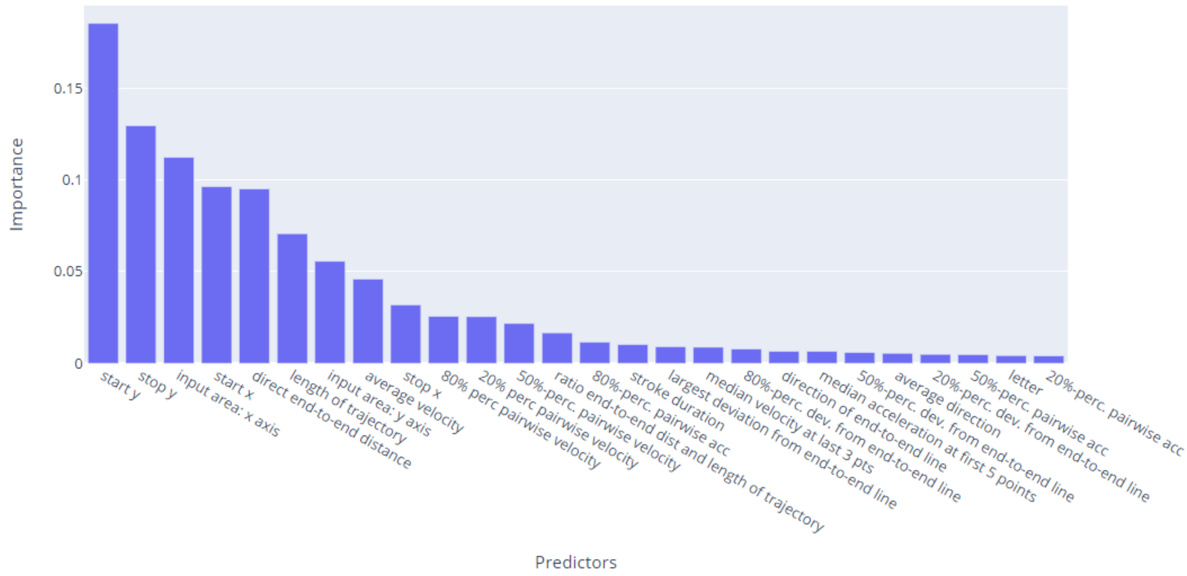


(c) True Negative Rate

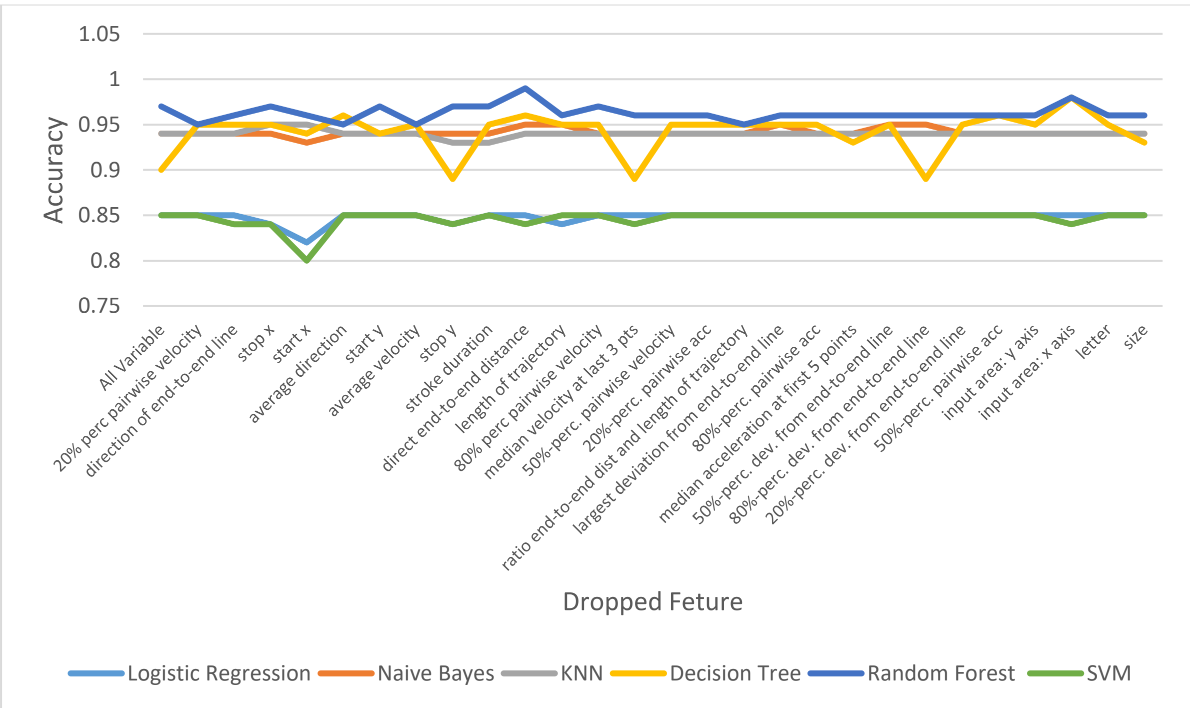
Figure 2. MUA Performance of the Selected Classification Models

Feature Importance

Given the lack of feature importance analysis aforementioned and the superior performance of the RF models in touch gesture based MUA, we used the RF models to analyze the importance of features for MUA. We sort the features in descending order of their importance and report them in Figure 3a. The sensitivity analysis (see Figure 3b) of various touch gesture based features further confirm the findings derived from the feature importance analysis that spatial features (e.g., start y, stop y, direct end-to-end distance) are most important for MUA. Operation features, such as input areas, also seem to be essential for the MUA performance. However, the temporal features (e.g., velocity and acceleration) and movement direction features are not so important as the first two types of features.



(a) Feature Importance Analyses



(b) Feature Sensitivity Analysis

Figure 3. The Importance of Input Features to MUA Performance

Discussion

To answer the first research question, we compared the two types of touch dynamics based MUA methods in terms of their password entry performance. The findings on password entry performance reveal a difference between the two types of MUA methods. Despite that no difference was detected between the authentic and role-player users for the keystroke based MUA method, there were significant differences between the two types of users for the touch gesture based method. The finding has important implications for MUA in that the role players had an equally good performance to the authentic users in keystroke based MUA, and the touch gesture based MUA appears to be more resistant to simulation attacks than the keystroke based method and is easy to learn.

To answer the second research question, we varied the training sample size for developing MUA models. For the touch gesture based MUA, a training sample size of four was found to approximate the optimal performance. This finding is encouraging because the small number of training samples provides evidence for the usability of the method, particularly in view of the limited computing and storage resources on mobile devices.

To answer the third research question, we performed both feature importance analysis and sensitivity analysis. The findings reveal that the spatial features such as starting and ending points of the touch gesture have the strongest effects on the performance of MUA. In view that the values of these features partly depend on users' finger length, MUA methods that combine touch dynamics and biometrics can be particularly promising. In contrast, the temporal and movement direction features were found to have little effect on MUA performance. It might be premature to draw a conclusion that such features are not useful. One possible explanation is that the sample size of the participants is relatively small and can not represent the performance of the overall population.

This study makes three-fold contributions to MUA research. First, through the comparison of two types of touch dynamics based MUA methods over multiple attempts, it provides the first empirical evidence for the superior and robust performance of the touch gesture based MUA methods. In addition, it examines user performance at two different stages of MUA: password entry and user authentication. Both sets of results suggest that touch gesture is a more promising alternative to keystroke based MUA method, despite that the former method requires more practice to achieve significant improvement in password entry performance. Second, the findings of this study reveal that training sample size matters to the touch gesture based MUA method, and more importantly, the method requires only a small training sample size to achieve near-optimal performance. Third, this study suggests important features for building touch gesture based MUA models. Among others, the spatial features are the most important, and the temporal and movement direction features the least. Our findings offer a guide for the design of touch dynamics based MUA methods and authentication template generation.

The research findings should be interpreted with the following limitations. It is common to use a small sample size in a lab experiment (Alsuhibany et al. 2019; Vertanen and Kristensson 2014). The model performance should benefit from a larger sample size with a diversified population. To extend our research scope, our study may consider other emerging touch dynamics based MUA methods. This study does not take user preferences for touch gestures into consideration. Future work may look into the moderating effect of password complexity and user preferences with a larger number of participants.

Conclusion

The touch gesture based MUA appears to be a more promising alternative to the keystroke based MUA. Despite that the authentication performance of touch gesture based MUA is sensitive to the training sample size, the method can achieve a near-optimal performance with a sample size of 4. The importance of input features for building touch gesture based MUA models varies greatly with spatial features being the most effective. The findings of the study can inform the design of secure and usable touch dynamics based MUA methods.

Acknowledgments

This work is supported in part by two grant awards from the National Science Foundation (Award #s: CNS 1704800 and SES 1912898). Any opinions, findings, or recommendations expressed here are those of the authors and are not necessarily those of the sponsor of this research.

References

Abuhamad, M., Abusnaina, A., Nyang, D., and Mohaisen, D. 2020. "Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Survey," *ArXiv:2001.08578 [Cs]*. (http://arxiv.org/abs/2001.08578).

Alsuhibany, S. A., Almushyti, M., Alghasham, N., and Alkhudhayr, F. 2019. "The Impact of Using Different Keyboards on Free-Text Keystroke Dynamics Authentication for Arabic Language," *Information & Computer Security* (27:2), pp. 221–232. (https://doi.org/10.1108/ICS-09-2017-0062).

Aviv, A. J., Sapp, B., Blaze, M., and Smith, J. M. 2012. "Practicality of Accelerometer Side Channels on Smartphones," in *Proceedings of the 28th Annual Computer Security Applications Conference*, ACSAC '12, Orlando, Florida, USA: Association for Computing Machinery, December 3, pp. 41–50. (https://doi.org/10.1145/2420950.2420957).

Balducci, F., Carolis, B. D., Impedovo, D., and Pirlo, G. 2019. *Touch Dynamics for Affective States Recognition: Your Smartphone Knows How You Feel since You Unlock It*, p. 5.

Bryan, W. L., and Harter, N. 1897. "Studies in the Physiology and Psychology of the Telegraphic Language," *Psychological Review* (4:1), pp. 27–53. (https://doi.org/10.1037/h0073806).

Burr, W., Dodson, D., Newton, E., Perlner, R., Polk, W., Gupta, S., and Nabbus, E. 2013. "Electronic Authentication Guideline," No. NIST Special Publication (SP) 800-63-2 (Withdrawn), National Institute of Standards and Technology, August 29. (https://doi.org/10.6028/NIST.SP.800-63-2).

Cai, L., and Chen, H. 2012. "On the Practicality of Motion Based Keystroke Inference Attack," in *Trust and Trustworthy Computing*, Lecture Notes in Computer Science, S. Katzenbeisser, E. Weippl, L. J. Camp, M. Volkamer, M. Reiter, and X. Zhang (eds.), Berlin, Heidelberg: Springer, pp. 273–290. (https://doi.org/10.1007/978-3-642-30921-2_16).

Crawford, H. 2010. "Keystroke Dynamics: Characteristics and Opportunities," in *2010 Eighth International Conference on Privacy, Security and Trust*, , August, pp. 205–212. (https://doi.org/10.1109/PST.2010.5593258).

Dee, T., Richardson, I., and Tyagi, A. 2019. "Continuous Transparent Mobile Device Touchscreen Soft Keyboard Biometric Authentication," in *2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID)*, , January, pp. 539–540. (https://doi.org/10.1109/VLSID.2019.00125).

Ferrag, M. A., Maglaras, L., Derhab, A., and Janicke, H. 2019. "Authentication Schemes for Smart Mobile Devices: Threat Models, Countermeasures, and Open Research Issues," *ArXiv:1803.10281 [Cs]*. (http://arxiv.org/abs/1803.10281).

Foody, G. M., and Mathur, A. 2004. "Toward Intelligent Training of Supervised Image Classifications: Directing Training Data Acquisition for SVM Classification," *Remote Sensing of Environment* (93:1), pp. 107–117. (https://doi.org/10.1016/j.rse.2004.06.017).

Frank, M., Biedert, R., Ma, E., Martinovic, I., and Song, D. 2013. “Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication,” *IEEE Transactions on Information Forensics and Security* (8:1), pp. 136–148. (https://doi.org/10.1109/TIFS.2012.2225048).

Giuffrida, C., Majdanik, K., Conti, M., and Bos, H. 2014. “I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics,” in *Detection of Intrusions and Malware, and Vulnerability Assessment*, Lecture Notes in Computer Science, S. Dietrich (ed.), Cham: Springer International Publishing, pp. 92–111. (https://doi.org/10.1007/978-3-319-08509-8_6).

Gong, N. Z., Payer, M., Moazzezi, R., and Frank, M. 2016. “Forgery-Resistant Touch-Based Authentication on Mobile Devices,” in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS ’16, Xi'an, China: Association for Computing Machinery, May 30, pp. 499–510. (https://doi.org/10.1145/2897845.2897908).

Gubernatorov, A. M., Teslenko, I. B., Muravyova, N. V., Vinogradov, D. V., and Subbotina, N. O. 2020. “Information Security of Mobile Systems,” in *Growth Poles of the Global Economy: Emergence, Changes and Future Perspectives*, Lecture Notes in Networks and Systems, E. G. Popkova (ed.), Cham: Springer International Publishing, pp. 677–686. (https://doi.org/10.1007/978-3-030-15160-7_68).

Khan, J., Abbas, H., and Al-Muhtadi, J. 2015. “Survey on Mobile User’s Data Privacy Threats and Defense Mechanisms,” *Procedia Computer Science* (56), The 10th International Conference on Future Networks and Communications (FNC 2015) / The 12th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2015) Affiliated Workshops, pp. 376–383. (https://doi.org/10.1016/j.procs.2015.07.223).

Kolly, S. M., Wattenhofer, R., and Welten, S. 2012. “A Personal Touch: Recognizing Users Based on Touch Screen Behavior,” in *Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones*, PhoneSense ’12, Toronto, Ontario, Canada: Association for Computing Machinery, November 6, pp. 1–5. (https://doi.org/10.1145/2389148.2389149).

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., and Egelman, S. 2011. “Of Passwords and People: Measuring the Effect of Password-Composition Policies,” in *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems - CHI ’11*, Vancouver, BC, Canada: ACM Press, p. 2595. (https://doi.org/10.1145/1978942.1979321).

Kunda, D., and Chishimba, M. 2018. “A Survey of Android Mobile Phone Authentication Schemes,” *Mobile Networks and Applications*. (https://doi.org/10.1007/s11036-018-1099-7).

Lai, J., Zhang, D., Wang, S., Kilic, I. D. Y., and Zhou, L. 2019. “ThumbStroke: A Virtual Keyboard in Support of Sight-Free and One-Handed Text Entry on Touchscreen Mobile Devices,” *ACM Transactions on Management Information Systems* (10:3), 11:1–11:19. (https://doi.org/10.1145/3343858).

Lin, Z., Meng, W., Li, W., and Wong, D. S. 2020. “Developing Cloud-Based Intelligent Touch Behavioral Authentication on Mobile Phones,” in *Deep Biometrics*, Unsupervised and Semi-Supervised Learning, R. Jiang, C.-T. Li, D. Crookes, W. Meng, and C. Rosenberger (eds.), Cham: Springer International Publishing, pp. 141–159. (https://doi.org/10.1007/978-3-030-32583-1_7).

Ma, J., Yang, W., Luo, M., and Li, N. 2014. “A Study of Probabilistic Password Models,” in *2014 IEEE Symposium on Security and Privacy*, San Jose, CA: IEEE, May, pp. 689–704. (https://doi.org/10.1109/SP.2014.50).

Meng, Y., Wong, D. S., and Kwok, L.-F. 2014. "Design of Touch Dynamics Based User Authentication with an Adaptive Mechanism on Mobile Phones," in *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, SAC '14, Gyeongju, Republic of Korea: Association for Computing Machinery, March 24, pp. 1680–1687. (https://doi.org/10.1145/2554850.2554931).

Obaidat, M. S., and Sadoun, B. 1996. "Keystroke Dynamics Based Authentication," in *Biometrics: Personal Identification in Networked Society*, A. K. Jain, R. Bolle, and S. Pankanti (eds.), Boston, MA: Springer US, pp. 213–229. (https://doi.org/10.1007/0-306-47044-6_10).

Ouyang, T., Rybach, D., Beaufays, F., and Riley, M. 2017. "Mobile Keyboard Input Decoding with Finite-State Transducers," *ArXiv:1704.03987 [Cs]*. (http://arxiv.org/abs/1704.03987).

Polyzotis, N., Roy, S., Whang, S. E., and Zinkevich, M. 2017. "Data Management Challenges in Production Machine Learning," in *Proceedings of the 2017 ACM International Conference on Management of Data*, SIGMOD '17, Chicago, Illinois, USA: Association for Computing Machinery, May 9, pp. 1723–1726. (https://doi.org/10.1145/3035918.3054782).

Rashid, A., and Chaturvedi, A. 2019. "Cloud Computing Characteristics and Services A Brief Review," *International Journal of Computer Sciences and Engineering* (7:2), pp. 421–426. (https://doi.org/10.26438/ijcse/v7i2.421426).

Raul, N., Shankarmani, R., and Joshi, P. 2020. "A Comprehensive Review of Keystroke Dynamics-Based Authentication Mechanism," in *International Conference on Innovative Computing and Communications*, Advances in Intelligent Systems and Computing, A. Khanna, D. Gupta, S. Bhattacharyya, V. Snasel, J. Platos, and A. E. Hassanien (eds.), Singapore: Springer, pp. 149–162. (https://doi.org/10.1007/978-981-15-0324-5_13).

Shekhawat, K., and Bhatt, D. P. 2019. "Recent Advances and Applications of Keystroke Dynamics," in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, , December, pp. 680–683. (https://doi.org/10.1109/ICCIKE47802.2019.9004312).

Teh, P. S., Zhang, N., Tan, S.-Y., Shi, Q., Khoh, W. H., and Nawaz, R. 2019. "Strengthen User Authentication on Mobile Devices by Using User's Touch Dynamics Pattern," *Journal of Ambient Intelligence and Humanized Computing*. (https://doi.org/10.1007/s12652-019-01654-y).

Teh, P. S., Zhang, N., Teoh, A. B. J., and Chen, K. 2016. "A Survey on Touch Dynamics Authentication in Mobile Devices," *Computers & Security* (59), pp. 210–235. (https://doi.org/10.1016/j.cose.2016.03.003).

Tse, K.-W., and Hung, K. 2019. "Behavioral Biometrics Scheme with Keystroke and Swipe Dynamics for User Authentication on Mobile Platform," in *2019 IEEE 9th Symposium on Computer Applications Industrial Electronics (ISCAIE)*, , April, pp. 125–130. (https://doi.org/10.1109/ISCAIE.2019.8743995).

Venugopal, P. C. 2020. "APPLYING EMPIRICAL THRESHOLDING ALGORITHM FOR A KEYSTROKE DYNAMICS BASED AUTHENTICATION SYSTEM," *Journal of Information and Communication Technology* (18:4), pp. 383–413.

Vertanen, K., and Kristensson, P. O. 2014. "Complementing Text Entry Evaluations with a Composition Task," *ACM Transactions on Computer-Human Interaction (TOCHI)* (21:2), 8:1–8:33. (https://doi.org/10.1145/2555691).

Wang, K., Zhou, L., and Zhang, D. 2019. *User Preferences and Situational Needs of Mobile User Authentication Methods*, 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 18–23. (https://doi.org/10.1109/ISI.2019.8823274).

Yong Sheng, Phoha, V. V., and Rovnyak, S. M. 2005. "A Parallel Decision Tree-Based Method for User Authentication Based on Keystroke Patterns," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)* (35:4), pp. 826–833. (https://doi.org/10.1109/TSMCB.2005.846648).

Zhang, D., Zhou, L., and Pisupati, S. 2019. "Tracing One's Touches: Continuous Mobile User Authentication Based on Touch Dynamics," *AMCIS 2019 Proceedings*. (https://aisel.aisnet.org/amcis2019/human_computer_interact/human_computer_interact/3).

Zhang, J., and Tao, D. 2019. "Implicit Identity Authentication Mechanism Based on Smartphone Touch Dynamics," in *2019 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, , May, pp. 1–2. (https://doi.org/10.1109/ICCE-TW46550.2019.8992015).

Zhao, X., Feng, T., Shi, W., and Kakadiaris, I. A. 2014. "Mobile User Authentication Using Statistical Touch Dynamics Images," *IEEE Transactions on Information Forensics and Security* (9:11), pp. 1780–1789. (https://doi.org/10.1109/TIFS.2014.2350916).

Zheng, N., Bai, K., Huang, H., and Wang, H. 2014. "You Are How You Touch: User Verification on Smartphones via Tapping Behaviors," in *2014 IEEE 22nd International Conference on Network Protocols*, , October, pp. 221–232. (https://doi.org/10.1109/ICNP.2014.43).

Zhou, L., Kang, Y., Zhang, D., and Lai, J. 2016. "Harmonized Authentication Based on ThumbStroke Dynamics on Touch Screen Mobile Phones," *Decision Support Systems* (92), pp. 14–24. (https://doi.org/10.1016/j.dss.2016.09.007).