Comparison of PIN- and Pattern-based Behavioral Biometric Authentication on Mobile Devices

Yanyan Li*, Junshuang Yang*, Mengjun Xie*, Dylan Carlson†, Han Gil Jang‡, Jiang Bian§
*University of Arkansas at Little Rock, Email: {yxli5, jxyang2, mxxie}@ualr.edu
†Lake Superior State University, Email: dcarlson10@lssu.edu
‡Washington and Lee University, Email: jangha15@mail.wlu.edu
§University of Florida, Email: bianjiang@ufl.edu

***Abstract*—Personal identification numbers (PIN) and unlock patterns are highly popular authentication mechanisms on smart mobile devices but they are not sufficiently secure. PIN or pattern mechanisms enhanced by additional, implicit behavioral biometric authentication can offer stronger authentication assurance while preserving usability, therefore becoming very attractive. Individual studies on PIN- and pattern-based behavioral biometric authentication on smartphones were conducted but their results cannot be directly compared. In this work, we present a comparison study on the authentication accuracy between PIN-based and pattern-based behavioral biometric authentication using both smartphone and tablet. We developed a uniform framework for both PIN-based and pattern-based schemes and used two representative methods—Histogram and DTW—for user verification. We recruited 15 users and collected behavioral biometric data for both simple and complex PINs and patterns. Our experimental results show that PIN-based and pattern-based behavioral biometric authentication schemes can achieve about the same level of accuracy but not all verification methods are equal. The Histogram method can achieve more consistent results and handle template aging better than the DTW method based on our results. Our findings are expected to shed light on the exploration and analysis of effective behavioral biometric verification methods and facilitate more comprehensive investigation on behavioral biometric authentication for mobile devices.**

***Index Terms*—behavioral biometrics, authentication, mobile devices.**

I. Introduction

Smart mobile devices especially smartphones and tablets have become ubiquitous. As those devices can carry a large amount of private and important data, it is critical to ensure the security of the information stored on them. Authentication stands in the first line of defense to prevent unauthorized accesses to the information on a mobile platform. User authentication on mobile devices, in general, consists of explicit approaches (e.g. [1]), implicit approaches (e.g. [2]), and hybrid approaches (e.g. [3]). There are a variety of explicit authentication methods available on mobile devices, e.g., personal identification number (PIN, often using four digits), draw pattern (or simply pattern), password, fingerprint, voice, and even face recognition, which can be roughly classified into biometrics based, token based, and knowledge based methods [4]. Among them, PIN and pattern authentication mechanisms are most popular as they are simple and easy to understand and apply.

Although being popular, PIN and pattern authentication approaches are vulnerable to a variety of attacks including shoulder surfing, a common attack in public settings, infamous smudge attack [5] in which finger traces left on touchscreen are exploited for extracting the secret, and more advanced attacks [1], [6]. According to [3] 41% of users showed concern about the security of using PIN. Moreover, average people tend to use simple (and therefore weak) PINs or patterns [1], [7]. A recent study reports that the 10 most popular PINs represent 15% of all 4-digit PINs [7]. Another study finds that the popular Android pattern unlocking mechanism is less secure than a 3-digit PIN [8]. Therefore, PINs or patterns alone may not be able to provide sufficient protection for the information stored on the device.

Implicit authentication mechanisms analyze specific time spans of behavioral cues like sensor data and usage patterns such as gait patterns, typing behavior, touch characteristics, file system access, or a combination of factors. Due to noticeable delays, many of those mechanisms are not suitable for direct and instant authentication but for continuous passive authentication (or called re-authentication) [9]. The hybrid authentication combines implicit verification with an explicit authentication challenge, which essentially turns the factor for implicit authentication into the second authentication factor.

Figure 1 shows an example of hybrid authentication that combines PIN/pattern authentication with implicit behavioral biometric verification. The user authentication process has two steps: a PIN/pattern verification step followed by a behavioral biometric verification step, and the second step is transparent to the user. If the unlock attempts have failed over the preset number of times in either the first step or the second step, the protection mechanism such as account disabling or system reset will be triggered. The threshold to trigger the protection mechanism in the first step can be different from that in the second step. For the ease of presentation, the same threshold is used for both steps in the figure.

PIN- and pattern-based behavioral biometric authentication has attracted strong research interests in that the schemes enhance the information protection on mobile devices with two-factor authentication while preserving almost the same user experience and usability. A pattern-based behavioral biometric authentication scheme [3] and a PIN-based scheme [7] have been extensively studied and their research results show that

978-1-5090-0073-9/15/$31.00 ©2015 IEEE

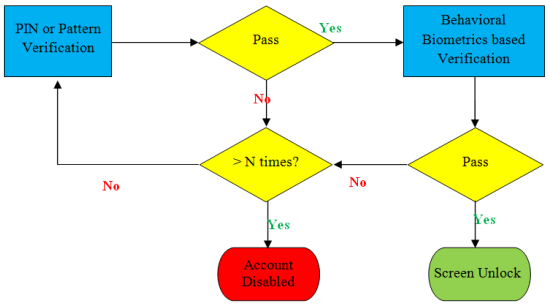


Fig. 1. An enhanced PIN/pattern authentication process with implicit behavioral biometric verification

both schemes have a high potential of being practically applied although the PIN-based scheme achieves much higher accuracy than the pattern-based scheme in their respective experiments. Given the popularity of PIN and pattern authentication and potentially high benefits of using behavioral biometrics, a natural research question is whether PIN-based behavioral biometric authentication is more accurate than pattern-based or vice versa. However, we cannot obtain an answer by directly comparing the results from previous individual studies as those two studies are very different in many aspects.

In this paper, we present our comparison study on the authentication accuracy between PIN-based and pattern-based behavioral biometric authentication on mobile devices. Our study is not a simple combination of repeating previous two studies [3], [7]. We have developed a uniform framework for both PIN-based and pattern-based behavioral biometric authentication schemes. We tested the schemes using both smartphone and tablet while only smartphones were used in the previous studies. We use two representative verification techniques that are applicable to both PIN- and pattern-based schemes for user verification. We design a simple form and a complex form for both PIN and pattern input. 15 volunteers were recruited to collect behavioral biometric data for those PINs and patterns in three different sessions. A smartphone was used in the first two sessions and a tablet was used in the last one.

New and interesting findings have been obtained from our experimental results. For example, we find that PIN-based and pattern-based behavioral biometric authentication schemes can achieve about the same level of accuracy and even a simple PIN or pattern can achieve quite high accuracy. We also find that not all verification methods are equal. The Histogram method can achieve more consistent results and handle template aging better than the DTW method based on our results. We believe our findings help shed light on the exploration and analysis of effective behavioral biometric verification methods.

The rest of this paper is organized as follows: Section II briefly describes behavioral biometrics and related work. Sections III and IV present the design and implementation of our study respectively. Section V details the evaluation including the method for data collection and the analysis of experimental results. Section VI concludes this paper.

II. Related Work

User authentication refers to the process in which a user submits her identity credential (often represented by paired username and password) to an information system and validates to the system that she is who she claims to be. In general, there are three types of authentication factors: something a user knows (e.g., a password), something a user has (e.g., a secure token), and something a user is (e.g., biometric characteristics). Passwords are the most common authentication mechanism. However, password-based authentication has many security issues [10], [11], [12].

In general, a biometric authentication system verifies a person based on either his/her physiological traits (e.g., fingerprint, face, iris, bioimpedance [13], etc.) or behavioral biometrics (e.g., finger or hand movements [14]). Thanks to rich sensing capabilities, both physiological and behavioral biometrics can be easily collected using today's smart mobile devices. While physiological traits can achieve high accuracy in user authentication, they are subjected to a variety of attacks [15] and also raise privacy concerns [16]. Moreover, accuracy of physiology-based mechanisms may be substantially degraded by environmental factors such as viewing angle, illumination, and background noise [17]. In contrast, behavioral biometrics appear less sensitive to ambient light or noise.

The popularity of mobile devices especially smartphones and tablets have attracted a great deal of research efforts to investigate how to effectively apply behavioral biometrics to mobile device authentication. Researchers have studied behavioral biometric features extracted from regular touch operations [18], [9], unlock pattern and PIN operations [3], [7], and multitouch gestures [19], [20], [21].

III. System Design

Our study focuses on accuracy comparison between PIN-based and pattern-based behavioral biometric authentication. We do not measure or compare consumption of CPU, memory, network, storage caused by the authentication. We develop a uniform framework for both PIN-based and pattern-based behavioral biometric authentication on touchscreen mobile devices. There are four important modules in the framework: data acquisition, feature extraction, template generation, and matching. In the data acquisition module, raw data are first collected from multiple sensors when a user enters a PIN or draws a pattern and they are then stored into a database that is either local or remote. In the feature extraction module, a set of features are obtained or derived from raw sensor data and fed into the template generation module. In that module, each sample of a PIN or pattern input is represented by a feature vector after applying certain transformation, and a template for a specific PIN or pattern for each user is generated from feature vectors derived from the user's training samples. The matching module takes user template (selected based on the claimed identity) and features extracted from a test sample and applies the matching algorithm to decide whether the test sample can be accepted as genuine.

There are two types of verification techniques that are commonly used in biometric authentication. They are function based techniques such as Dynamic Time Warping (DTW) and Hidden Markov Models (HMM) and feature based techniques that use descriptive features of the biometric. DTW has been widely used in various studies on behavior biometric authentication including [3]. We also include a feature based histogram technique (or simply Histogram) adapted from [22], which is shown effective and efficient for online signature verification. As PINs and patterns can be seen as special signatures drawn with a finger, the Histogram method should be applicable to the behavioral biometrics collected during PIN- or pattern-based user verification.

We developed an Android application for data acquisition, which is detailed in Section IV. The collected data are used for both DTW and Histogram methods. Participants were asked to repeatedly enter either a pattern or a PIN on the touchscreen of a smartphone or tablet to get a sample of behavioral biometric data. A sample begins when the user touches the screen to start either PIN or pattern authentication process and the data will be captured at every interval (10ms). In each sample, data of 10 raw features were recorded including x and y coordinates, pressure, size (the area of the finger tip), 3-axis acceleration (measured through the accelerometer), and 3-axis angular acceleration (measured through the gyroscope). All of this information was gathered using the same smartphone for the first two sessions and the same tablet for the third session. More information on data collection is given in Section V-A.

Let vectors $X = \{x_1, x_2, ..., x_n\}$, $Y = \{y_1, y_2, ..., y_n\}$, and $P = \{p_1, p_2, ..., p_n\}$ be the x, y coordinates and pressure attribute respectively, of a user input with length n sampled at times $T = \{t_1, t_2, ..., t_n\}$. Two more features—distance (d) and angle (θ)—are derived from x, y coordinates. For $i \in [1, n]$, $d_i = \sqrt{x_i^2 + y_i^2}$ and $\theta_i = tan^{-1}(y_i/x_i)$.

A. Histogram Method

1) Feature Extraction: First, we compute the first derivatives for the 10 raw features and 2 derived features. For a feature denoted by a vector $V = \{v_i | i = 1, 2, ..., n\}$, its first derivative $V' = \{v'_i | v'_i = v_{i+1} - v_i, i = 1, 2, ..., n-1\}$. Combining raw and derived features and their derivatives, we have 24 features in total.

Then, each feature vector is converted to a probability distribution histogram through binning. We create a given number of equidistant histogram bins with the given minimal and maximal values of the histogram and put each element of the vector into those bins. We then calculate the frequency of each bin by dividing the number of elements falling into that bin by the total number of elements. Let b_i be a frequency value for bin i. A feature vector B_j ($1 \leq j \leq 24$) is represented by concatenating the bin frequency values for feature j, i.e., $B_j = \{b_1^j || b_2^j || ... || b_{jm}^j\}$, where jm is the number of bins. Finally, a sample is represented by concatenating all the feature vectors B_j into a single feature vector F, i.e., $F = \{B_1 || B_2 || ... || B_{24}\} = \{b_1^1 || b_2^1 || ... || b_{1m}^1 || ... || b_1^{24} || b_2^{24} || ... || b_{24m}^{24}\}$.

2) Template Generation: A user template is created based on the user's training samples. A template for a given PIN or pattern is generated from the feature set derived from the training samples of that PIN or pattern. Since each sample is represented by a feature vector F_i, we have a sequence of vectors $F_1, F_2, ...F_k$ from k training samples. For each $F_i, 1 \leq i \leq k$, $F_i = \{f_1^i || f_2^i || ... || f_n^i\}$, where f_j^i ($1 \leq j \leq n, n = 1m + 2m + ... + 30m$) is a frequency value. The template F_t is defined as $F_t = \{f_1^t || f_2^t || ... || f_n^t\}$, where

$$f_j^t = \frac{avg(f_j^1, f_j^2, ..., f_j^k)}{std(f_j^1, f_j^2, ..., f_j^k) + \epsilon}, 1 \leq j \leq n,$$

and ϵ is a small value 0.002 to prevent division by zero. The feature vector F_t and standard deviation vector $Q = \{std(f_1^1, f_1^2, ..., f_1^k) || std(f_2^1, f_2^2, ..., f_2^k) || ... || std(f_n^1, f_n^2, ..., f_n^k)\}$ are stored as the user's profile for verification purpose.

3) Matching: A feature vector is created from a testing sample of input using the same procedure of data acquisition and feature extraction. To verify the claimed user, given a testing sample F_s, the similarity distance score D_{sim} is calculated using Manhattan Distance between F_t and F_s. $D_{sim} = \sum_{i=1}^{n} |f_i^t - f_i^s / Q_i|$. If the score is less than a predefined threshold the sample is accepted and the user passes the verification. Otherwise, the sample is rejected.

B. DTW Method

1) Feature Extraction: The DTW method extracts the same set of features as the Histogram method does, but its data representation of samples is different. All samples in DTW are represented using original time series. Assume n features (n is 24 in our case) are extracted from a sample with length (i.e., the number of time points) m, the sample is represented as a vector with $n \times m$ elements.

2) Template Generation: Let S and $Train$ be a training sample and the set of training samples, respectively. We use $min(d(S, Train - \{S\}))$ to denote the minimum DTW distance between S and all the other training samples. First, we calculate DTW distances between every pair of training samples to derive the average of minimum DTW distances $avg(D_{min})$, where $D_{min} = \{min(d(S, Train - \{S\})) : S \in Train\}$. Then, we identify a training sample T that has the minimal sum of the DTW distances to the other training samples. This sample is used as the user's template for the given PIN or pattern. The minimum DTW distance between T and the rest of training samples, $min(d(T, Train - \{T\}))$, is saved along with $avg(D_{min})$ as the user profile.

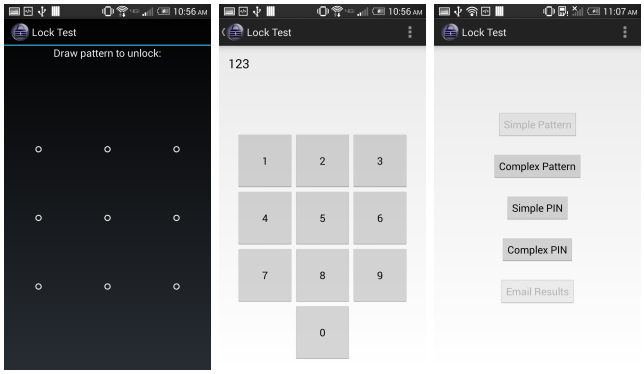
3) Matching: Assume sample S' is collected for the user to be verified. We compute the similarity score D_{sim} between sample S' and template T.

$$D_{sim} = \left| \frac{min(d(S', Train)) - min(d(T, Train - \{T\}))}{avg(D_{min})} \right|$$

where $d(S', Train)$ returns the set of DTW distances between S' and each training sample. The testing sample S' will be accepted if D_{sim} is lower than the predefined threshold; otherwise it will be rejected.

IV. Implementation

We implemented an Android application for data collection on both smartphone and tablet. Figure 2 shows the screenshots for the draw pattern unlock (a), PIN unlock (b), and the application's main interface (c).



(a) (b) (c)

Fig. 2. Screenshots of pattern unlock (a), PIN unlock (b), and main UI

An open source lock pattern library was modified to collect the behavioral biometric data when a pattern was entered. Using the `onTouchEvent` method, a timer is started when a user first touches the screen. The timer is set to run a task every 10 milliseconds. The task associated with the timer collects the x and y coordinates, the screen pressure, and the size of the user's touch. It then adds all of these values as well as the readings of the accelerometer and gyroscope to `ArrayLists`. The accelerometer and gyroscope values are collected using a `SensorManager`, which changes the values of specific variables each time the sensor value is changed. The timer is stopped and the `ArrayLists` are written to files when the user lifts his/her finger from the screen.

The same approach was also used for the PIN unlock. The major difference with this activity is that the timer will only stop running once 4 digits are entered by a user. This portion of the app does not use an external library but was manually coded, as it only consists of 10 buttons and a `TextView`.

The main activity of the app was designed with 5 buttons on the layout. The first 4 are for the simple and complex pattern entries and the simple and complex PIN entries. The last button, which is disabled by default, is used to email the results of the data collection. When a user presses one of the four data acquisition buttons, the appropriate activity will be launched within a loop that ends upon 30 successful attempts. Once the data collection activity is completed, the user is returned to the main activity and the button that was previously pressed is disabled. After all four activities have been completed and the associated buttons have been disabled, the email button is enabled. When the email button is pressed, the GMail app is launched with the appropriate recipients and subject filled in, and the files containing a user's data are attached. It is then up to the user to type an identification number that was previously assigned in the body of the email. Once the email is sent, the main activity is opened again, with all buttons disabled. The files are then manually deleted from the device.

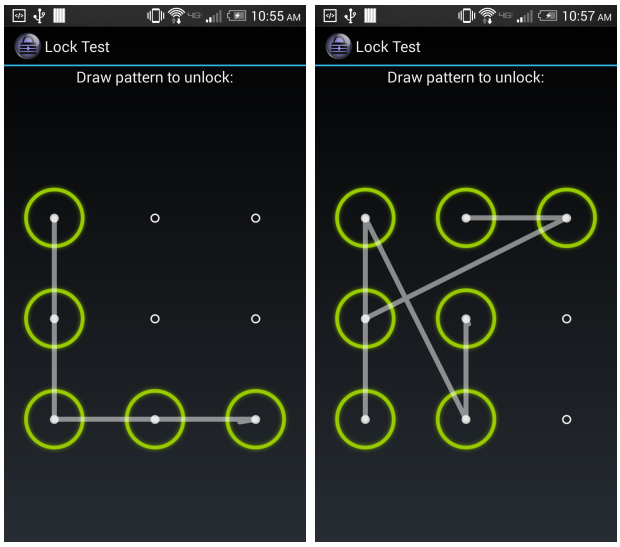
TABLE I
The mobile devices used in the experiments

Device	HTC Droid DNA (phone)	Samsung Galaxy Tab 10 (tablet)
CPU	1.5 GHz (Quad-core)	1.0 GHz (Dual-core)
RAM (GB)	2.0	1.0
Dimension (in)	5.55 x 2.78 x 0.38	10.09 x 6.81 x 0.34
Display Size (in)	5.0	10.1
Pixel Density (ppi)	441	149
Weight	4.9 oz (140 g)	19.93 oz (565 g)
Android Version	4.4.2	3.1

V. Evaluation

A. Data Collection

We recruited 15 volunteers (9 males and 6 females) for data collection. Among them, 3 are high school students, 10 are undergraduate or graduate students, 2 are college faculty. The ages of participants range from 19 to 48. A unique integer was assigned to each participant as their ID to protect participants' privacy. The study was reviewed and approved by the Institutional Review Board (IRB) of the University of Arkansas at Little Rock.



(a) (b)

Fig. 3. Screenshots of the simple pattern (a) and the complex pattern (b). If each dot is mapped to a digit (1-9) using the layout in Figure 2 (b), the sequence of the dots to be touched for the simple pattern is 1-4-7-8-9 and that sequence for the complex pattern is 2-3-4-7-1-8-5.

Each participant was asked to perform the test while sitting or standing with the device in one hand and performing the test with the other. At each session the participant was asked to perform 4 different tests: a simple pattern, a complex

TABLE II
MEAN (STD) OF EER VALUES (%) OF THE HISTOGRAM AND DTW METHODS

	Simple PIN		Complex PIN		Simple Pattern		Complex Pattern	
	Histogram	DTW	Histogram	DTW	Histogram	DTW	Histogram	DTW
Session I (phone)	6.5 (2.2)	6.4 (7.4)	4.8 (1.6)	3.4 (4.4)	4.6 (2.3)	3.8 (5.3)	2.7 (1.1)	5.1 (6.6)
Session II (phone)	5.5 (1.9)	5.5 (5.8)	5.6 (2.1)	3.3 (4.5)	5.0 (1.7)	7.6 (9.1)	3.7 (1.2)	8.7 (14.8)
Session III (tablet)	4.2 (2.4)	3.8 (4.9)	4.3 (1.3)	2.5 (3.0)	4.8 (2.1)	8.1 (6.4)	5.5 (2.6)	3.9 (4.0)
Sessions I & II	4.2 (2.8)	7.1 (5.8)	3.6 (2.0)	6.2 (7.5)	2.7 (0.9)	9.2 (11.4)	1.8 (0.7)	7.5 (6.8)

pattern, a simple PIN, and a complex PIN. Figure 3 depicts the screenshots of the simple pattern (a) and the complex pattern (b). Sequences 1-2-3-4 and 7-2-6-6 were uses as the simple PIN and the complex PIN, respectively. The simple and complex PINs and patterns were chosen specifically to emulate weak and strong PINs and patterns in real world based on the previous studies [8], [7]. Each of these tests was performed 30 times in a session. The two contiguous sessions were conducted at least 2 days apart. A HTC Droid DNA smartphone was used in the first two sessions while a Samsung Galaxy Tab 10.1 was used in the third session. The information of the smartphone and tablet is listed in Table I.

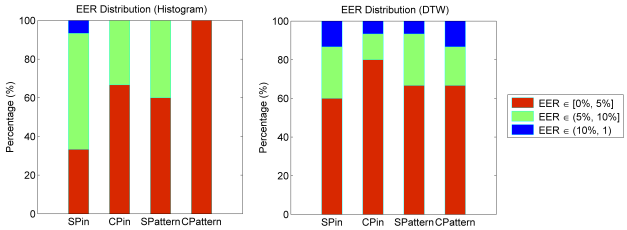


Fig. 4. Distribution of individual user EER values in session I

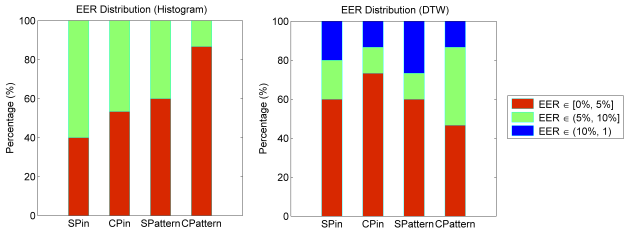


Fig. 5. Distribution of individual user EER values in session II

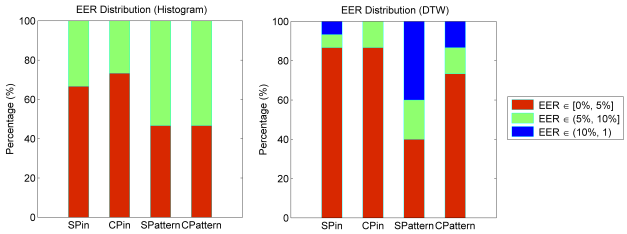


Fig. 6. Distribution of individual user EER values in session III

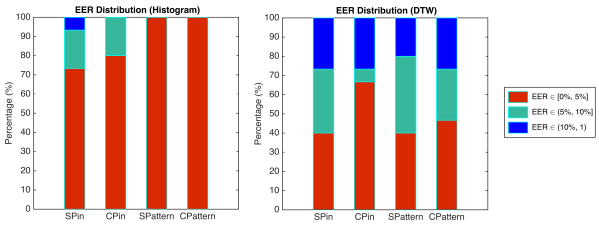


Fig. 7. Distribution of individual user EER values in sessions I & II

B. Data Analysis

We use false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER) as the metrics for measuring the accuracy of a verification method. FAR measures the likelihood of an unauthorized user being incorrectly accepted while FRR measures the likelihood of an authorized user being incorrectly rejected. EER is the rate when FAR and FRR are equal at a certain threshold value. In general, the lowest EER indicates the most accurate authentication decision. We evaluate authentication accuracy of the Histogram and DTW methods in terms of EER for both PIN and pattern samples.

We collected 90 samples (3 sessions) from each of the 15 participants (i.e., the "users") for each PIN/pattern and in total 5,400 samples are used in our evaluation. To measure the FRR of a PIN/pattern for each user, we use leave-one-out cross validation to test that user's samples of the given PIN/pattern. To measure the FAR of a PIN/pattern for each user, all other users' samples of that PIN/pattern are treated as impostors' samples and are tested against the genuine user's template. All testing results are represented as similarity scores from which we calculate FAR and FRR and derive EER. Table II shows the average EER values (in %) for the simple and complex PINs and patterns using the Histogram and DTW methods. Besides 3 individual sessions, we also combine the data in sessions I and II to test the template aging effect.

From Table II, both Histogram and DTW methods can achieve fairly low EER values ($< 5\%$). However, the EER values from DTW have significantly large standard deviations compared to their means in all cases while the standard deviations of the EER values from Histogram are consistently smaller than their means. This sharp contrast indicates that the EER values from DTW are much more diverse than those from Histogram. We depict the distributions of individual user EER values for each PIN/pattern in sessions I, II, III, and I & II in Figures 4, 5, 6, and 7 respectively. For each distribution, we

group EER values into 3 intervals $[0\%, 5\%]$, $(5\%, 10\%]$, and $(10\%, 1)$. We can clearly see that the portion of $(10\%, 1)$ only appear for simple PIN in 2 scenarios for the Histogram method while that portion persistently shows up for every PIN and pattern in every scenario for the DTW method. In general, the Histogram method appear more stable than the DTW method in terms of verification accuracy.

The EER results in Table II also suggest that when using the Histogram method the pattern-based schemes can achieve slightly higher accuracy than the PIN-based schemes on smartphone and the complex pattern (PIN) scheme has marginally better accuracy than the simple pattern (PIN) scheme. However, the obversion does not hold for results on the tablet. The simple pattern (PIN) scheme has even slightly better accuracy than the complex pattern (PIN) scheme. The difference between smartphone results and tablet results may be attributed to the size factor. The smartphone can be steadily held in one hand. The tablet is much larger and some noise may be introduced when a use enters a PIN or draws a pattern especially that PIN or pattern is complex. It is rather surprising that the difference between simple PIN/pattern and complex counterpart is pretty marginal. Based on the results, we believe that PIN-based and pattern-based behaviorial biometric authentication schemes can achieve the same level of accuracy with appropriate designed PINs and patterns.

For the DTW method, it is clear that the results for the complex PIN have better accuracy than those for the simple PIN in all 4 scenarios. This consistency, however, is lost for patterns' results. To our surprise, the Histogram method can handle template aging much better than the DTW method.

VI. Conclusion

In this paper we have compared the authentication accuracy between PIN-based and pattern-based behavioral biometric authentication on both smartphone and tablet using a uniform framework. We tested two representative verification techniques, namely Histogram and DTW in the comparison. We recruited 15 users and conducted 3-sessions data collection for both simple and complex PINs and patterns. Our experimental results reveal a few interesting findings regarding the accuracy of PIN-based and pattern-based behavioral biometric authentication schemes and the applied verification methods, which we believe is helpful for more comprehensive investigation on behavioral biometric authentication for mobile devices.

We would like to overcome some limitations of this study such as limited number of PINs, patterns, and testing users in our future investigation. One approach we plan to apply is to collect the behavioral biometric data through crowdsourcing, which has been shown effective in similar studies.

Acknowledgment

This work was supported partially by the Research Experiences for Undergraduates (REU) Program of the National Science Foundation under Award Number 1359323.

References

[1] E. von Zezschwitz, P. Dunphy, and A. De Luca, "Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices," in *Proc. MobileHCI'13*, 2013, pp. 261–270.

[2] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," in *Proc. HotSec'09*, 2009.

[3] A. De 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. CHI'12*, 2012, pp. 987–996.

[4] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.

[5] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. WOOT'10*, 2010, pp. 1–7.

[6] Z. Xu, K. Bai, and S. Zhu, "Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors," in *Proc. WiSec'12*, 2012, pp. 113–124.

[7] N. Zheng, K. Bai, H. Huang, and H. Wang, "You are how you touch: User verification on smartphones via tapping behaviors," in *Proc. ICNP'14*, 2014.

[8] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: The case of android unlock patterns," in *Proc. CCS'13*, 2013, pp. 161–172.

[9] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *Proc. SOUPS'14)*, Jul. 2014, pp. 187–198.

[10] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in *Proceedings of the 2nd USENIX Security Workshop*, 1990, pp. 5–14.

[11] A. Narayanan and V. Shmatikov, "Fast dictionary attacks on passwords using time-space tradeoff," in *Proc. CCS'05*, 2005, pp. 364–372.

[12] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proc. the 2012 IEEE Symposium on Security and Privacy*, 2012, pp. 553–567.

[13] C. Cornelius, R. Peterson, J. Skinner, R. Halter, and D. Kotz, "A wearable system that knows who wears it," in *Proc. MobiSys '14*, 2014, pp. 55–67.

[14] N. Zheng, A. Paloski, and H. Wang, "An efficient user verification system via mouse movements," in *Proceedings of the 18th ACM conference on Computer and communications security*, ser. CCS '11, 2011, pp. 139–150.

[15] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[16] Q. Tang, J. Bringer, H. Chabanne, and D. Pointcheval, "A formal study of the privacy concerns in biometric-based remote authentication schemes," in *Proc. ISPEC'08*, 2008, pp. 56–70.

[17] F. Bimbot, J.-F. Bonastre, C. Fredouille, G. Gravier, I. Magrin-Chagnolleau, S. Meignier, T. Merlin, J. Ortega-García, D. Petrovska-Delacrétaz, and D. A. Reynolds, "A tutorial on text-independent speaker verification," *EURASIP J. Appl. Signal Process.*, vol. 2004, pp. 430–451, Jan. 2004.

[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 and Security*, vol. 8, no. 1, pp. 136–148, 1 2013.

[19] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: A novel approach to authentication on multi-touch devices," in *Proc. CHI'12*, 2012, pp. 977–986.

[20] M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it," in *Proc. MobiCom'13*, 2013, pp. 39–50.

[21] M. Sherman, G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvirta, and T. Roos, "User-generated free-form gestures for authentication: Security and memorability," in *Proc. MobiSys'14*, 2014, pp. 176–189.

[22] N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 933–947, June 2014.