ABSTRACT
We propose a biometric authentication scheme suitable for multi-touch devices such as tablet computers. Our scheme is based on hand geometry. It improves on prior work by introducing a dynamic element, where movement challenges are issued based on static hand geometry data. Specifically, we demonstrate a set of multi-touch interactions that can capture hand geometry information of users. For each of the interactions, we extract different but complimentary hand geometric information from the user. Our approach has several advantages over traditional text password and other biometric authentications. First, unlike other recognition based authentication schemes, a user is only expected to interact with the multi-touch surface according to the challenges she is posed. In other words, she does not have to memorize any type of credential. In addition, the system provides security against replay attacks—which is a drawback associated with many authentication schemes, such as traditional biometric system based on recognition of face, iris or fingerprint. Last but not least, our approach works on current tablet computers without any needs for updates of hardware, firmware or drivers—it can be carried out by an application. We demonstrate experimentally a configuration using 14 consecutive challenges on iPod2 tablet (taking approximately 3.32 minutes for novice users to respond to), wherein the user is authenticated with almost 97% accuracy.

Categories and Subject Descriptors
K.6.5 [Security and Protection]: User authentication

Keywords
Biometric, Hand geometry, Multi-touch interaction

1. INTRODUCTION
We are provided with constant reminders of the risk associated with passwords: Every time another service provider’s password database gets compromised and millions of password records are stolen, financial institutions all over the world see a rise in fraudulent access attempts using credentials that are the same or similar to those that were stolen. For users without good spam filtering, phishing emails are a frequent reminder of the relation between abuse and authentication. Of course, the password problem is not restricted to site compromises and phished credentials but includes weak passwords that were brute-forced and credentials that are used by so-called ‘friendly fraudsters’ [16]. Deloitte recently estimated that more than 90 percent of user-generated passwords—including those considered strong by IT departments—are vulnerable to hacking [6]. While it is only in the last few years that the risk associated with passwords has become commonly accepted and has received serious media attention [5], Bill Gates famously argued already in 2004 that it is only a matter of time until passwords would be dead [3]. Whether or not passwords will truly vanish, we are very likely to increasingly see alternative authentication methods being offered. One such method is biometrics. Apart from relieving users from having to recall large numbers of credentials, and strengthening credentials against brute-force guessing, biometric methods offer additional protection in comparison to what passwords do. For example, biometrics offer additional protection against friendly fraud—abuse where credentials are shared and where users (such as family members of the account owner) perform transactions without the permission of the account owners. While there is hope for broad hardware support for biometric authentication in the near future [1, 2], it will most likely be many years until such technologies are ubiquitous. In the meantime, and in order to address what will then be considered legacy devices (and which represents current state-of-the-art consumer devices), there is a need for biometric authentication that does not require additional hardware. In this paper, we consider biometric authentication on tablets.

Biometric methods can be used for regular authentication, step-up authentication and backup authentication—depending mostly on the convenience and speed of the method and the tolerance for error. In its current guise, the method we propose is primarily useful for step-up and backup authentication due to the relatively long engagement needed from the user to obtain sufficiently low error rates. However, our implementation should be seen as a proof of concept—showing that one can attain low error rates without need for specialized hardware and without relying on user recall. We are optimistic that the novel approach we introduce—the use of so-called dynamic challenges—can be streamlined to improve the speed-error tradeoff enough to make the resulting version meaningful for regular authentication needs as well. Here, a dynamic challenge is one that is generated on the fly, based on knowledge of the biometric features of the account owner—whereas traditional (static) challenges do not use this type of information. For example, based on knowledge of the length and flexibility of a given user’s fingers, a dynamic challenge can be selected to maximally distin-
The outline of the paper is as follows. First, we begin by describing the related work in section 2. Next, in section 3, we present the details of hand geometry challenges that are designed for authentication purposes as well as describing the method to derive features and similarity score. In section 4, we provide experimental details along with the qualitative and quantitative results. Then, we present limitation of this work in 5. Lastly, we conclude and discuss future work in section 6.

2. BACKGROUND

Fingerprints—the earliest type of biometric method used at a large scale—have been used for over 150 years, and fingerprint readers are increasingly incorporated in mainstream consumer devices. In spite of increasing consumer acceptance and greater deployment of fingerprint readers, it is likely to take many years until the presence of fingerprint technology can be relied on. In the meantime, biometric authentication based on hand geometry promises to bridge the gap, and potentially maintain a sizeable marketshare. This realization has spurred significant research efforts (e.g., [11, 13, 18]) and its commercial impact is expected to exceed $150 millions in 2018 [4].

In terms of research effort on hand geometry authentication, a large portion of the previous work has focused on acquiring the information through imaging devices—scanners, 2D cameras and 3D cameras [14, 17]. The images captured using scanners introduce less variation and require less sophisticated image processing techniques to extract features than those captured from cameras due to the more uniform background as well as the static distance and orientation between the sensor and a user’s hand. However, such schemes are not very user-friendly for public access control application as they require users to make direct, physical contact to the publicly shared sensor [11]. In addition, it is not appropriate for mobile applications as the scanner is typically too large to carry. In contrast, the upshot of using cameras is that they provide a contact-free authentication, which addresses hygiene concerns. Camera-based approaches are therefore well suited for physical access control systems, but less natural in the context of mobile authentication, since many methods require extra hardware as well as a careful distance setup between the object and camera.

To apply hand geometry authentication on mobile devices, and without introducing additional sensors, researchers have proposed to use a mobile camera to capture the pattern of palmprint in a user’s hand [10, 12]. Systems of this type are disturbed by lighting conditions and noisy background. Moreover, they are easily abused using replay attacks, since these methods do not (yet) offer any liveness detection mechanisms to ensure that the presented object is indeed a user’s hand and is not a replayed image or video footage. In our effort, we have limited ourselves to approaches that rely solely on sensors that are already part of commercial off-the-shelf devices—a multi-touch sensor in particular. Therefore, we do not have the benefit of using such palmprint texture [15], vein pattern, 3D features [22], etc. Without such information, Julian et al. [9] demonstrated that a system could still achieve 98% identification rate using just the lengths of four fingertips–thumb excluded. While, in their approach, a scanner is used as a sensor device, the result is nevertheless encouraging since the type of features they use could also be measured via multi-touch interactions. However, while theoretically possible, designing such interactions to capture robust and detailed information is a challenging problem due to the limited capability of today’s multi-touch sensors. More specifically, common sensors can only capture a limited number of touchpoints at any particular time—20 points for iOS 6, for example. In addition, each touchpoint may not coincide with user’s intention [8, 21], whereby introducing additional noise to data captured from the touch sensor.

We note that we are not the first to focus on deriving biometric information from multi-touch interaction. Sae-Bae et al. [19] showed that 5-finger multi-touch gestures like pinch, zoom and drag can be used to authenticate users, given that such gestures communicate hand geometry information. Their method is based on users having to recall a sequence of actions (namely, the gestures), and as such, it is not a pure biometric approach, but also relies on recall. In contrast, we develop a set of multi-touch authentication challenges that are designed to capture a user’s hand geometric information without having to rely on any memorization. Based on experiments we describe, we show that multi-touch challenges can be used to authenticate users using hand geometric information.

3. OVERVIEW OF HAND AUTHENTICATION ON MULTI-TOUCH TABLET

The proposed authentication system has two stages: enrollment and verification. During the enrollment, a user is asked to respond to a set of predefined multi-touch challenges that are designed to capture different but complementary characteristics of his hand geometry. The system then captures time-series data of the multi-touch attributes and use it to build the user’s profile. Later, when the user requests access, he would be prompted to provide multi-touch responses to a set of challenges. Based on the user’s responses and the stored profile, the system decides whether to grant the requested access.

Authentication Challenges: The design goal of multi-touch authentication challenges here is to derive hand geometry information that is different from one user to the others but which remains largely the same between different sessions for one and the same user. Specifically, the system should be able to authenticate a user using his response to a set of designed challenges. The details of authentication challenges that are used in our experiment are as follows. Broadly speaking, the challenges in this study are divided into two types: Spread and Tap—where a user is asked to spread his fingers and tap them on the screen, and Place and Draw—where a user is ask to place three fingers on the screen and use another to draw a pattern.

3.1 Hand Measurement Using Spread and Tap Challenges

In this set of challenges, a user is asked to spread two fingers as much as possible and then tap them on the screen (see example of instruction in Figure 1). A spread distance between two fingertips depends on the geometry of user’s hand and its flexibility with respect to those two fingertips. Therefore, the
more number of distinct spread distances, the more information the system learns about the user’s hand resulting in higher authentication accuracy. In total, there are \( \binom{6}{2} = 15 \) challenges deriving from one hand.

### 3.1.1 Feature Extraction

This spread distance is computed from the first pair of touch points that are tapped by different fingers. Then, it is used as a feature for the challenge \( i \), namely \( f_i^a \). The algorithm to compute \( f_i^a \) is described as follows.

Let \( P = \{ (x_1, y_1), \ldots, (x_n, y_n) \} \) be a set of points that is sorted in a timely manner:

1. distance := 0
2. \( i := 1 \)
3. While \( \text{distance} < \text{Threshold} \)
   
   \[
   \text{distance} := \sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2}
   \]
   
   \( i := i + 1 \)
   
   \( f_i^a := \text{distance} \)
4. Return \( f_i^a \)

### 3.1.2 Distance Metric

Since the proposed scheme is an interaction based verification system, it is important that the user is honest – pay attention and be cooperative. However, a small outlier between different trails of the same user due to human error (which is common) should be tolerated. The proposed distance metric is designed to cope with this outlier. Specifically, for any given two sets of features, a feature with the largest difference between the two sets is eliminated before computing 1-norm pairwise distance or Manhattan distance. That is,

\[
D_1(F_a, F_b) = \sum_{i=1}^{N} | f_i^a - f_i^b | - \max_i | f_i^a - f_i^b | 
\]

where \( F_a = < f_1^a, \ldots, f_N^a > \) is the vector of \( N \) distance measurements of user \( a \) and \( F_b = < f_1^b, \ldots, f_N^b > \) is the vector of \( N \) distance measurements of user \( b \).

### 3.2 Flexibility Measurement Using Place and Draw Challenges

In this set of challenges, a user is asked to place three fingers at the fixed position in order to lock their hand down before using the forth one to draw an arc (see an instruction example in Figure 2). It should be noted that, since the movement of hand and fingertips in this set of challenges are different from those Spread and Tap, they can provide additional information about user’s hand geometry. More specifically, two users who respond to Spread and Tap challenges similarly might have different hand sizes and shapes since the user with the smaller hand may have better flexibility in spreading fingers. In this case, their responses to the same Place and Draw challenge would be different since their hands would be placed at different positions and in different configurations. In total, there are 4 challenges consisting of the following combinations. For the first two challenges, the placing fingers are thumb-index-ring and thumb-middle-ring, respectively, while the drawing finger is little finger. For the last two, the placing fingers are thumb-middle-little and thumb-middle-ring, respectively, while the drawing finger is index finger. Finally, we ensure that the distances between those placing fingers are not too far to reach for each and every user by setting them at 80% of the ones derived from Spread and Tap response of that user. The user response in this set is considered as dynamic interaction since a drawing path of the specific fingertip is indeed a series of touch points.

#### 3.2.1 Feature Extraction

Given that a user’s hand is static while drawing, a drawing path would be a circular arc centered at the corresponding joint. For example, if the little finger is used to draw an arc pattern, the center would be at a position of the joint between the little finger and palm where its radius is specified by the length of the little finger.

However, while the drawing pattern is expected to be an arc (a smooth and continuous curve), this is not always the case. We noticed that some users could hardly stabilize their hand position and other fingers while drawing a pattern. Therefore, a polynomial of degree 2 is chosen as a curve description for the sake of generalization and simplicity. In addition, it is not straightforward to compare and derive a pairwise distance from any given two drawing paths when they are series of points with unequal length. To cope with this unequal length issue, a drawing path with arbitrary length is first summarized using a short and fixed size description. Finally, a feature is derived from this fixed size description. The process to derive polynomial description is as follows. First, all touchpoints are manually labeled by the corresponding fingertips before performing point alignment. Then, those labeled points are processed as follows.

1. Point alignment: Let \( x_0 \) and \( y_0 \) be a mean value of \( x \) and \( y \) coordinates of all thumb touch points, respectively. All the touch points are then offset by \( x_0 \) and \( y_0 \) as follows:
   \[
   (x, y) \rightarrow (x - x_0, y - y_0).
   \]

2. Polynomial curve fitting: Let \( P = \{ (x_1, y_1), \ldots, (x_n, y_n) \} \) be a set of points that are drawn by the specific fingertip. The goal is to find \( A_2, A_1 \) and \( A_0 \) that minimize
3.2.2 Distance Metric

Finally, the dynamic challenge's distance is defined as:

\[
D_2(F_a, F_b) = \min_{i \in \{1, \ldots, m\}} |f_i^b - f_i^a|
\]  

(2)

where \(F_a = \{f_1^a, \ldots, f_M^a\}\) is the set of \(M\) average angle features of user \(a\) and \(F_b = \{f_1^b, \ldots, f_M^b\}\) is the set of \(M\) average angle features of user \(b\). Noting that, from our observation, the consistency of user's responses in this set of interactions is lower than the first set. Therefore min rule is chosen as the metric in order to alleviate this issue.

4. EXPERIMENT

In this section, the details of data collection are described. Then the result in terms of verification performance, verification time, user feedback and other observations that we came across while running the experiment are provided.

4.1 Data collection

Before an experiment started, the users were seated in front of the iPad 2 that placed on the table. First, they were informed that it was an experiment about hand geometry biomometric without revealing recognition algorithm that we planned to use, and were instructed that they were expected to follow the given instructions that appeared graphically on the screen. Then, the process began by asking the users to perform exercises with their hand and fingers by slowing making fist for three times. Then, they were asked to follow the instructions that would appear on the screen step by step. In addition, at the beginning of the first interaction of its kind, an illustration video of a user performing an interaction was presented to the users. This was to give visual instruction to them and to ensure that all of them received the same information about the test. The experimenter supervised the users only to ensure that correct interactions had been entered to the system. At the end, they were asked to provide feedback about the scheme. In total, there were 15 different interactions where each subject were asked to perform 2 independent set of interactions back to back in order to avoid muscle memory. In other words, each pair of the same interaction was interrupted by 13 other interactions.

**Apparatus:** We developed and used an iPad application to consistently present the challenges to the users. The user response-time series of multi-touch points and its time-stamps–was collected and sent back to the server for analysis purpose. The real-time feedback, i.e., the scattered plot of touchpoints were also presented on the application at real-time to notify the user about whether the data were received properly or not.

4.2 Results

Overall, 44 subjects were recruited. 12 out of these were female. Most of the subjects were 25 to 40 years old. One subject that had to leave before finishing experiment was excluded from the dataset. All the experiments were performed using a subject’s right hand regardless of his or her hand-wise since the interactions were not meant to measure the hand’s skill of the subject but rather to extract his or her hand geometric information. The data that were collected included time series of multi-touch points and its time-stamps–was collected and sent back to the server for analysis purpose. The real-time feedback, i.e., the scattered plot of touchpoints were also presented on the application at real-time to notify the user about whether the data were received properly or not.
3,655 comparisons. If the pair is drawn from the same user, the dissimilarity score is counted as genuine score. Otherwise, it is counted as imposter score. Therefore, the number of genuine and imposter scores are 43 and 3,612 respectively. First, we use only the features from Spread and Tap challenges, or spread distances between a pair of fingertips. In total, there are 10 features. Using all 10 features to derive a first order Manhattan distance between a pair of samples as a similarity score, some statistic about these two distributions and performance are as follows. For that of genuine samples, its mean and standard deviation is 199.24 and 90.76, respectively. For that of impersonation samples, its mean and standard deviation is 728.30 and 396.64, respectively. Figure 4 shows the Receiver Operational trade off between FAR (False Acceptance Rate) and FRR (False Rejection Rate) where HTER (Half Total Error Rate) is at 8.04%. Also, FAR at which FRR* = 2.33% and sample rejection rate = 1/43, or 2.33%. Noting that, in Figure 5, the curves are drawn without removing outliers. As a result, the false rejection rate that is presented is the sum of FRR* and the sample rejection rate.

Furthermore, when the distance that is derived from this 8-feature subset is combined with the distance computed from Place and draw challenges, the verification performance is depicted in Figure 6. Specifically, FAR decreases from 8.06% to 3.93%, at FRR* = 2.33%. This implies that complementary information could be derived from different types of multi-touch challenges. Noting here that, the two distances were thresholding before combined using "AND" rule where the threshold for the Place and draw gesture is placed at FRR = 0%. That is, a sample is accepted if and only if both distances were below experimentally defined thresholds.

4.2.2 Verification Time

On average, the users spent 5.14 minutes (σ = 1.04) to complete the first set which consists of 15 tasks, and they spent 3.32 minutes (σ = 0.72) for the second set. One-tailed student t-test indicates that the amount of time the user spends on the second set of the same challenges is statistically less than that of the first set (p = 6.2 × 10⁻¹⁵). This implies that the users could quickly get familiar with the interaction within one session of training.

4.2.3 User feedback

We anticipated that we incurred a set of brand new interactions to the users at the time they performed experiment. In other words, it was likely their first time to interact with the touch panel in the way we proposed. Hence, it is equally important to us to learn whether the users could comfortably perform interactions and in which extent. Therefore, at the end of the session, the users were asked about general comments they have for the instruction that were given to them. Some of the users raised a concern that there were too many steps to follow and some did not keep their hand still while responding to Place and Draw challenges. However, in general, most of them responded that it is not hard to perform and got much better in their second times. In addition, some people asked questions about its applications and expressed their interests in this new concept.
5. LIMITATION

While this paper presents a proof-of-concept set of user interactions to demonstrate that the approach is viable, it is likely that a more practical version of the scheme could be developed by selecting other user interactions. For example, one could potentially design other interactions that would extract unique and consistent information from users more effectively, thereby achieving better performance. Furthermore, like most biometric approaches, our approach cannot guarantee that all users can successfully authenticate. Specifically, our approach is not suitable for users with injured hands. Second, while our initial results are promising, a more in-depth study shall be performed before deploying the system. This includes testing of a larger number of users as well as an investigation of the effects of the time between enrollment and verification. While our approach does not rely on recall, there are long-term flexibility changes that may affect the utility of the approach after long periods of time – especially for elderly users. It would also be interesting to more carefully study the effects of gender and age. Finally, the system security against various threat models shall be investigated.

6. CONCLUSION

In this work, we demonstrated that reading hand geometry biometrics using multi-touch tablets is viable and is a new plausible unobtrusive biometric approach for authentication.

One advantage of the proposed system over legacy backup authentication system is that it is designed only to take users’ biometric information as an input; the users are not expected to memorize any verification’s credentials. Schechter et al. [20] reported that 16% of the users are unable to recall his/her answer within six months for the most memorable set of questions, Yahoo! webmail service. In addition, security is another advantage of the proposed system. Security password questions are typically guessable. They [20] also showed that between 44% and 18% of the questions were correctly guessed by his/her partners for the answers. It could also be applied as an additional authentication factor by combining with other available credentials or other biometrics, for example, voice or face, without exacerbating the memorability problem.

Finally, while this paper provides a glimpse of possible hand geometry verification gestures, the complete sets of gestures are countless. One area of future work would be to focus on searching and redefining a set of static and dynamic interactions that optimize both usability and performance of authentication. In addition, the performance improvement as a function of user’s familiarity also deserves further investigation.

Acknowledgment

The authors would like to thank all participants in this study. We also would like to express our special thanks to Jim Palmer and Anke Werner for their help.

7. REFERENCES


