Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TOUCH GESTURE AUTHENTICATION FRAMEWORK FOR TOUCH SCREEN MOBILE DEVICES

[1] ALA ABDULHAKIM ALARIKI, [2] AZIZAH ABDUL MANAF

[1]PHD Student, Advanced Informatics School, University Technology Malaysia, Kuala Lumpur;
[2] Professor. Dr, Advanced Informatics School, University Technology Malaysia, Kuala Lumpur, Malaysia.
Email: [1]altop_2010@yahoo.com

ABSTRACT

With the increased popularity of touchscreen mobile phones, touch gesture behavior is becoming more and more important. Increasing demand for safer access in touch screen mobile phones, ancient strategies like pins, tokens, or passwords fail to stay up with the challenges conferred. Most of the current touch gesture authentication schemes facing problem with accuracy based on score classifiers of EER, FAR and FRR. In addition, collecting touch duration feature only may not be able to achieve the desired authentication accuracy and robustness. However, gathering more touch features such as finger pressure, finger size and acceleration would help to get a better authentication accuracy and verification performance. These efforts have allowed us to provide a comprehensive summary of recent work on touch behavior authentication and a frame work to implement the system. Finally, we conclude the future work in this topic which is implement and test the framework of touch gesture gesture-based behavioral biometrics and obtain more accuracy and robustness authentication system.

Keywords: *Behavioral Biometrics, Gesture authentication, Touch Behavioral, Touch Authentication.*

1. INTRODUCTION

Up to date, mobile devices such as smart phones, has been gaining popularity, which has led to reach set of instruments that allow us to store this sensitive or private information in our laptop and mobile devices. Market analysis predicts that in 2015 there will be 1.5 billion smartphones and 640 million tablets in use worldwide [1].McAfee's threat report discovered that ten million new mobile malwares were found in 2010. Such malware causes serious harm to users, like the discharge of non-public identification data. A requirement for improved authentication strategies exists in an exceedingly wide selection of sensible phones on demand [2].

However, organizations are too depending on digital technology to make, process, store, communicate, and use information in their activities[3]. With the increased popularity of touchscreen mobile phones, touch behavior is becoming more and more important, as many smartphones now feature touchscreens as the main input method [4]. One of the most important topics in information security today is user authentication. There is a good security when using the text-based strong password schemes but often memorizing the password is so difficult and users writing them down on a piece of paper [5]. In addition, most of the previous study [6],[7],[8],[9] and [10] have reported that biometric-based person recognition is a good alternative to classical systems and overcomes the difficulties of password and token approaches.

From the existing works, most of the researcher collected and tested their methods in small group of users. In addition, most of the schemes facing problem with accuracy based on score classifiers of EER, FAR and FRR. Furthermore, gathering more touch features such as finger pressure, finger size and acceleration would help to get a better authentication accuracy and verification performance.

Thus, the aims of this paper are to present current user authentication biometrics techniques and to review and classify features and methods for touch behavior authentication system. The organization of the article is as follow: Section 2 presented biometrics authentication. Section 3 touch gesture behavioral biometric. Section 4 presented related work on touch gesture behavioral authentication. Section 5 presented the conclusion and future work.

2. RELATED WORK

In this section, we report some of recent researches on touch gesture-based behavioral biometrics authentication.

In [11] looked at the different sensors provided by mobile phones, and show that data collected from these sensors can distinguish mobile users by analyzing the user's touch interaction with the device. Based on fifteen minutes of real-world device interaction from six test subjects, he was able to correctly identify the test subject that generated a 90 second sample 83% of the time using a subset of features extracted from the data. However, they evaluated the experiment with six participant only. Including more users and larger sample sizes is needed in order to make a more robust determination on the ability to identify users based on their behavior metric data.

In [4] proposed a unique user authentication theme supported touch dynamics that uses a group of behavioral options associated with touch dynamics for correct user authentication. The experimental results show that a neural network classifier is well-suited to evidence completely different users with a mean error rate of regarding 7.8% for our designated options. However, by victimization different classification methodology techniques, involving a lot of participants and assembling a lot of touch gesture knowledge would facilitate to induce a good higher accuracy and performance.

In [12] proposed a technique for distinguishing users supported touch dynamics. The study explored many measures for classifying users and extracting distinctive user characteristics like left or right dominance. The study has shown that it's attainable to with success find distinct characteristics like gesture size and gesture time characteristics. However, a lot of analysis into touch characteristics is required before the approach will be used for distinguishing users, particularly for automatic of purloined hand-held devices.

In [13] showed that multi-touch gestures contain sufficient biometric info, ensuing from variation in hand pure mathematics and muscle behavior, to permit discrimination between users. A multi-touch gesture is essentially a time-series of the set of x-y coordinates of finger touch points. With score-based classifiers using the time feature only they achieved 4.46 % EER. Further, with the combination of three commonly used gestures: pinch, zoom, and rotate, 58% EER was achieved using a score-based classifier. However, to improve the authentication accuracy and performance incorporate with more features like finger pressure and finger size is need it.

In [14] expanded on their work with a bigger study of youngsters and adults playacting similar touch and surface gesture interaction tasks on mobile devices. A complete of thirty participants (16 youngsters, 14 adults) participated within the study. The extracted options area unit x-coordinate, y-coordinate, time, touch pressure, and touch size for every down, move, and up event because the user created the gesture. They have found frequent intentional and unintentional touches outside of ON screen targets for children, and age-related challenges in recognizing children's gestures, both of which will impact the success of children's interactions. For example, youngsters miss a bigger proportion of targets than do adults, associate degreed generate a bigger quantity of holdover touches when an onscreen target has been chosen. In future studies, they conceive to explore different classification methodology can facilitate to boost accuracy.

In [15] proposed to authenticate people within a biometric technique consisting of recognizing a person performing a 3-D gesture with one of his/her hands while holding a mobile device that integrates an accelerometer. The requirement for the mobile device to be valid for this technique is that it must include a 3-axis accelerometer embedded in it, so that the movement involved in the gesture can be registered. The robustness of this biometric technique has been studied within test analyzing a database of 25 users with real falsifications. Equal Error Rates of 2.01 and 4.82% have been obtained in a zero-effort and an active impostor attack, respectively. Involving more participants and collecting more touch gesture data would help us to get an even better understanding of the performance of the scheme.

In [16] has presented a completely unique approach to authentication, that makes use of biometric data which will be gleaned from multi-touch gestures. They make the most of the multitouch surface to mix biometric techniques with gestural input. The participant practiced a given gesture a couple of times, and once snug thereupon gesture, they were asked to perform it ten times, with the system recording their touches throughout these ten trials.

In [17] developed an application for the android mobile platform to collect data on the way individuals draw lock patterns on touch screen. The data collected on the participants' finger movement times were used to calculate the common standard metrics used to assess biometric systems The EER makes it easier to compare the performance of various biometric systems or classifiers, and the lower its value the better the classifier. Their result showed a relatively low EER of 10.39% was achieved by analyzing the data from 32 individuals using a Random Forest classifier when combining the three different lock patterns and without any analytical enhancements to the data.

3. TOUCH BEHAVIORAL FEATURES

There are several different features of touch behavior biometrics which can be used when the user presses the touch screen. [18] have listed touch behavior features which can be extracted from touch behavior biometrics which are:

3.1 X-coordinate

This parameter is a sequence of numbers which stores the finger position on X-axis on the touchscreen while gesturing [19].

3.2 Y-coordinate

This feature is equal as the previous but it refers to the finger position on Y-axis on the touchscreen while gesturing [20].

3.3 Finger Pressure

This parameter, like X and Y coordinates, keeps track of the finger pressure on the touchscreen. Pressure can be obtained by using Android API MotionEvent. getpressure().The returned pressure measurements are of an abstract unit, ranging from 0 (no pressure at all) to 1 (normal pressure), however the values higher than 1 could occur depending on the calibration of the input device according to Android API documents [21].

3.4 Finger size

Size can be obtained by using Similar to Android API call MotionEvent.getsize() measures the touched size, associated with each touch event. According to Android document, it returns a scaled value of the approximate size for the given pointer index. This represents the approximation of the screen area being pressed. The actual value in pixels corresponding to the touch is normalized with the device’s specific range and is scaled to a value between 0 and 1 [21].

3.5 Finger Time

Time can be obtained by using Android API MotionEvent. getEventTime();.it retrieves the time this event occurred [22].

3.6 Acceleration

Therefore, by getting the distance of touch event form action down to action up and square calculated time, the desired acceleration has been calculated. Moreover need to insert inside the database

4. PROPOSED FRAMEWORK

Fig 1 shows the enrollment capture, training phase, verification procedure and outcome of the behavioral biometric authentication overall works. Enrollment phase consists of three parts enter user name, six times gesture and sample capture. Training phase consists of four parts: feature selection, extract the feature selected, classify and store in database. Verification phase consists of five parts; feature selection, extract the feature selected, classify, comparison template and matching process. Three objectives of this research are feature extraction from the user, classify the features and overall performance of the scheme.

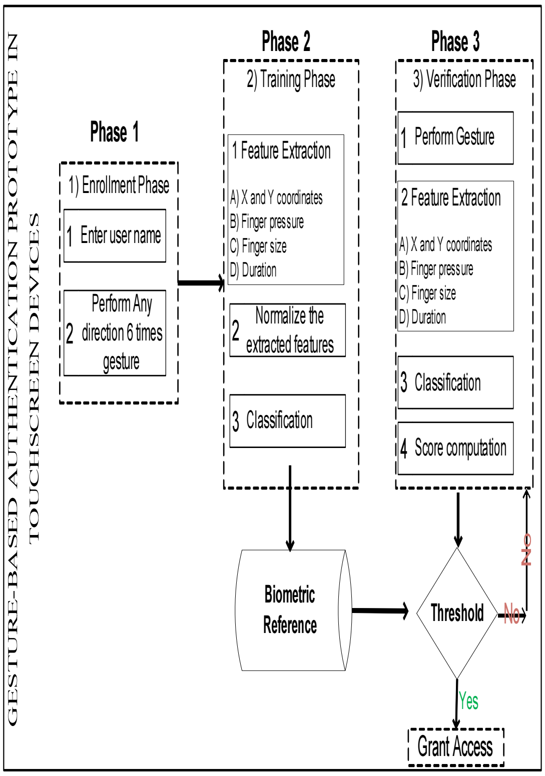

Figure 1: Proposed Framework

4.1 Enrollment Phase

During the enrollment phase as shown in figure 2 each user will be registered in the system. The method in this study is every user will enter his name, six times gesture in any direction and moving to enrollment phase.

4.1.1 User entry

First the participants were given instructions on the task and explained the operation of the system. The second step the user entry start displaying a form where the user has to insert his name. This step is important because the system stores name in a unique string named personal data and will display the content of this variable when the corresponding gesture will be performed in the verification authentication phase.

4.1.2 Gesture entry

In this phase of the study, participants were shown an interface screen allowing the user must to perform his own gesture in any direction. The participants must remember the inserted at least 6 times. The participant practiced a given gesture a few times, and once comfortable with that gesture, was asked to perform it 6 times in any direction, with the system recording their touches during these 6 trials.

4.2 Training Phase

During the enrollment phase as shown in figure 2 each user gesture and will be recorded into the database. However, the timing, acceleration, finger size, finger pressure will be captured and processed to get qualified values for matching in the future. Registered with the system user biometric data is acquired, processed and stored as a reference file in a database. This is treated as a template for future use by the system in subsequent authentication operations. The method in this study is getting required quantities, normalize the extracted featured, calculate the desired quantities, and save the records into the database.

4.2.1 Feature Extraction

The features are the project parameters which allows the system to accept or reject an input gesture. Feature extraction is an automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template called feature extraction. Feature extraction takes place during enrollment and verification-any time a template is created. The feature extraction process includes filtering and optimization data in order to accurately locate features. There are several features of the gesture biometrics which can be used when the user presses the touch screen such as time, finger size, finger pressure and acceleration.

4.2.2 Normalization

Gesture is a dynamic biometric and hence each action time is different from the others. This results in the different number of sampled data even in genuine gesture. In addition, different touch place and different distance of the gesture moving angles factor.

4.2.3 Database

Template generation is the stage where user's gesture feature samples are combined and transformed into a compact yet representative form. These templates are then stored in database for future authentication and retraining use.

```
Get identification
Prepare a touch screen
Attach ID to new dataset
Switch
Case
 MotionEvent.ACTION_DOWN :
        Get pressure;
        Get size;
        Get time;
        Get coordination;
Case
 MotionEvent.ACTION_MOVE:
        Paint
Case
 MotionEvent.ACTION_DOWN :
        Get pressure;
        Get size;
        Get time;
        Get coordination;
Switch end
        If valid()
         then
        Set interface
        Accumulate data
        Save data in database
        Make a dialog
```

Figure 2: Enrollment Pseudo Code

4.3 Verification Phase

Once a user has been enrolled in the system by repeating a certain gesture six times, he/she is able to access the system by performing his/her identifying gesture again. During the verification phase user biometric data are acquired, and processed. When a user make gestures action such as rotate or flick, he/she used to leave some of the important features which can be extracted such time, acceleration, finger size, and finger pressure. The authentication decision shall be based on the outcome of a matching process of the newly presented features to the pre-stored reference templates. The method in this study is getting required quantities, normalize the extracted featured, retrieve the record from database, classification and matching process.

4.3.1 Classification

Classification is to find the best class that is closest to the classified pattern. SVM algorithm is used to classify the features in classification phase. We define a score and we use a threshold to decide if the user is the genuine one or an impostor.

4.3.2 Matching

In order to evaluate the feasibility of applying behavioral biometrics for authentication in secure systems, SVM clustering were used in different experiments. We computed a profile for each member who will be later used as a reference in testing and evaluation.

```
Prepare a new touch screen
        Get pressure;
        Get size;
        Get time;
        Get coordination;
        Accumulate data
Matching the data with existing dataset
        Verification message
```

Figure 2: Verification Pseudo Code.

5. CONCLUSION AND FUTUR WORK

With the increased popularity of touchscreen mobile phones, touch behavior is becoming more and more important compared to the biometric authentication techniques. A gesture based authentication system would make it more difficult for a shoulder surfer to replay the password, even if he observes the entire gesture. Subtleties like force, speed, flexibility, pressure, and individual anatomical differences would prevent the casual observer of the password. Although several researchers have been done touch gesture behavioral biometrics authentication system, there are still some issues are highlighted. The main issue being focused is regarding accuracy rate of EER, FAR and FRR. The second issue is about gathering more touch features in order to get robust authentication and verification result. Hence, extracting touch duration only may not be able to achieve the desired authentication accuracy and robustness. The third issue is collected tested the touch gestures in large group of users. Not many researchers discuss regarding choosing artificial intelligence classification techniques. Our plan for future work in this topic is to implement and test the framework of touch gesture gesture-based behavioral biometrics and obtain more accuracy and robustness authentication system.

6. ACKNOWLEDGMENT

This authors would like to express greatest appreciation to Advanced Informatics School (AIS), Universiti Teknologi Malaysia (UTM) for financial support.

REFERENCES:

[1] 1. Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunar, B., Jiang, Y., et al. Continuous mobile authentication using touchscreen gestures. In Homeland Security (HST), 2012 IEEE Conference on Technologies for, 2012 (pp. 451-456): IEEE

[2] 2. Crawford, H. Keystroke dynamics: Characteristics and opportunities. In Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on, 2010 (pp. 205-212): IEEE

[3] 3. Manaf, Z. A., Ismail, A., Razlan, N. M., Daruis, R., & Manaf, A. A. (2012). Initial Study of the Content Authentication on Digital Preservation of Cultural Institutions. In Advanced Machine Learning Technologies and Applications (pp. 509-515): Springer.

[4] 4. Meng, Y., Wong, D. S., & Schlegel, R. Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones. In Information Security and Cryptology, 2013 (pp. 331-350): Springer

[5] 5. Lashkari, A. H., Manaf, A. A., & Masrom, M. A Secure Recognition Based Graphical Password By Watermarking. In Computer and Information Technology (CIT), 2011 IEEE 11th International Conference on, 2011 (pp. 164-170): IEEE

[6] 6. Sesa-Nogueras, E., & Faundez-Zanuy, M. (2012). Biometric recognition using online uppercase handwritten text. Pattern Recognition, 45(1), 128-144.

[7] 7. El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. A study of users' acceptance and satisfaction of biometric systems. In Security Technology (ICCST), 2010 IEEE International Carnahan Conference on, 2010 (pp. 170-178): IEEE

[8] 8. Jain, A. K., & Kumar, A. (2010). Biometrics of next generation: An overview. Springer Berlin, Germany.

[9] 9. Shanmugapriya, D., & Padmavathi, G. (2011). An Efficient Feature Selection Technique for User Authentication using Keystroke Dynamics. IJCSNS International Journal of Computer Science and Network Security, 11(10), 191-195.

[10] 10. Karnan, M., Akila, M., & Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. Applied Soft Computing, 11(2), 1565-1573.

[11] 11. Wolff, M. (2013). Behavioral Biometric Identification on Mobile Devices. In Foundations of Augmented Cognition (pp. 783-791): Springer.

[12] 12. Sandnes, F. E., & Zhang, X. User Identification Based on Touch Dynamics. In Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on, 2012 (pp. 256-263): IEEE

[13] 13. Sae-Bae, N., Ahmed, K., Isbister, K., & Memon, N. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems, 2012 (pp. 977-986): ACM

[14] 14. Anthony, L., Brown, Q., Nias, J., Tate, B., & Mohan, S. Interaction and recognition challenges in interpreting children's touch and gesture input on mobile devices. In Proceedings of the 2012 ACM international conference on Interactive tabletops and surfaces, 2012 (pp. 225-234): ACM

[15] 15. Guerra-Casanova, J., Sánchez-Ávila, C., Bailador, G., & de Santos Sierra, A. (2012). Authentication in mobile devices through hand gesture recognition. International Journal of Information Security, 11(2), 65-83.

[16] 16. Sae-Bae, N., Memon, N., & Isbister, K. Investigating multi-touch gestures as a novel biometric modality. In Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on, 2012 (pp. 156-161): IEEE

[17] 17. Angulo, J., & Wästlund, E. (2012). Exploring touch-screen biometrics for user identification on smart phones. In Privacy and Identity Management for Life (pp. 130-143): Springer.

[18] 18. Chauhan, S., Arora, A., & Kaul, A. (2010). A survey of emerging biometric modalities. Procedia Computer Science, 2, 213-218.

[19] 19. Miluzzo, E., Varshavsky, A., Balakrishnan, S., & Choudhury, R. R. Tapprints: your finger taps have fingerprints. In Proceedings of the 10th international conference on Mobile systems, applications, and services, 2012 (pp. 323-336): ACM

[20] 20. Westerman, W. C., & Haggerty, M. M. (2011). Detecting and interpreting real-world and security gestures on touch and hover sensitive devices. Google Patents.

[21] 21. Zheng, N., Bai, K., Huang, H., & Wang, H. (2012). You Are How You Touch: User Verification on Smartphones via Tapping Behaviors.

[22] 22. Kerfs, J. (2011). Beginning Android tablet games programming: Apress. 013. Vol. 56 No.2