INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

CONTINUOUS USER AUTHENTICATION USING TOUCH GESTURE STATISTICAL IMAGES FOR SMARTPHONE

Ajay Kumar R C[1], Dr. Sanjay Chitnis[2]

[1]M.Tech in Computer Science & Engineering, CMR Institute of Technology, Bangalore, India.
[2]M.Tech, Ph.D. (IISc), Principal, CMR Institute of Technology, Bangalore, India.

Abstract: - Behavioural biometric for mobile user authentication have started to put on more concentration in the resent years. Authenticating user on the mobile devices can be hard, and at present mobile applications have come up with many solutions which either compromises security or usability. The use of touch gestures as a new biometric modality has been investigated most recently. In this paper the proposed system uses the Touch Gesture Statistical Images (TGSI) to mine the identity traits from the touch traces on the Smartphone screen. The distance value between the traces is used to estimate the authorization of the user's identity. To assess its usability on the authentication setback, touch gesture datasets have been collected which includes commonly used touch gestures. It appreciably reduces the computational time.

Keywords: - Touch gesture, user authentication, mobile security, Touch Gesture Statistical Images, behavioural biometrics.

1. Introduction

The increased use of Smartphone raises the security issues of great importance. In such devices, the user's data that are stored and accessed are merely protected by a point based authentication at the login time. This is lacking because it cannot sense intruders once a user have passed the point entry approach and hence is open to simple attack for example smudge attacks, following loss or theft. In contrast to password or image-pattern-based authentication, Continuous authentication has received bigger concentration in recent years. It either complements point-based authentication or even substitutes it when continuous authentication by cleverly monitoring and analysing the user-device relations to guarantee truthful identity, which satisfies meticulous accuracy requirements. While using a Smartphone, multiple integrated sensors - the touch screen, motion sensors, microphone, or camera - can be used to sense the user's identity. Users' face and voice can be used for verification, but it is not suitable or most favourable to apply these approaches while the user is using most of the apps like reading news and email, surfing the internet, etc. Users must face the camera or keep talking to be always authenticated, which very much reduces the device usability. Due to signal noise and difficulty in decoupling identity from activity, authentication using motion data case in point Accelerometer/Gyroscope data, currently can only be applied on motion-specific activities example phone pick-up motion during answering the call. On the other hand, the touch screen is pretty appropriate for authentication, not only since it is the most regularly used sensor but also the touch gesture contains identity-rich user behavioural character. Investigating

the probability of using touch gestures as a biometric modality, it can be practical that most of the touch traces from a single user have a propensity to go behind a similar pattern while the patterns differ among diverse users.

In this paper, we investigate a touch gesture based continuous mobile user authentication presenting a novel Touch Gesture Statistical Images (TGSI). TGSI sees the touch gesture traces as x-y coordinates and converts them into images with the help of these statistical data. The statistical information of the x-y coordinates are collected from a sequence of commonly used touch traces. They are then shaped into images for a fixed number of sample points. TGSI learns the intra-person variation making a statistical analysis on these images and it is able to synthesize a new instance according to a new probe trace. Here the distance between the probe trace and the gallery traces corresponding to the given user specific TGSI. This distance tends to a large value if the trace originates from a user other than the original user [1]. We evaluate the proposed method on four touch gestures – scroll up/down, scroll left/right – since they are the most commonly used gesture types by any set of users. Scroll up/down is usually used for reading text or browsing menus while Scroll left/right is usually used for browsing photos, translating screen, and unlocking phones.

Our important contributions are: (i) applying the feature representation principle in SFM to touch gestures by TGSI; (ii) developing the algorithms to apply the TGSI on the mobile user verification and recognition problems; (iii) systematically evaluating the proposed algorithm by varying different parameters; and (iv) develop an Android app and testing performance of the verification algorithm in a real-world scenario.

The rest of paper is organized as follows. First, we discuss the related work in Section 2. Proposed system is briefed out in Section 3. Section 4 presents the experimental results. In Section 5, we conclude our study.

2. Related Works

The system of biometrics is an active way to recognise and verify users authenticity based on their natural characteristics. The uses of biometric have been studied for many years [2]. Biometrics can be broadly classified into types – physiological biometrics and behavioural biometrics. Physiological biometric include identifying user by finger print [3], facial characters [4], etc., while behavioural biometric include identifying user by implementing identity invariant characters of human behaviour to authenticate users during their daily activities [5].

Previous investigations on behavioural biometrics have revealed that biometric qualities can be mined from physical characteristics of arm gestures [6] [7], strokes and signatures with pen or stylus [8][9]. Yamazaki et al. [10] showed identity of an individual can be dug out from individual features like stroke shape, pen inclination and writing pressure. Cao et al. [11] deliberated a measureable human performance model of making single-stroke pen gestures. Ferrer et al. [12] used local patterns to section signature and extract identity features. Impedovo et al. [13] presented the state-of-the-art in automatic signature verification. Yet, authenticating users with the strokes of pen cannot be persistently used in mobile user verification as only a few mobile types have come up with pen and stylus. Also, maximum operators choose to use their finger for the direct interaction with their mobile phones. In the resent years studies are made discovering the touch gesture a biometric type [14]. Feng et al. [15] pulled out finger motion speed and acceleration of touch gesture as character for proof of identity. Luca et al. [16] figured out the distance between traces using the dynamic time warping algorithm. Sae-Bae et al. [17] involving different combinations of five fingers, designed 22 touch gestures for authentication. They computed the Freshet distance between multi-touch traces and dynamic time warping distance. But, users must still perform their pre-defined touch gestures, which would not be clear and no conspicuous to users for authentication. Frank et al. [18] calculated the correlation between 30 logical skins from touch traces and classified these features using K-nearest-neighbour and Support Vector Machine approaches. Still, the analytic features did not capture the touch trace dynamics.

The proposed method is quite different from existing works. TGSI applies the similar feature representing principle of the statistical feature model in [19] to learn the intra-person variations from many traces by a user so that scores are computed between pairs of gallery traces and probing traces, which significantly reduces the computational time.

3. Proposed Method

The scenario of authentication considered in this paper comprises exposed set user recognition and user verification. In the open set user authentication scenario, the sensitive data stored in the device must be accessible only by its correct owner. Hence this method validated the access of the user continuously to know if the right person is only able to access the device. To achieve this moto, we arrest the touch traces from the touch screen output and segment the traces with provision from the Android API. We use a series of x-y coordinates of the finger touch points. We find a variation in the different variations. To exclude this variation, the captured traces are pre-filtered into one of these four predefined gestures based on screen regions where the traces start and end. The four gestures ensure the generality and usability of the proposed method.

A. Touch Gesture Statistical Image

We propose a system that uses Touch Gesture Statistical Image (TGSI) and works with the help of Statistical Feature Model (SFM). TGSI learns the intra-class variation mode and synthesizes the new instance using the learned base characteristic and affine merging of these learned modes. The system first learns the sample patterns from the original user generating n (n=15) number of gesture images. These gestures are then converted into a single probe which is stored to the device storage. Then when the system is run the user will be continuously authenticated in the background. This will generate gesture images of the user and is verified with the saved probe. In the testing phase, the TGSI expresses the probe trace in the new basis as synthesized instances. The distance between the synthesize probe instance and the original probe instance is computed for verification. This distance tends to be greater when the probe is from different users than those from the same user as the one on which the TGSI trained. Since the TGSI is learned with the specific knowledge of the user, its representation power decreases for others. Thus, less similarity exists between the synthesized and original instances extracted from others' traces.

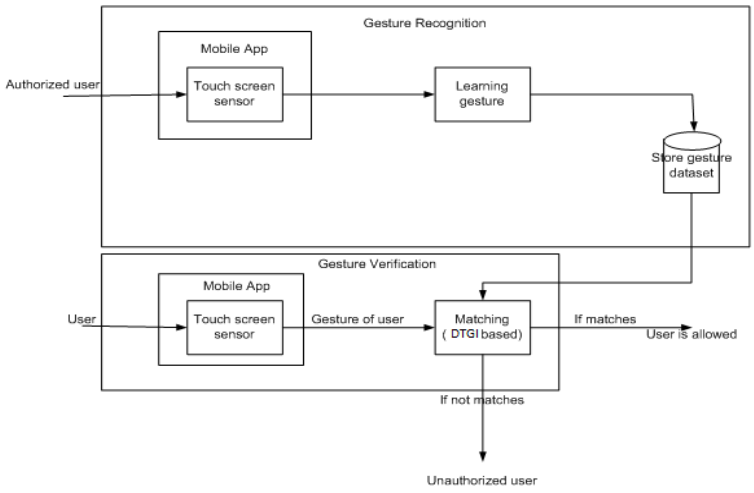

Fig 1: System Architecture

The architecture of TGSI mainly contains two major parts

- **Gesture Recognition**
- **Gesture Verification**

Gesture recognition part is where the authorized user provides the sample traces for the purpose of learning the characteristics of his/her commonly used swipe gestures through the touch screen sensor. These samples are merged into one single probe and this is stored in the storage device.

In the Gesture Verification, mobile app runs at the background to collect the traces of any user who access the through touch screen sensor. This is then validated with the original probe stored at the stored gesture dataset. If

the validation is matched, then the user is considered authorized and will be certified to access the device. Otherwise the user is restricted from the access to the device.

B. User Authentication Algorithm

1) *TGSI Training*: The training algorithm takes as input a set of touch traces per gesture type from the user and outputs the trained TGSI. This training process runs repeatedly for all types of touch gestures (i.e., LEFT - RIGHT, RIGHT - LEFT, DOWN - UP, UP-DOWN) to finish the training every trace in the training set, it is first reshaped into gesture image. The 2D shape information lost due to reshaping can be easily restored by a reverse reshaping process before score computation.

Algorithm 1: Training Algorithm (Pre Gesture Type)

Input: The Training set of touch gesture (type t) traces S^t_u from the user u.
Output: The user-specific Statistical Touch Images D^t_u.

1. For each trace S_i e $S^t_{u:}$
    1. Extract the Gesture image T_i,
    2. Reshape the 2D matrix T_i into vector t_i,
2. Learn the base vector v' and basis feature vectors v_i by applying Statistical Analysis.

2) *TGSI Testing*: The testing algorithm takes a probe trace and a trained model as input, where the model and the trace share the same gesture type. The output is a score d representing the distance between the trace and the user represented by the trained model Dtu. The trained TGSI has the capability to synthesize different instances. If the score d varies in a major way, then the user is unauthorized and is restricted from the access.

Algorithm 2: Testing Algorithm

Input: A probe trace S^t_p and the trained model D^t_u.
Output: The score d.

1. Extract the GTGF T^t_p from the probe trace S^t_p ,
2. Reshape T^t_p into v^t_p ,
3. Synthesize the instance v'^t_p ,
4. Reshape the vector v'^t_p back to T'^t_p
5. Compute the score d between T^t_p and its responding instance T^t_p .

4. Experimental Results

A. Data Acquisition

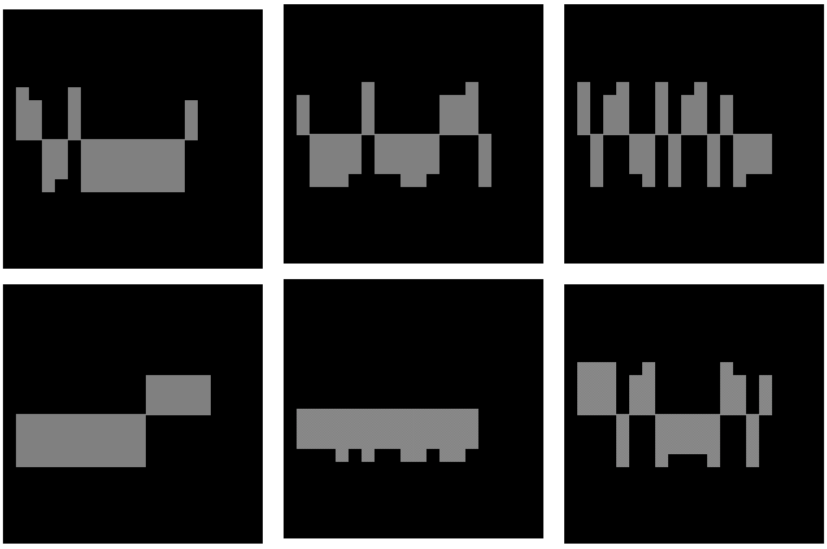

Fig 2: Trace probes from different subjects

We developed an Android App to collect the touch gesture data that captures the touch gestures using the standard API of Android system. When the fingers came in contact to the touchscreen, it begins recording the raw touch samples from the API. For each sample in a trace, an event flag (e.g., onDown, OnScroll, onFling, Zoom), the (x,y) coordinates are captured. We requested 10 subjects for our study, of which 6 were right-handed, 5 had touchscreen device experience. First the purpose of the study and the usage of our data acquisition program were explained to all the subjects. Once the subject can use the App in a natural way, they provided 30 touch traces they commonly use. The touch gestures are performed in the way that the subjects feel normal and ease. Thus, subjects may vary the manner they held the phone like, left-hand holding vs right-hand holding, whole palm holding vs half palm holding, the hand pose (palm down vs palm up) or the fingers used to perform the single touch gesture (thumb vs index finger) or the finger orientation between sessions.

Equal Error Rate was mostly used as the evaluation criterion for our verification experiments. It is the common value when the false acceptance rate (FAR) and the false rejection rate (FRR) are equal. We opt to use it simply because it accounts for the trade-off between FAR and FRR. Meanwhile, we also reported ROC curves in some experiments for clarity purpose.

B. Experimental Results

First we evaluated the performance of TGSI different time stamp of acquiring the stored probes stored in the gallery and computing them against the generated probe. To evaluate the performance of the proposed method using different combinations of touch gestures and compared the methods with the methods available in the literature. The same gallery and probe set were used. as in the previous experiment. After score computation, we obtained one score matrix for each gesture. Then, we fused the score matrix of multiple gestures using the sum rule, which is proved by Kitller et al. [20] to be superior in comparison to other rules The same gallery and probe set were used (i.e., product, min, max, median rule). An average EER of 4.1% and RR of 88.4% was found.

To test the performance and usability of the TGSI based user authentication method in a real world scenario, we used the implemented App TGSI to verify the users. Open set user recognition is excluded from this test since the Android system (version 4.1.x) does not currently support multiple user account management. A gallery of traces for each subject is formed by randomly selecting traces to cover variations in touch manner. During testing, the app ran on a Samsung Galaxy S3 phone with Android version 4.1.1. It has Quad-core 1.4 GHz Cortex-A9 CPU and 1GB RAM. TGSI is built for each subject per gesture from a number of traces in the gallery. The computational time for TGSI remains at around 12:90 ms. As increased from 30 traces per gesture to 100 traces, the EERs achieved by TGSI decreased.

The distance from the probe trace and the distances from the following consecutive probe traces are averaged to obtain the score for authentication. If it is above the threshold (16), the app classifies the user as an unauthorized intruder and invokes explicit user authentication message.

5. Conclusion and Future work

In this project we present an authentication approach based on touch gestures. This project provides a statistical way to verify and validate the mobile users in a continuous manner. In this way the unlike the point based authentication which only authenticate at the entry stage, the TGSI continuously verifies every touch traces made by the user and validates to authorise the user to access the device. The TGSI based authentication app has been implemented and tested on a dataset collected during the daily use of the phone. The results show that the use of the TGSI in the real world will enhance the mobile user security in a greater way.

Also this paper discusses a method of converting the touch gestures into statistical image and is verified for authorization. A possible way of transforming the touch gestures into binary images and make use of them may offer a better way of authentication. Unlike the TGSI which requires the touch gestures to be converted into statistical image and then compared, this proposal for the future work would directly compare the generated resource reducing the time of conversion and storage space.

6. Acknowledgment

I would like to Dr. Sanjay Chitnis, Manoj Chella and Prathap for their valuable guidance and feedback which was a major requirement for the creation of this work. Thanks also to the reviewers for their helpful comments.

REFERENCES

[1] A. Bragdon, E. Nelson, Y. Li, and K. Hinckley, "Experimental analysis of touch-screen gesture designs in mobile environments," in Proc. the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada: ACM, 2011, pp. 403–412.
[2] M. S. Obaidat and B. Sadoun, "Keystroke dynamics based authentication," in Biometrics, A. K. Jain, R. Bolle, and S. Pankanti, Eds. New York: Springer, 2002, pp. 213–229.
[3] S. Li and A. Kot, "Fingerprint combination for privacy protection," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 350–360, 2013.
[4] X. Zhao, S. K. Shah, and I. A. Kakadiaris, "Illumination normalization using self-lighting ratios for 3d2d face recognition," in Proc. European Conference on Computer Vision: Workshops and Demonstrations. Firenze, Italy: Springer Berlin Heidelberg, 2012, pp. 220–229.
[5] A. Messerman, T. Mustafic, S. Camtepe, and S. Albayrak, "A generic framework and runtime environment for development and evaluation of behavioral biometrics solutions," in Proc. International Conference on Intelligent Systems Design and Applications , Cairo, Egypt, 2010, pp. 136–141.
[6] D. Gafurov and E. Snekkkenes, "Arm swing as a weak biometric for unobtrusive user authentication," in Proc. International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, 2008, pp. 1080–1087.
[7] T. Feng, X. Zhao, and W. Shi, "Investigating mobile device picking-up motion as a novel biometric modality," in Proc. IEEE International Conference on Biometrics: Theory, Applications and Systems, Washington D.C., USA, 2013, pp. 1–6.
[8] M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW," Pattern Recognition, vol. 57, no. 3, pp. 981-992, March 2007.
[9] A. Kholmatov and B. Yanikoglu, "Biometric authentication using online signatures," in Proc. International Symposium on Computer and Information Sciences, Antalya, Turkey, 2004, p. 373-380.
[10] Y. Yamazaki, Y. Mizutani, and N. Komatsu, "Extraction of personal features from stroke shape, writing pressure and pen inclination in ordinary characters," in Proc. Fifth International Conference on Document Analysis and Recognition, Bangalore, India, 1999, pp. 426–429.
[11] X. Cao and S. Zhai, "Modeling human performance of pen stroke gestures," in Proc. SIGCHI Conference on Human Factors in Computing Systems, San Jose, California: ACM, 2007, pp. 1495–1504.
[12] M. A. Ferrer, A. Morales, and J. Vargas, "Off-line signature verification using local patterns," in Proc. 2nd National Conference on Telecommunications, Arequipa, Peru, 2011, pp. 1–6.
[13] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 38, no. 5, pp. 609–635, 2008.
[14] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong, "Senguard: Passive user identification on smartphones using multiple sensors," in Proc. International Conference on Wireless and Mobile Computing, Networking and Communications, Cagliari, Italy, 2011, pp. 141–148.
[15] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in Proc. IEEE Conference on Technologies for Homeland Security, Boston, Massachusetts, 2012, pp. 451–456.
[16] A. D. Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: implicit authentication based on touch screen patterns," in Proc. SIGCHI Conference on Human Factors in Computing Systems, Austin, Texas, 2012, pp. 987–996.
[17] N. Sae-Bae, N. Memon, and K. Isbister, "Investigating multi-touch gestures as a novel biometric modality," in Proc. IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington D.C., USA, 2012, pp. 156–161.
[18] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," IEEE Transactions on Information Forensics ad Security, , vol. 8, no. 1, pp. 136–148, 2013.
[19] X. Zhao, E. Dellandr´ea, J. Zou, and L. Chen, "A unified probabilistic framework for automatic 3D facial expression analysis based on a bayesian belief inference and statistical feature models," Image and Vision Computing, vol. 31, no. 3, pp. 231–245, 2013.
[20] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On combining classifiers," IEEE Transactions on Pattern Analysis and Machine Learning, vol. 20, no. 3, pp. 226–239, 1998.