Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-touch Devices

Napa Sae-Bae, Kowsar Ahmed, Katherine Isbister and Nasir Memon
NYU-Poly
Five Metrotech Center, Brooklyn NY 11201
{nsae-b01, kahmed01}@students.poly.edu, {isbister, memon}@poly.edu

ABSTRACT

In this paper, we present a novel multi-touch gesture-based authentication technique. We take advantage of the multi-touch surface to combine biometric techniques with gestural input. We defined a comprehensive set of five-finger touch gestures, based upon classifying movement characteristics of the center of the palm and fingertips, and tested them in a user study combining biometric data collection with usability questions. Using pattern recognition techniques, we built a classifier to recognize unique biometric gesture characteristics of an individual. We achieved a 90% accuracy rate with single gestures, and saw significant improvement when multiple gestures were performed in sequence. We found user ratings of a gestures desirable characteristics (ease, pleasure, excitement) correlated with a gestures actual biometric recognition ratethat is to say, user ratings aligned well with gestural security, in contrast to typical text-based passwords. Based on these results, we conclude that multi-touch gestures show great promise as an authentication mechanism.

Author Keywords
Multi-touch interfaces; multi-touch gestures; behavior biometric; authentication; password.

ACM Classification Keywords
H.5.2 [Information Interfaces and Presentation]: User Interfaces - Interaction styles;

General Terms
Human Factors, Design.

INTRODUCTION

With the growing popularity of mobile computing devices, and their use for activities such as banking and other transactions that require security, protecting user credentials on mobile devices is becoming increasingly important. Current applications typically maintain the privacy of users' sensitive data by authenticating the user at every login. Most mobile devices today make use of traditional text-based password schemes in order to authenticate a user. However, users have been known to choose weak passwords [15]. This is especially true with touch devices that are rapidly becoming ubiquitous. Findlater et al [12] have shown that the speed of typing on flash glass is 31% slower than a physical keyboard. This typically results in a shorter password chosen by users to shorten their log-in time.

The development of multi-touch technology opens up avenues for new authentication techniques that go beyond text passwords. One example of this is the touch-based password scheme called "Pattern Lock" implemented in the Android OS [21]. The password here is simply the pattern or sequence of dots connected by lines which a user must draw in order to gain access to the system. However, this method has many limitations. First, the password created has low entropy [1]. Second, it is shown to be vulnerable to disclosure based on the traces left on the screen by finger oils [2]. Third, it does not provide protection against shoulder surfing attacks since the password does not contain any personal traits of the user [18, 24]. Finally, Pattern Lock does not exploit the full capabilities of the newer multi-touch interfaces emerging in tablets and touch pads where one can use multiple fingertips to interact with the device [23].

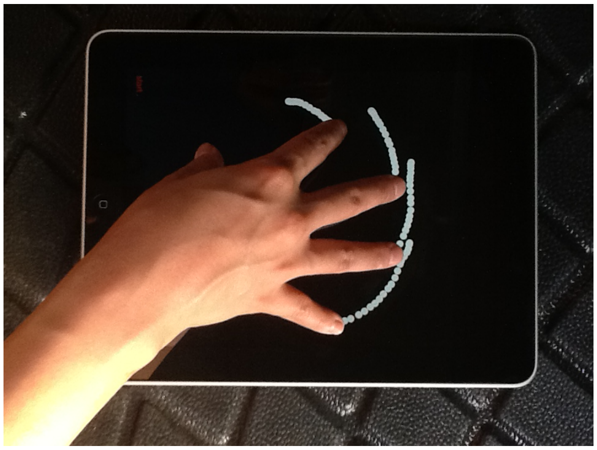


Figure 1: Example of a multi-touch gesture with sufficient biometric characteristics to allow for authentication.

Given the increasing prevalence of multi-touch technology, our aim is to develop a new user authentication system that does not have the limitations of text passwords and Pattern-Lock-like mechanisms as described above. The system we propose is based on multi-touch gestures and can be seen as an instance of a behavioral-biometric-based authentication technique. It is not susceptible to shoulder surfing or finger oil attacks and potentially provides significantly large entropy. Figure 1 is an example of the sort of multi-touch gesture that we have in mind, using our iPad test application. The user performs the gesture with all five fingers at once, and biometrics are drawn from the hand's geometry as well as the dynamics of the gesture itself.

Thus far, users have readily accepted multi-touch gestures in the interface, and much has been made of the accessibility of this mode of interaction to a broad user public [22, 26]. And although there has traditionally been some public suspicion and resistance of biometric systems, not all biometric systems raise the same degree of concern. Biometric systems can be divided into two main categories–physiological and behavior-based. Behavior-based biometric systems, such as online signature verification, are typically more acceptable to users [13]. This gives us reason to hope that a multi-touch gesture-based authentication system would prove to be both usable and acceptable.

To test our idea, we first developed a multi-touch authentication technique, then implemented a simple iPad application that allowed us to conduct a user study of the viability of the approach. We developed a comprehensive set of multi-touch gestures, working from characteristics of five-finger movement of the hand, that served as candidate gestures for our method.

We then conducted a user study, with the following questions in mind: a) whether biometric data obtained from gestures (positioning and movement dynamics inherent to an individual's hand) is sufficient and reliable enough to authenticate specific users and b) whether the gestures would be acceptable and enjoyable for end users as an authentication method. The goal was to find a set of gestures that met both criteria. Pretesting of the prototype suggested that it would be possible to achieve this combination.

RELATED WORK

Text passwords have been known to impose a cognitive burden on users that results in selection of weak passwords [24, 8]. In 1996, Blonder first proposed graphical passwords to tackle this problem based on a memory study by Calkins [6] that showed human memory for visual words is stronger than for pronounced words. This was later improved by Passpoints [24] and Cue Click Points [7]. Passfaces is another instance of a visual memory based authentication scheme where users are asked to repeatedly pick faces out of those presented [3]. Draw-a-Secret is a graphical password where the secret is a simple picture drawn on a grid [10]. In 2010, Citty et al [16] proposed a touch-screen authentication scheme similar to Passpoints that requires users to sequentially tap on pre-selected images to input their password.

However, all of the above schemes are susceptible to a "shoulder surfing attack" as they can be potentially observed by an attacker [18]. There have been many alternative approaches proposed to tackle this problem. In 2004, Roth et al [19] proposed a PIN-based challenge response approach. To enter one digit, the user repeatedly chooses the color of the focus digit shown on the screen (either black or white). Wiedenbeck et al [25] have proposed a graphical challenge response scheme. Here, given a convex hull generated by the preselected icons, the user clicks on any icon that appears inside that convex hull and the process is repeated multiple times. Recently, Kim et al [18] have proposed a pressure-based authentication scheme to reduce the visibility of the secret to an attacker. The idea is to blind an attacker by placing fingertips simultaneously in different zones. The user then communicates with the device by increasing the pressure on the fingertip located in a specific zone to select an object.

Another approach to counter shoulder surfing is not to rely completely on a shared secret (i.e. knowledge-based scheme or "what you know" scheme) but use a behavior component as well ("what you are"). One way to achieve this is by using biometric technology. In a biometric authentication system, a personal trait is used to verify a user. In order to increase the level of security, biometrics can be combined with any other authentication system to get multi-factor authentication. Several biometric traits have been studied including physiological ones such as retina, iris, fingerprint, face, vein and palm, and behavioral ones such as dynamic signatures, voice, key-stroke, and gait. Our approach–using the touch screen as a biometric sensor to capture user traits–has not been previously explored. We do know from prior research, though, that biometric data can be gleaned from both hand geometry [14], and from the movement of the hand [11, 17].

DEFINING A SET OF GESTURAL POSSIBILITIES

There are existing patented and open source gesture libraries that multi-touch developers draw upon, such as the iPhone 3G multi-touch gesture dictionary [5] and the Gesture Works open source gesture library [4]. These frameworks are not targeted towards the use context we have in mind, namely, multi-touch gestures that could serve as biometric keys for authentication. This is due to the fact that most of the gestures in these libraries use only two fingers whereas we need the use all five fingers to get maximal data from the hand geometry and muscle behavior of an individual. This led us to create our own gestural taxonomy based upon movement of the two major components of the hand, the palm and the fingertips.

PALM MOVEMENT

Palm movement is defined as whether the hand itself needs to move during the gesture, as opposed to just the finger tips. Some gestures place the users's hand in one static position for the entire gesture, whereas other gestures require the hand to traverse or rotate while executing the gesture. Thus, we can divide gestures into two classes for palm movement:

1. Static palm position: Defined as the gesture where the palm or hand position remains static while performing the gesture. In other words, only the fingertips are moving without changing the position of the hand. Examples of this type include pinch or zoom gesture.

2. Dynamic palm position: The center of the hand is moving while performing the gesture. For example, a Drag or Swipe.

FINGERTIP MOVEMENT

Most of the distinguishing features of a multi-touch gesture derive from movement of the fingertips. We divide fingertip movement into four categories.

1. Parallel: All fingertips are moving in the same direction during the gesture. For example, a five-finger swipe, in which all five fingers move from left to right on the screen.

2. Closed: All fingertips are moving inward toward the center of the hand. For example, a pinch gesture.

3. Opened: All fingertips are moving outward from the center of the hand. For example, a reverse pinch gesture.

4. Circular: All fingertips are rotating around the center of the hand. For example, a clockwise or counterclockwise rotation.

FURTHER FINGERTIP DYNAMICS

Sometimes the fingertips are not moving all at once in a gesture–there may be one or more fingertips resting in a fixed position on the screen. This can help to stabilize the gesture for the user. So we developed one additional classification in our taxonomy.

1. Full Fingertip: All fingertips are moving in the gesture.

2. Partial Fingertip: Some fingertips moving during the gesture, others resting in a static position on the screen.

These three classifications allowed us to define a comprehensive set of authentication gesture possibilities. Below is the list of 22 gestures that we studied (we use the indicated abbreviations in the rest of the text–see Figure 2 for an illustration of some sample gestures):

Close: All five fingers move toward the palm's center, in a closing motion.

FTC: Thumb is fixed, and the other fingers move toward the palm's center in a closing motion.

FPC: Pinky is fixed, other fingers move toward the palm's center in a closing motion.

Open: All five fingers move away from palm's center, in an opening motion.

FTO: Thumb is fixed, and the other fingers move away from palm's center in an opening motion.

FPO: Pinky is fixed, other fingers move away from palm's center in an opening motion.

CW: All fingertips rotate in a clockwise direction.

FTCW: Thumb is fixed, other fingertips rotate around it in a clockwise direction.

CCW: All fingertips rotate in a counter-clockwise direction.

FTCCW: Thumb is fixed, other fingertips rotate around it in a counter-clockwise direction.

FPCCW: Pinky is fixed, other fingertips rotate around it in a counter-clockwise direction.

Drag: All fingers move in parallel from top to bottom of screen.

DDC: The dynamic (moving from top to bottom) gesture performing a closing motion with all fingertips.

FTP: Thumb is fixed, other fingertips move in parallel from top to bottom of screen.

FPP: Pinky is fixed, other fingertips move in parallel from top to bottom of screen.

FBD: Pinky and thumb are both fixed; other fingertips move in parallel from top to bottom of screen.

Swipe: All fingers move in parallel from left to right of screen.

Flick: Quick top-left to bottom-right parallel movement of all fingertips.

FBSA: The static gesture performing parallel(⟩ shape) with fixed thumb and pinky

FBSB: The static gesture performing parallel(⟨ shape) with fixed thumb and pinky

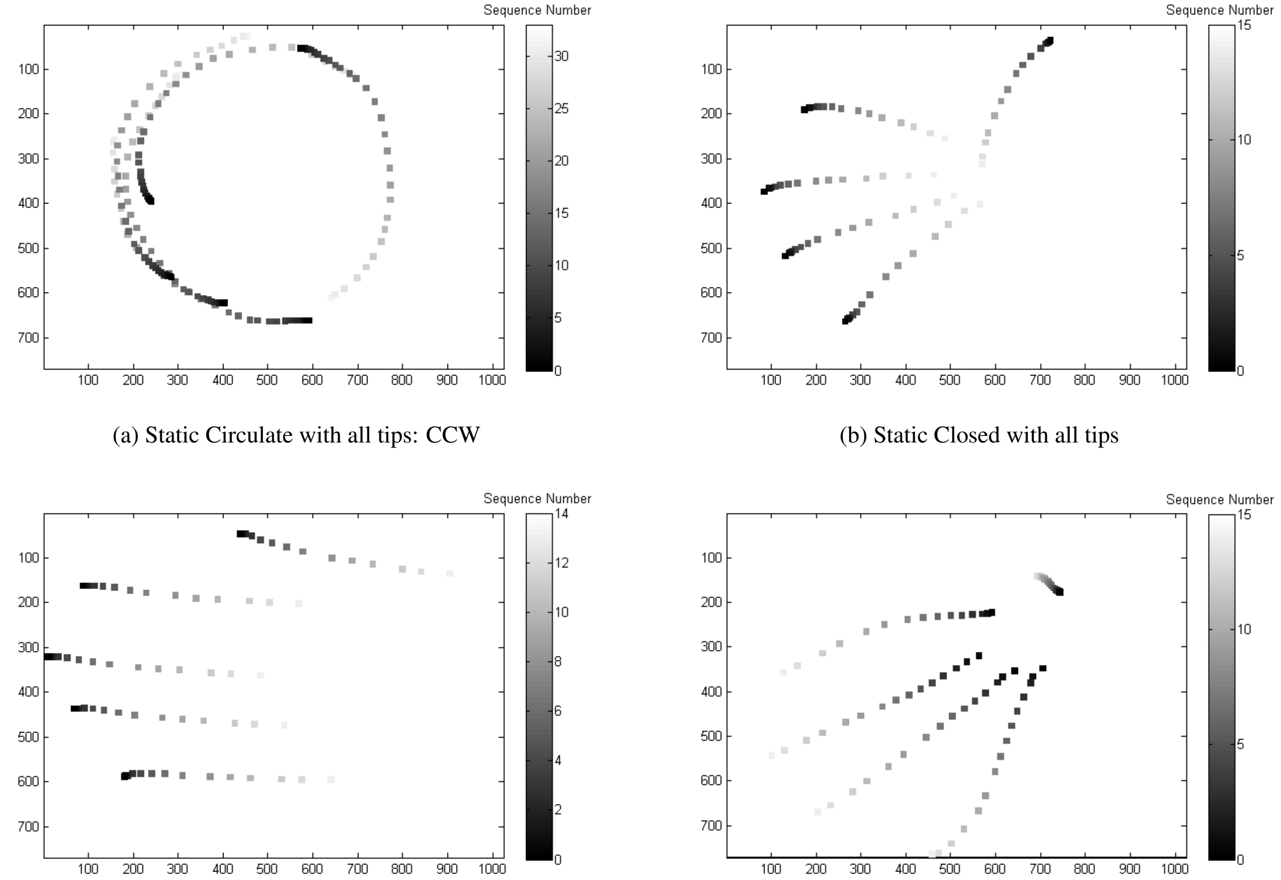
User Defined: All five fingertips move as the person pretends to sign his/her signature on the screen.

DUO: The dynamic(moving from bottom to top) gesture performing a opening motion with all fingertips.

We tested out all the above gestures in our study, to find those gestures that were both most robust in terms of biometrics, and also, the most appealing to users.

DEVELOPING A GESTURE AUTHENTICATION TECHNIQUE

In a biometric verification or authentication system, the identity of the user is given to the system along with a proof of identity (the biometric). Correctness of the proof of identity is then evaluated by the system. After that, the answer, either accept or reject the user, is given based on the evaluation result. In order to verify the proof, the system needs to have a prior knowledge about it. To achieve this, there are generally two stages in a verification system: enrollment stage and verification stage. The purpose of the enrollment stage is to register the user's data in the system by acquiring and storing biometric templates corresponding to the user. Since biometric data is unlikely to be repeated (for example two iris scans of the same user will never be the same due to acquisition noise and variation of environment in which they are acquired), one sample is not good enough to represent an individual's biometric. In the verification stage, the in-



(a) Static Circulate with all tips: CCW

(b) Static Closed with all tips

(c) Dynamic Parallel with all tips

(d) Static Opened with fixed thumb

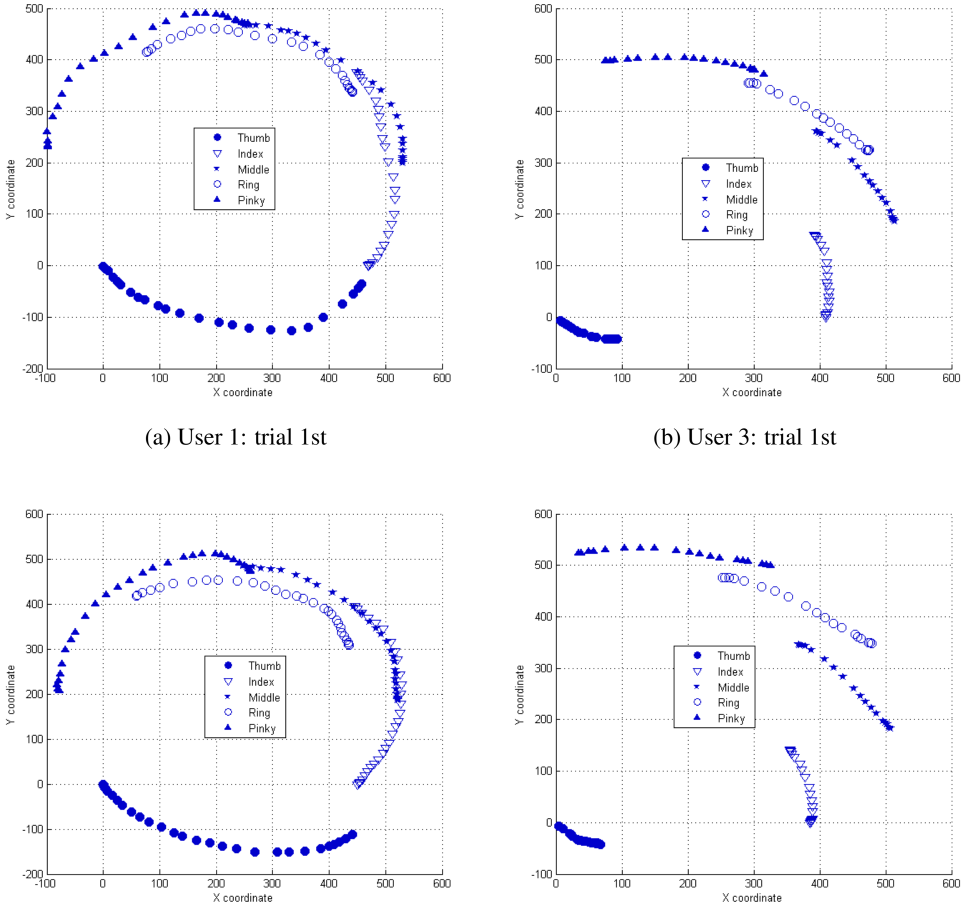
Figure 2: Examples of the gestures categorized by the movement characteristics as mentioned

put biometric instance is compared with the stored biometric templates of the claimed identity in order to authenticate a user.

In the rest of this subsection we summarize the biometric verification algorithm for multi-touch gestures we developed, implemented and tested in our study. The verification process begins with the user performing a multi-touch gesture. All x-y coordinates, time-stamps and labels of the resulting 5 touch sequences from 5 fingertips are sequentially captured by the device. The given labels of touch points are not related with the actual fingertips. In other words, the touch generated from the thumb can appear in any label from 1 to 5. To verify the multi-touch gesture input by the user by comparing with the stored templates of the user, all the touch points need to be correctly labeled and ordered in a consistent manner. Next, the fingertip trails or touch sequences need to be normalized to maintain the invariants of location, rotation and path. Then, a Dynamic Time Warping algorithm is used to compute the distance between each of the normalized stored templates and the normalized input multi-touch gesture. Finally, a dissimilarity score is derived from the distances obtained and a decision is then made by comparing the dissimilarity score with a threshold in order to accept or reject a user. In the rest of this section we provide some additional details about each of these steps. A more detailed description of the algorithm appears in a companion paper[not to be cited due to the blind review].

Matching Touch Sequences to Specific Fingers

To correctly compare any two multi-touch sequences (each touch sequence has 5 touch point trails), they need to be stored in a consistent order. Hence the first step is to re-order the touch sequences into a canonical form. The standard order employed was that the touches generate by Thumb, Index, Middle, Ring and Pinky respectively labeled 1^{st} to 5^{th}. To achieve this one has to match a touch sequence to the corresponding finger. This is not an easy task as the acquisition process may capture points in an arbitrary order depending on which fingertips made contact with the touch surface first. To correctly match touch sequences with fingers we use known natural characteristics of human hand geometry. First, we construct a simple polygon that connects the starting points of each touch sequence. Then, the thumb position is identified based on pairwise distances between polygon vertices.



(a) User 1: trial 1st

(b) User 3: trial 1st

(c) User 1: trial 2nd

(d) User 3: trial 4th

Figure 3: Examples of the CW gestures from 3 different users.

Finally, we identify and label touch sequences corresponding to each of the remaining fingers based on a circular order starting from the thumb position.

Gesture Normalization

Location and Orientation Invariance: The position of user touch sequences can be anywhere and in any orientation on the screen and differ from one instance to another. Hence location and orientation of the touch sequences need to be normalized before making comparisons. In our work, all the touch sequences were normalized based on the thumb and index's fingertips of the touch sequence generated when the 5 fingertips first contact the screen. All the gestures are normalized such that the thumb's tip in the first template is at the origin and the index finger's tip is at 0 degree of the plane. Examples of the same gesture from 3 different users after location and orientation normalization are shown in Figure 3. For the same user, the gestures are similar whereas they look different from the other users' gestures.

Length Invariance: The actual length of the fingertip trails can be different each time even when performed by the same user. However, the relative length of each fingertip trail is another useful characteristic of the user's gesture. In other words, some might perform the gesture in such a way that has an equal length for all the tips' trails. Others might perform in different ways. Hence the path length of the gestures are normalized as follows before making comparisons between input and stored gesture templates.

$$x'''(i,j) = \frac{x''(i,j) - \min_j(x''(1,1))}{\max_j(x''(1,1)) - \min_j(x''(1,1))}$$

$$y'''(i,j) = \frac{y''(i,j) - \min_j(y''(1,1))}{\max_j(y''(1,1)) - \min_j(y''(1,1))}$$

Dynamic Time Warping Algorithm

The distance between two time-series signals with the different lengths is defined as the sum of the distance at the optimal non-linear path such that the distance or matching cost sum is minimized. Firstly, an input gesture is formatted as the time series of touch sequences; $Gesture\,(t) = [Touch_1, Touch_2,..., Touch_n]$ where n is the number of the touches sequence of the gesture. $Touch_i$ is the vector of x-y coordinates of the touches in the i^{th} sequence; $Touch_i = [x_1, y_1, x_2, y_2, ..., x_5, y_5]$. Dynamic programming can be used to implement the optimal path searching algorithm. Euclidean distance is calculated as a matching cost between 2 touch sequences. The sum of the Euclidean distances is then defined as the distance between 2 different gestures.

Dissimilarity Score

The decision of whether the biometric is coming from the claimed user or not depends on the similarity of the input biometric to the stored template. In other words, if the dissimilarity score of the input biometric compared to the template is lower than a threshold, the input biometric is verified. Otherwise, the system will reject the user. To calculate the dissimilarity score between the registered user's templates and the input, all distances between the coming gesture and templates are used to calculate the dissimilarity score along with the distances between all the stored templates themselves. The idea is to normalize the inter-user variation with the intra-user variation and use as a dissimilarity score as suggested in [17].

We implemented and tested our classifier on the data set from our user study described in the next section. We achieved accuracy at the level of 90% accuracy for single gesture. It can be significantly improved with multiple gesture authentication. Results are discussed in detail in the Analysis of Biometric Data section.

USER STUDY

We conducted a study that combined a trial of our technique in terms of robustness of authentication results, with eliciting user feedback on the individual gestures, and on the general practice of using multi-touch gesture for authentication. We recruited 34 participants. 24 were male, 30 were right-handed, 28 had some multi-touch device experience, while only 6 had prior experience with the iPad. Age ranged from 15 to 50: 18 participants were 15-19, 10 were 20-25, 3 were 26-30, 2 were 31-40 and 1 was 41-50.

We created an application on the iPad, using version 3.2 of iOS, which has multi-touch capability to track up to 5 points at a time. The multi-touch screen resolution was $1024 * 768$. Data provided by the device at each point were x and y coordinates of the touch point's trajectory, time stamp, touch order (of the different fingertips), touch sequence, and touch type. The number of touch events created were in the range of 20-30 per second. As a visualization aid, the application provides simple visual traces of the user's fingertip movement during each gesture (see figure 1).

In each session, we first explained the purpose of the study to participants, and solicited their informed consent to proceed. Next the participant filled out a brief pre-survey with demographic questions, and then we moved on to the gesture trials. Each person was taken through all 22 gestures (in a randomized order), however, they could skip any gesture that they did not feel comfortable performing (all gestures had at least 26 participants who performed them–see Table 1). The participant practiced a given gesture a few times, and once comfortable with that gesture, was asked to perform it 10 times, with the system recording their touches during these 10 trials. The person answered a few questions about ease of use and how they felt after trying the gesture, before moving on to the next gesture. For soliciting emotional response, we used a technique called Emocard [9], a pictogram-based approach to eliciting emotional feedback about products that can be analyzed in terms of valence and arousal, two commonly used dimensions of affective response [20]. After completing the entire gesture set, the person answered a final set of questions about the overall experience, before leaving.

Analysis of Biometric Data

We used Equal Error Rate (EER) to measure accuracy. This is the rate at which False Acceptace Rate (FAR) and False Rejection Rate (FRR) are equal. We use this measure because typically the number of genuine cases in a verification system are much smaller than the number of forgery cases.

To test each gesture, we treated the first 5 samples of each gesture from each user as the template for that user in the enrollment process. The last 5 samples were used as the test for a genuine case. Samples of the same gesture from other users in the study were used to test as the forgeries of that gesture. For each gesture, we have at most $5*34 = 170$ cases for genuine and $10*34*33 = 11,220$ forgeries. This reflects the fact that some participants opted out of certain gestures because they were uncomfortable to perform.

FAR and FRR can be calculated using the following:

$$FAR = \frac{\sharp \text{ of verified forgery cases}}{\sharp \text{ of forgery cases}} \tag{1}$$

$$FRR = \frac{\sharp \text{ of rejected genuine cases}}{\sharp \text{ of genuine cases}} \tag{2}$$

To calculate EER, first the dissimilarity scores for all the test examples are calculated. The threshold value will then be varied. At the particular threshold value, the corresponding FAR and FRR are derived. All pairs of (FAR,FRR) are used to plot Receiver Operating Characteristic or ROC curve. The corresponding value of the point at which FAR and FRR are equal is an EER.

EER for all the gestures is shown in Table 1 (Figure 4(a) provides a graphical version of these results). Individual gestures achieved an average level of 10% EER. 7 out of 22 gestures achieved an EER of lower than 10%. 6 of them achieved an EER of 10-15% and 9 of them achieved an EER of 15%.

To find out whether using multiple gestures would improve the system's performance, we combined scores of 2 different gestures from the same user in the same order and evaluated the EER of the combined gestures. The results in Table 2 give examples of combinations to show that different gestures can

Gesture	EER	Threshold	Number of users
Close	9.56	10.01	34
FTC	10.36	9.34	34
FPC	15.67	9.29	31
Open	18.9	9.02	33
FTO	17.81	10.00	32
FPO	17.43	8.75	30
CW	9.42	9.56	33
FTCW	12.44	9.53	33
CCW	7.21	9.86	33
FTCCW	6.60	10.02	30
FPCCW	16.60	8.78	28
Drag	10.66	8.39	33
DDC	9.40	9.63	31
FTP	7.89	8.93	27
FPP	13.25	9.08	30
FBD	15.18	8.62	26
Swipe	15.9	8.50	30
Flick	14.9	10.12	30
FBSA	16.10	8.28	30
FBSB	10.91	9.37	26
User Defined	2.88	13.93	30
DUO	15.97	9.84	28

Table 1: Equal Error Rate performance for each gesture along with the derived threshold for dissimilarity score.

be used to provide complementary biometric data and raise accuracy levels to a range of 2-5% EER.

Analysis of User Experience

We wanted to find gestures that not only provided strong biometric authentication support, but that were also easy to use and that created positive feelings in users. The security of any authentication approach depends upon the user response, and as was mentioned earlier in the paper, text-password methods suffer from a lack of such qualities for users. We analyzed results from the questions that we asked participants about each gesture, and about multi-touch authentication in general, to understand the user experience of this authentication method. We also looked at how participant answers about the user experience of particular gestures related to the biometric strength of those gestures.

At the end of the study, we asked whether multi-touch gestures would be easy to memorize, which type of password they would prefer (gesture or text) and why, which they thought would be faster, and whether they thought gesture passwords would get easier with practice. We collected comments about the general approach as well. All 29 participants thought that gestures would be faster than text passwords, and the 25 out of 29 participants said they would prefer this method, 26 out of 28 participants said that it would be easy to memorize, and 27 out of 29 participants said that it would get even easier with practice. User comments about why they would prefer this method included: 'No typing and easy to perform', 'It is faster, simpler and cooler' and 'I have too many passwords to memorize.' People who preferred text passwords reported that this was because they were used to the method.

Gesture 1	Gesture 2	EER
Closed	CCW	3.88
Closed	FTCCW	3.7
Closed	CW	4.56
CW	CCW	2.93
CW	FTCCW	2.58
CCW	FTCCW	3.45

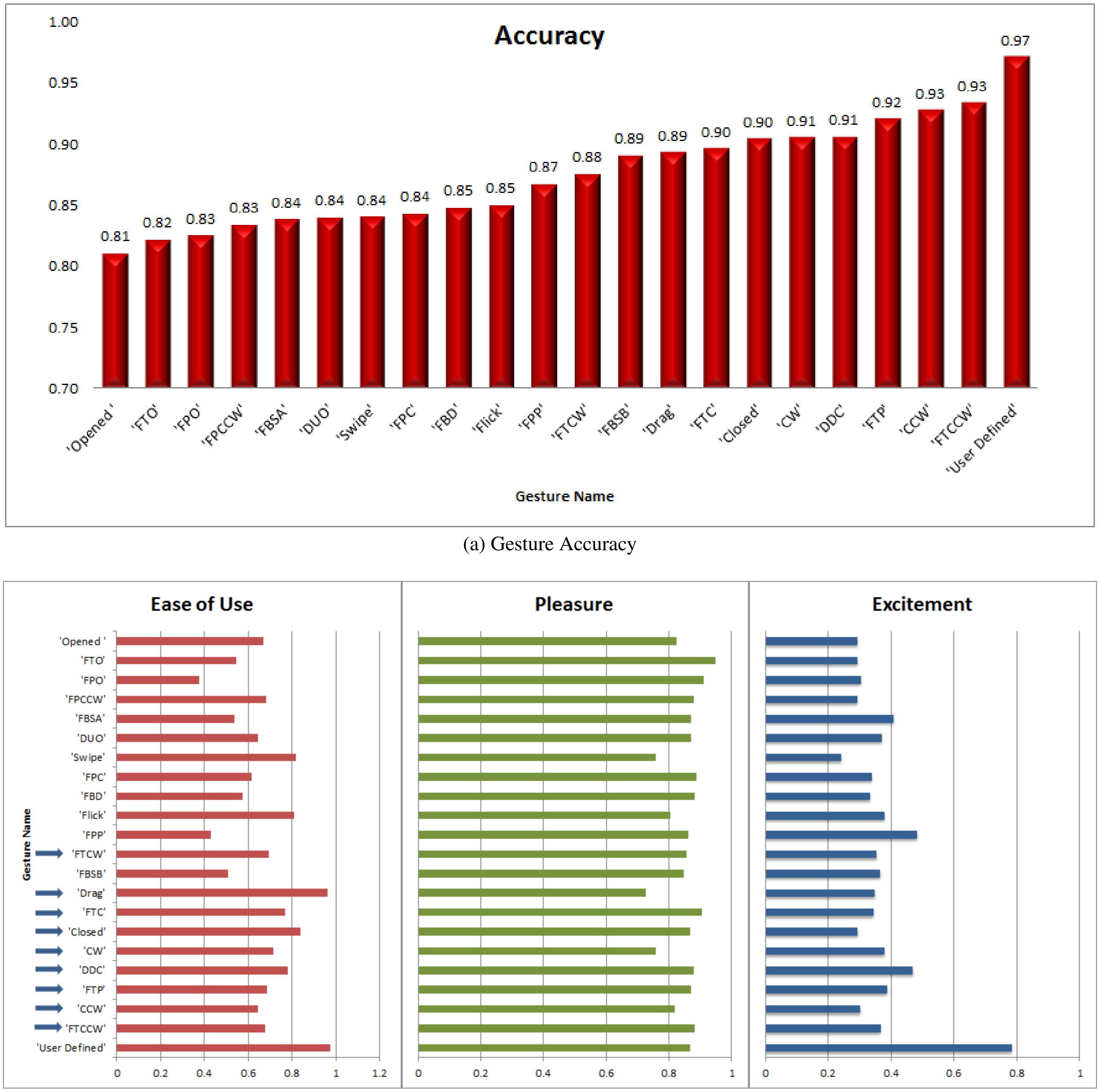
Table 2: Equal Error Rate performance of multiple gestures along with the derived threshold for dissimilarity score.

Figure 4 shows user ratings of each gesture on ease of use, pleasure, and excitement, with that gesture's accuracy rating also included for reference. Participant's Emocard [9] responses gave us scores for pleasure and excitement ranging from 1 to 3. We also asked participants how hard/easy the gesture was (scaled from 1 to 5), and whether they thought they would use this gesture for authentication/log-in. We collected comments about each gesture from participants, to support these numeric ratings. We used the combination of the gesture's user ratings and accuracy ratings to identify the most promising gestures for this kind of authentication. Given these results, candidate gestures that optimize for both authentication accuracy and user experience: Close, Clockwise, Counter Clockwise, Drag, Drag Down Close, Fixed Thumb Parallel, Fixed Thumb Close, Fixed Thumb Clockwise, and Fixed Thumb Counter Clockwise.

In terms of static gesture type preference ratings, 13 preferred closing, 11 preferred circular and only 5 of them preferred opening gesture. In terms of the set of fingertips, the majority preferred to perform with all tips and followed by fix thumb and fix pinky, respectively. Some users remarked that opening gestures began with fingernails on the screen, and they worried that this could damage the screen, whereas closing gestures began with fingertips firmly placed on the screen. Gestures that made use of all fingertips were most highly rated, in contrast to gestures that involved fixed fingertips. Participants did like the fixed thumb rotation gestures, but in general, users did not like the fixed pinky gestures.

Figure 5a shows the relationship between EER and user experience ratings of each gesture. Positive ratings showed a strong linear relationship with system accuracy. In other words, gestures that users liked better were also more secure from a biometric point of view.

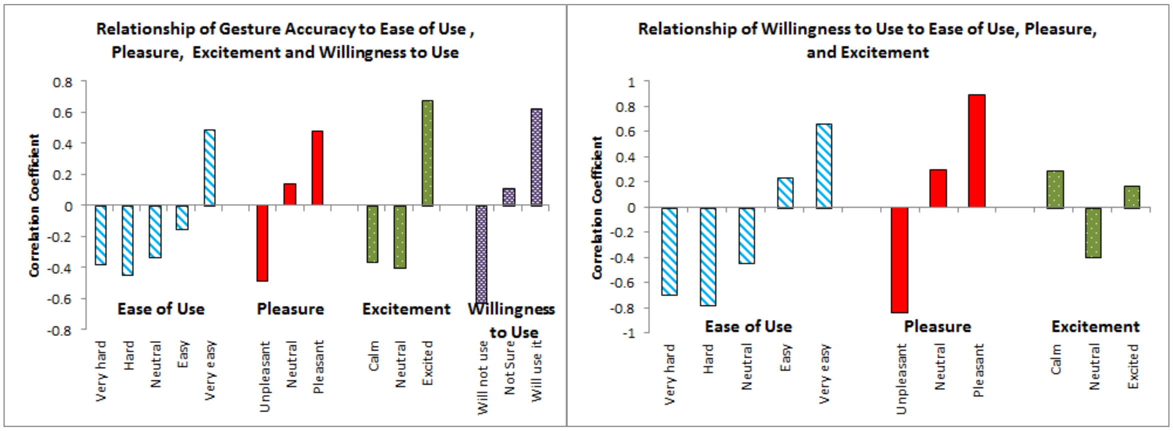
Figure 5b shows that participants' reports of which gestures they are most willing to use correlate with ratings of those gestures as exciting, easy, and pleasant. This relationship leads us to conclude that, unlike with text-based passwords, ease of use and preference ratings seem to correlate with those gestures that are also most biometrically secure. This is a fan-



(a) Gesture Accuracy

(b) Self-reported user experience

Figure 4: The percentage of self-reported user experience and accuracy for each gesture. → indicate the candidate gestures.



(a) Biometric Accuracy (b) User Experience

Figure 5: The correlation coefficients a) Associated with gesture accuracy and b) Associated with willingness to use.

User Experience	FAR	FRR	FAR+FRR
Excitement (1 to 3)	0.0563	-0.0202	0.027
Pleasure (1 to 3)	0.0848	-0.0726	0.027
Ease of Use (1 to 5)	0.1288	0.0872	0.1657

Table 3: Correlation Coefficient of performance associated with self-report of user experience.

tastic result from the point of view of achieving better security results for a greater numbers of users.

To examine the relationship between accuracy and user rating more closely, we used the derived threshold value of each gesture to evaluate the FAR and FRR of different gestures corresponding to different users. In total we have 658 instances, and each instance has 8 attributes which are the user's ID, the gesture's ID, FAR, FRR, excitement level, pleasant level, easiness level and willingness to use level.

Table 3 shows that rating of ease of use is positively linearly related to the level of FAR, with a 95% confidence level. The relationship is stronger when considering FAR + FFR, which is a general accuracy term. Self-reported pleasure is also positively linearly related to the level of FAR + FRR. These results imply that the more pleasant and easier the gesture, the more accurately users are likely to perform the gestures. In terms of accuracy, the static, open gestures are low, and it can be seen that user ratings of these gestures were also low. Users seemed to like fixed pinky gestures the least, and they also scored low in terms of accuracy. Interestingly, sometimes having the thumb fixed seemed to lead to stabilization of the gesture, such as in the CCW gesture. Some users, especially those with shorter fingers, mentioned this in their comments about this gesture, as well.

CONCLUSION

In this paper we have presented a novel approach to authentication, which makes use of biometric information that can be gleaned from multi-touch gestures. We outlined a gestural possibility space, and created a generic gesture classifier and a simple iPad application to test out the classifier. We then conducted a user study of the gestures we defined, testing out both authentication accuracy and participants' ratings of the user experience. We were able to achieve system performance of 10% EER on average for single gestures, and 5% EER on average for double gestures. We discovered that user preferences seem to have a linear relationship to system performance (not the case for text-based password schemes). We also showed that users rated the method highly and seemed very open to adopting it for everyday use. We believe this method shows great promise as a technique for improving the everyday experience of authentication on multi-touch devices, and also for raising the level of security of user data.

We are working on ways to raise the accuracy level even higher. For example we improved accuracy 5% on average by implementing a translation factor optimization to minimize gesture distance. If we can get access to more touch attributes such as pressure or touch surface area, we can further improve accuracy. We are also exploring ways to combine this method with other biometric information, such as face recognition using a device's on-board camera.

It is interesting to note from the data, that the one gesture which created a strong self-report of excitement, was performing a 'user defined' gesture (participants pretended to sign their signature on the screen with all five fingers). The research team theorizes that one potential reason for this excitement was the opportunity to make use of something highly personal, and we are currently exploring ways to adapt our method that make use of personalization of the gestures and the gesture context as well.

ACKNOWLEDGMENTS

Thanks to Sharanya Ravichandran and Najee Gardner for their help in conducting pretests of this user study.

REFERENCES

1. http://beust.com/weblog2/archives/000497.html.
2. http://techcrunch.com/2008/10/12/androids-login-is-cool-but-is-it-secure/.
3. http://www.passfaces.com/pfphelp/logon.htm.
4. http://gestureworks.com/features/open-source-gestures/.
5. Apple. Multi-touch gesture dictionary.
6. Calkins, M. W. Short studies in memory and in association from the wellesly college psychological laboratory. In *Psychological Review*, Vol 5(5), ACM (New York, NY, USA, Sep 1898), 2453–2462.
7. Chiasson, S., van Oorschot, P., and Biddle, R. Graphical password authentication using cued click points. In *Computer Security ESORICS 2007*, vol. 4734 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg (2007).
8. Denning, T., Bowers, K., van Dijk, M., and Juels, A. Exploring implicit memory for painless password recovery. In *Proceedings of the 2011 annual conference on Human factors in computing systems*, CHI '11, ACM (New York, NY, USA, 2011), 2615–2618.
9. Desmet, P. M. A., Overbeeke, C. J., and Tax, S. J. E. T. Designing products with added emotional value: development and application of an approach for research through design. In *The Design Journal*, vol. 4 (2001), 32–47.
10. Dunphy, P., and Yan, J. Do background images improve "draw a secret" graphical passwords? In *Proceedings of the 14th ACM conference on Computer and communications security*, CCS '07, ACM (New York, NY, USA, 2007), 36–47.
11. Faundez-Zanuy, M. On-line signature recognition based on vq-dtw. In *Pattern Recogn.*, Elsevier Science Inc. (New York, NY, USA, March 2007), 981–992.
12. Findlater, L., Wobbrock, J. O., and Wigdor, D. Typing on flat glass: examining ten-finger expert typing patterns on touch surfaces. In *Proceedings of the 2011 annual conference on Human factors in computing systems*, CHI '11, ACM (New York, NY, USA, 2011), 2453–2462.
13. Gamboa, H., and Fred, A. A behavioral biometric system based on human-computer interaction. In *SPIE 5404 - Biometric Technology for Human Identification*, A. K. Jain and N. K. Ratha, Eds., 381–392.
14. Jain, A., Ross, A., and Pankanti, S. A prototype hand geometry-based verification system. In *2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication, Washington D.C.* (1999).
15. Jain, A., Ross, A., and Pankanti, S. Biometrics: a tool for information security. In *Information Forensics and Security, IEEE Transactions on*, vol. 1 (june 2006), 125 – 143.
16. Jonathan Citty, D. R. H. Tapi: Touch-screen authentication using partitioned images. In *ELON UNIVERSITY TECHNICAL REPORT 2010-1* (2010), 1–6.
17. Kholmatov, A., and Yanikoglu, B. Biometric authentication using online signatures. In *Proc. ISCIS, Springer LNCS-3280 (2004) 373380*, Springer-Verlag (2004), 373–380.
18. Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J., Nicholson, J., and Olivier, P. Multi-touch authentication on tabletops. In *Proceedings of the 28th international conference on Human factors in computing systems*, CHI '10, ACM (New York, NY, USA, 2010), 1093–1102.
19. Roth, V., Richter, K., and Freidinger, R. A pin-entry method resilient against shoulder surfing. In *Proceedings of the 11th ACM conference on Computer and communications security*, CCS '04, ACM (New York, NY, USA, 2004), 236–245.
20. Russell, J. A circumplex model of affect. In *Journal of Personality and Social Psychology*, vol. 39 (1980), 1161 – 1178.
21. Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., and Glezer, C. Google android: A comprehensive security assessment. In *Security Privacy, IEEE*, no. 2 in 8 (march-april 2010), 35 –44.
22. Stöß el, C. Familiarity as a factor in designing finger gestures for elderly users. In *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '09, ACM (New York, NY, USA, 2009), 78:1–78:2.
23. Wang, F., and Ren, X. Empirical evaluation for finger input properties in multi-touch interaction. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, ACM (New York, NY, USA, 2009), 1063–1072.
24. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., and Memon, N. Passpoints: Design and longitudinal evaluation of a graphical password system. In *International Journal of Human-Computer Studies*, no. 1-2 (2005), 102 – 127.
25. Wiedenbeck, S., Waters, J., Sobrado, L., and Birget, J.-C. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces*, AVI '06, ACM (New York, NY, USA, 2006), 177–184.
26. Wigdor, D., and Wixon, D. *Brave NUI World: Designing Natural User Interfaces for Touch and Gesture*, 1 ed. Morgan Kaufmann, Apr. 2011.