The Effectiveness of Dynamic Features of Finger Based Gestures on Smartphones' Touchscreens for User Identification

Suleyman A. Al-Showarah
Mutah University, Mutah - Karak, Jordan
Showarah@mutah.edu.jo

Abstract—This paper presents methodology for user identification on smartphone and mini-tablet using finger based gestures. In this paper, a set of four features, namely Signature Precision (SP), Finger Pressure (FP), Movement Time (MT), and Speed were extracted from each gesture of eight using dynamic time warping and Euclidean distance. The features are then used individually and combined for the purpose of user identification based on the Euclidean distance and the k-nearest neighbour classifier. We concluded that the best identification accuracy results from the combinations of FP and MT features where 78.46% and 78.33% were achieved on small smartphone and Mini-tablet respectively using a dataset of 50 users.

1 Introduction

The popularity of smartphones devices make them a frequent storage medium for the users sensitive information such as personal photos, email, credit card numbers, and banking passwords. As smartphone devices are easily lost or stolen, the problem of securing the user access to this data considers one of paramount importance [1].

Unlock screens using text based password, graphical based password, or grid based schemes are most current access systems prompt users to authenticate themselves. This authentication method relies on the password's/username's secrecy. If this secrecy is not breached, the assertion is that these tokens uniquely identify a valid user. The problems of user authentication associated with maintaining password secrecy are well understood. Passwords that consist of common words, or terms associated with a particular user are generally considered weak because of the relative ease with which a malicious users can guess them [2].

The need for strong authentication is influenced by the input methodology of touchscreen devices and the different expectations of user for interaction models [1]. As shown in a study [3] over 3.3 million leaked passwords, number of their list was

still "123456". Moreover, the additional cost makes biometric authentication techniques to be still unpopular on mobile devices [1].

The main motivation of finger based gestures on smartphone and tablet for user identification is preventing a malicious users from breaching the unlock screen of smartphone devices. As mentioned early, users prefer using text based password, graphical based password, and grid based schemes because of it is easy to remember. The need to enhance the authentication users on smartphones is required in order to make the illegal user access on smartphones impossible; because of this required we examined finger based features on smartphone and tablet for user identification. Our study relay on the users attributes and behaviours on touchscreen, so breaching unlock screen will not be easy even if the password also was stolen. In our study, the features were analysed individually features, combined of two features, and combined of three features to increase the accuracy.

In the results, we concluded that the best identification accuracy results were from the combinations of FP and MT features where 78.46% and 78.33% were achieved on small smartphone and Mini-tablet respectively using a dataset of 50 users. However, not all features help increasing identification power.

The contributions of this work can be highlighted as follows. First, we use widely available consumer devices in our experiments. Secondly, our experimental procedure was designed differently to previous studies; the required gesture remained displayed on the screen as a guide whilst the participant executes the gesture. Thirdly, the way on how we analysed data is different from previous studies, as Dynamic Time Warping algorithm was used to calculate distances between the optimal path of a gesture and the executed one considering all points along the trajectory of the gesture to produce a signature precision. As well as the three aspect of analysis for individually, combined of two features, combined of three features were considered in this study.

The rest of this paper is organized as follows. Section 2 discussed the related work on which we prepared our study. Section 3 explained the analysis of our experimental results. The data collection processes are described in Section 4. The experimental results are explained in Section 5. As well as the final conclusions are presented in section 6.

2 Related Work

The need for finger based gestures on smartphones for user identification is increasing day by day because text or graphical based passwords and grid based schemes are easy to recall and stolen from a malicious users. Finger based gestures on smartphones for user identification has greater potential to provide a more dynamic movement for users on screen for using some a specific features (e.g. SP, FP) than other used in text based passwords. Many researchers are working on the concept of user identification using finger based gesture; some of them also introduced new ideas to provide more secure approach related to text or signature passwords. One of the studies that examined finger based gesture for user identification was conducted by [1]. The researchers Tao Feng and Nguyen in [1] use touch data collected from 40 users based on sensor gloves in order to collect information of finger movement for

six types of gestures: down to up swipe, up to down swipe, left to right swipe, right to left swipe, zooming, and zoom-out. The two features used in the study are: the length of touch input sequences and the authentication threshold (i.e., number of accepted touch inputs during one sequence). Their results showed that 4.66% a false accept rate and 0.13% a false reject rate.

Early researches, the examining focused on the possibility of applying keystroke dynamics and typing patterns for user identification. Keystrokes were used as samples by intercepting output from a keyboard [1]. But Mäntyjärvi, et al. in [4] examined identifying people by their gait using accelerometers worn. Also, the researchers in [5] and [6] examined user identification using gait recognition. The researchers Koreman, et al. in [7] proposed a multi-modal biometric for user identification.

Some of the researchers' efforts were put on a graphical authentication approaches that use the doodles for user authentication. The researchers Jermyn, et al. in [8] proposed and evaluated graphical password schemes that exploit features of graphical input displays to achieve better security than text based passwords. Furthermore, doodles method was proposed by [9] rather than signatures. Several methods were investigated to confirm the identity of the doodle; distribution grid, speed, point variance across the distribution grid, and a combination of all the above. The analysis showed that the combined three features of the system yields extremely accurate results. There have been a number of studies on combining multiple biometric inputs to produce user identification results. The researchers Indovina, et al. in [10]examined a biometric integration of fingerprint and face biometrics on a population of 1000 users. The biometric integration can occur on the feature level, or the score level. In feature level integration, all of the initial features are grouped together into a one feature vector. Their work showed that multimodal fingerprint and face biometric systems achieved significant accuracy gains over any biometric alone.

Grid technique based schemes are also examined in the body of the literature which uses recall method. This technique allows a user draws the password on a 2D grid, and then the information of an occupied grid (e.g. coordinates) will be recorded. The user will be authenticated when drawing touches the grid in the same order. In order to enter the password correctly and distinguishable, the drawing must be sufficiently away from the grid lines and intersections [1] and [8].

A signature using a mouse approach for an authentication user was conducted [11]. The advantage of using a mouse to draw a signature is that the signatures are hard to fake. It can therefore be hard to drawn, as not everybody is familiar with using mouse as a writing device [12]. A graphical authentication scheme was also conducted in [13], in that a set of pictures are presented on the interface, where some of these pictures are taken from the user's portfolio, and some pictures are selected randomly. During registration, the user should select some number of pictures from a set of random pictures. For successful authentication, the pictures must be correctly selected amongst the distracters by the users.

There were number of studies conducted for user' identification using a stylus device. The researchers Orozco, et al. in [14] examined users' haptic characteristics for 4 users. The results showed that the probability of verification reached up to 78.8% with 25% false acceptance rate. The researchers (Alsulaiman, et al. in [15] examined

user identification for 16 users based on handwritten signatures and haptic information such as velocity and angular rotation gathered during the creation of the user's handwritten signature and the consistency in the user's behaviour. The users were identified at an average success rate of 81%.

Some the latest studies were conducted for authentication users to unlock interfaces on smartphones using gestures. The researchers Xu, et al. in [16] examined an authentication biometrics for 32 users on slide, pinch, handwriting, and finger based keystroke that involves a series of taps on the soft; on-screen keyboard. A classification algorithm of Support Vector Machine (SVM) was used in the analysis. The researchers considered the data of the position, pressure, and size of a touch, as well as a timestamp in order to calculate the accuracy and error rate as two straightforward metrics. They concluded in their study that touch operation can be a form of good biometrics. And they found that there is still room for the accuracy to reach up to 100%, and it is a promising solution to consider a join of a set of touch operations for making an authentication decision rather than using one at a time. This indicates a need for further research to make touch-based authentication a practical solution. Another study proposed gestures and algorithms (using Support Vector Distribution Estimation (SVDE)) as classifier to model multiple behaviours of a user in performing each gesture. The study used seven types of features: velocity magnitude, device acceleration, stroke time, inter-stroke time, stroke displacement magnitude, stroke displacement direction, and velocity direction. The feature values were extracted based on sub-strokes and strokes for some features. The total data collected is 15009 gesture samples from 50 users. Experimental results showed that their scheme achieves an average equal error rate of 0.5% with 3 gestures using only 25 training samples [17]. In what follows, we will discuss the processes on how the data was analysed considering the algorithms used in this study.

3 User Identification Processes

Following to the analysis conducted based on Dynamic Time Warping (DTW) in study ([18]: section 6.2), the same users (i.e. 50 users), and feature (i.e. SP, FP, MT, and Speed) were involved in this paper. As each user has six samples of performing eight different gestures on smartphones; where 26 users were involved in small smartphone, and 24 users were involved in mini-tablet.

After extracting data using DTW and ED in the study [18], then we arranged them into two parts: testing dataset and training dataset (Reference). On small smartphone the testing dataset consists of (130) samples, and the training dataset consists of (26) samples. On mini-tablet the testing dataset consists of (120) samples, and the training dataset consists of (24) samples.

Fig. 1 below shows set of numbered processes used in user identification study on each smartphone device, as follows: 1. Feature Extraction. After collecting data were entered into set of analysis processes to produce SP using DTW, Speed using ED, MT, and FP. This part one in the Fig. 1 was prepared in the study ([18]: Section 6.2). 2. Part two of Fig. 1 reviews user identification processes in three subsections. 2.1.

Training. One trial of six was used in the training dataset for each user across eight gestures; as each feature has eight different gestures, and this will be 32 if the four features were combined (SP, FP, MT, and Speed) and so on, as shown in Fig. 2 that shows feature factor of all trials we collected on smartphones for study's features in the training and testing datasets. The matrix D [8 x N] in the Fig. 1 represents training dataset for 1 feature, where 1 feature (8 gestures) and N users. 2.2. Testing. The remaining five trails of six for each user are in the matrix M [8 x Z] and considered to be testing section, where 1 feature (8 gestures) and Z is (number of users * 5 trials of each user). 2.3. User identification. Based on using the ED between the matrices M [8 x Z] and D [8 x N], and KNN used to compare the trail in M [8 x Z] to which exemplar in D [8 x N] is the user belong to. We will discuss the eight gestures that were collected from the 50 users in the next section.
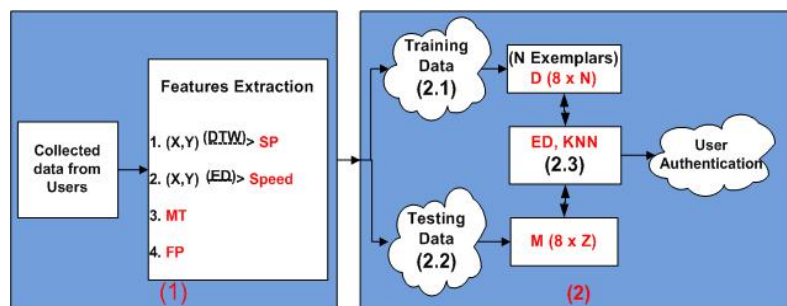

Fig. 1. Users identification process.

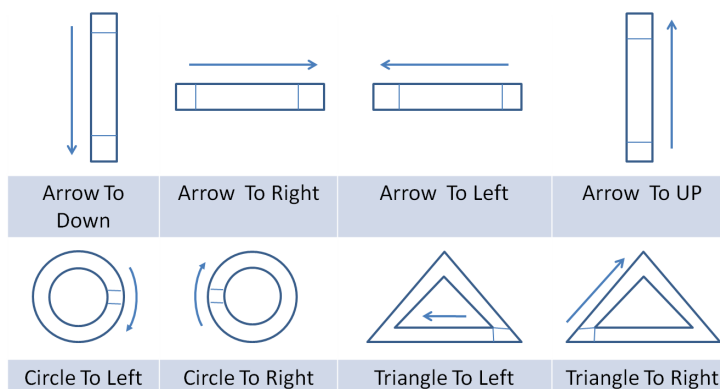**Fig. 2.** Feature factor for all trials (i.e. G: gesture and F: feature).

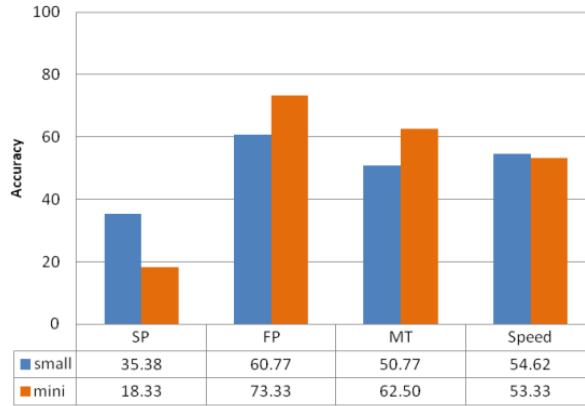**Fig. 3.** Eight Gesture Applications.

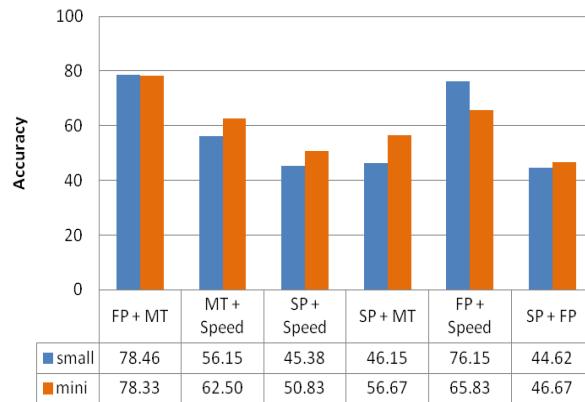|	SP	FP	MT	Speed
■ small	35.38	60.77	50.77	54.62
■ mini	18.33	73.33	62.50	53.33

Fig. 4. Features individually

	FP + MT	MT + Speed	SP + Speed	SP + MT	FP + Speed	SP + FP
■ small	78.46	56.15	45.38	46.15	76.15	44.62
■ mini	78.33	62.50	50.83	56.67	65.83	46.67

Fig. 5. Two features combination results.

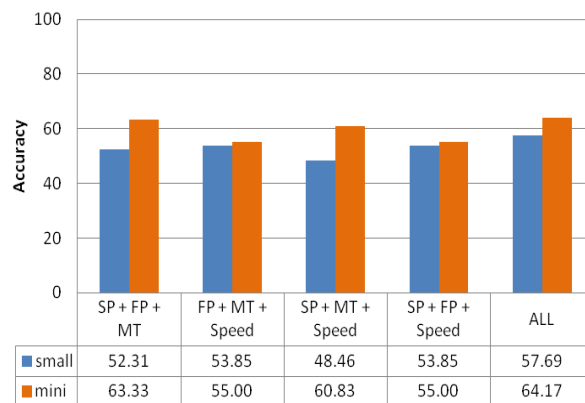|	SP + FP + MT	FP + MT + Speed	SP + MT + Speed	SP + FP + Speed	ALL
■ small	52.31	53.85	48.46	53.85	57.69
■ mini	63.33	55.00	60.83	55.00	64.17

Fig. 6. Three features combination and all features results.

4 Data Set And Experimental Protocol

The dataset consists of 50 participants where each participant was asked to repeat eight different gestures for six times producing a total of 48 trials per participant. Therefore, the total number of trials collected is2400, which increases to 9600 when implemented the combination of four features. The Gesture Applications used in the research were illustrated earlier in Section 4.8 of the study [18].

This research includes eight gestures (i.e., circle to right, circle to left, triangle to right, triangle to left, arrow down, arrow left, arrow right, and arrow up) as shown in Fig. 3 Each user was asked to trace gestures for each of the two circles and two triangles from the centre of the box (start point) through the middle of the path to the centre of the same box (start and the end points of the triangle and circle are represented by the same box). With regard to the remaining four gestures (i.e., arrow down, arrow left, arrow right, and arrow up), the start and the end points of the gestures were represented by two boxes. In all gestures, an arrow was used as a guide to indicate the direction of the gesture. Following the instruction of [19], the participants were asked to trace the complete gestures as quickly and accurately as possible. In what follows, the results of this study will be discussed considering the user identification accuracy and performance variations across different users.

5 Results And Discussions

In this study, accuracy of user identification on individually features, combined of two features, and combined of three features were considered, as follows:

5.1 Accuracy of User Identification on Individually Features

Our results were analysed individually, and in combined features. In individually features, Fig. 4 below shows FP on both smartphones has high accuracy result 60.77% and 73.33% on small smartphone and mini-tablet respectively compared to other individually features. This indicates that this feature (i.e. FP) could be used largely to provide stronger results accuracy. Then, the second high accuracy can be MT or speed. We will investigate which one of features (MT or speed) can provide high accuracy result in the next paragraph (combined of two features).

The results also show that SP has the least discrimination power, which can be mainly due to the small samples were used in the training dataset, as this feature depend on how accurately the user can perform the gesture. If partly, the gesture is not performed correctly, the SP will decrease the accuracy.

5.2 Accuracy of User Identification on Two Features Combination

In term of combined of two features i.e. feature-level fusion, Fig. 5 shows the results on both smartphones for two features combination: FP and MT have high accuracy result compared to other combined of two features, where on small smartphone

is 78.46% and on mini-tablet is 78.33%. This is for the high influence of features (e.g. FP) on results than any other influences (e.g. screen sizes). The second high accuracy result on two features combinations are FP and Speed. The results prove that the FP has increased the influence also on accuracy for the two features except FP and SP for the lower accuracy results, this is because The SP has influenced negatively on the accuracy as mentioned early in the individually features section regarding the SP influence.

This indicates that the combined features have high accuracy results compared to the individually features, and this provides evidence that the combination can enhance the accuracy results, this is agree with the study [18] in the field of the combination influence on the accuracy results.

5.3   Accuracy of User Identification on Three Features Combination

In term of combined of three features and all, Fig. 6 shows the accuracy results for all features have high accuracy result compared to other combined of three features, where on small smartphone is 57.69% and on mini-tablet is 64.17%.

Adding the feature Speed to (FP and MT) has not enhanced the identification accuracy results. In fact, it had negative impact due to the level of noise introduced as a result of adding the feature. However, we found the combined of two features have high accuracy result compared to the individually, the combined of three features and all features as well. Not all features help increasing the identification power.

To the best of our knowledge we have not came across a study conducted for biometric identification on smartphones using eight different gestures, the way on how we analysed the data using DTW and ED algorithms to calculate the accuracy and speed in order to prepare the features to the user identification processes, as well as the way on how we combined features to enhance the accuracy that were not considered in the previous studies.

6   Conclusion And Future Work

This paper presents methodology for user identification on smartphone and mini-tablet using finger based gestures, which improves user identification. The individually, combined of two features, and combined of three features were considered in this paper to verify the user. After extracting the gestures trails from users, the trials then compared with trusted user values using ED and KNN.

The results provide evidence that the combined features can enhance the accuracy results, where not all feature help increasing identification power and some of features has high accuracy result influence such as FP. Using minimal number of samples in the training dataset led to decreasing the identification accuracy when SP was fused with other features.

In the future work, we are planning to consider the combined features based on the percentage of power discrimination of users improve the user identification accuracy. Also, we are going to conduct the same study using image processing.

7   Acknowledgment

8   References

1. Feng, T., Liu, Z., Kwon, K. A., Shi, W., Carbunar, B., Jiang, Y., & Nguyen, N. (2012, November). Continuous mobile authentication using touchscreen gestures. In Homeland Security (HST), 2012 IEEE Conference on Technologies for (pp. 451-456). IEEE.
2. Peacock, Alen, Xian Ke, and Matthew Wilkerson. "Typing patterns: A key to user identification." IEEE Security & Privacy 2.5 (2004): 40-47. https://doi.org/10.1109/MSP.2004.89
3. Epstein, Z. "These are the worst passwords in the world – do you use any of them?," 2016. [Online] Available at: http://bgr.com/2016/01/19/worst-passwords-2016-list/ (accessed 3Sep 2016).
4. Mantyjarvi, Jani, et al. "Identifying users of portable devices from gait pattern with accelerometers." Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.. Vol. 2. IEEE, 2005.
5. Kale, Amit, et al. "Gait-based recognition of humans using continuous HMMs." Automatic Face and Gesture Recognition, 2002. Proceedings. Fifth IEEE International Conference on. IEEE, 2002. https://doi.org/10.1109/afgr.2002.1004176
6. Gafurov, Davrondzhon, Kirsi Helkala, and Torkjel Søndrol. "Biometric gait authentication using accelerometer sensor." Journal of computers 1.7 (2006): 51-59. https://doi.org/10.4304/jcp.1.7.51-59
7. J. Koreman, A. C. Morris, D. Wu, S. Jassim, H. Sellahewa, J. Ehlers, G. Chollet, G. Aversano, H. Bredin, S. G. salicetti, L. Allano, B. L. Van and B. Dorizzi, Multi-modal biometric authentication on the SecurePhone PDA, 2006.
8. Jermyn, I. Mayer, A. Monrose, F. Reiter M. K. and Rubin, A. "The Design and Analysis of Graphical Passwords," in 8th USENIX Security Symposium, 1999.
9. Varenhorst, Christopher, M. V. Kleek, and Larry Rudolph. "Passdoodles: A lightweight authentication method." Research Science Institute (2004).
10. Indovina, Michael, et al. "Multimodal biometric authentication methods: a COTS approach." Proc. MMUA (2003): 99-106.
11. Syukri, Agus Fanar, Eiji Okamoto, and Masahiro Mambo. "A user identification system using signature written with mouse." Australasian Conference on Information Security and Privacy. Springer Berlin Heidelberg, 1998. https://doi.org/10.1007/bfb0053751
12. Walanjkar, D. P. V. N. D. "User Authentication Using Graphical Password Scheme: A More Secure Approach using mobile interface," International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization), Vols. Vol. 2, Issue 12, December 2014.
13. Dhamija, Rachna, and Adrian Perrig. "Deja Vu-A User Study: Using Images for Authentication." USENIX Security Symposium. Vol. 9. 2000.
14. M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler and A. El Saddik, "Haptic-based biometrics: a feasibility study," in 2006 14th Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems, 2006.

15. Alsulaiman, Fawaz A., Jongeun Cha, and Abdulmotaleb El Saddik. "User identification based on handwritten signatures with haptic information." International Conference on Human Haptic Sensing and Touch Enabled Computer Applications. Springer Berlin Heidelberg, 2008. https://doi.org/10.1007/978-3-540-69057-3_12

16. Xu, Hui, Yangfan Zhou, and Michael R. Lyu. "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones." Symposium On Usable Privacy and Security (SOUPS 2014). 2014.

17. Shahzad, Muhammad, Alex X. Liu, and Arjmand Samuel. "Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it." Proceedings of the 19th annual international conference on Mobile computing & networking. ACM, 2013. https://doi.org/10.1145/2500423.2500434

18. Al-Showarah, Suleyman. Effects of age on smartphone and tablet usability, based on eye-movement tracking and touch-gesture interactions. Diss. University of Buckingham, 2015.

19. Teather, Robert J., Daniel Natapov, and Michael Jenkin. "Evaluating haptic feedback in virtual environments using ISO 9241–9." 2010 IEEE Virtual Reality Conference (VR). IEEE, 2010. https://doi.org/10.1109/vr.2010.5444753

9 Author

S. A. Al-Showarah is with the faculty of nformation Technology, Mutah University, Mutah- Karak, 61710 Mutah, Jordan (e-mail: Showarah@mutah.edu.jo). He is granted a PhD in Computing from the University of Buckingham, 2015, UK.