A Novel Nonintrusive User Authentication Method Based on Touch Gestures for Smartphones

Chien-Cheng Lin[1,2], *Chin-Chun Chang*[1], *Deron Liang*[2,3]
[1]*Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan*
[2]*Software Research Center, National Central University, Taiwan*
[3]*Department of Computer Science and Information Engineering, National Central University, Taiwan*
hammerlin@hotmail.com, cvml@mail.ntou.edu.tw, drliang@csie.ncu.edu.tw

Abstract

Novel nonintrusive authentication mechanisms for smartphones have recently been investigated to complement existing protection mechanisms. A major reason is that a nonintrusive approach can continually authenticate users without interrupting their operations. In this paper, a novel approach to nonintrusive authentication of smartphone users involving flick gestures is proposed. Sixteen histogram-based features of flick gestures, including five novel features related to the habitual touch positions of a user, were used for authentication. Empirical results based on 51 participants indicated that the proposed approach was feasible. The equal error rate of the proposed approach was approximately 4.37% ~ 5.13% when the histogram-based features were calculated based on 30 flicks and decreased to approximately 2.35% ~ 2.99% for features based on 60 flicks. In addition, the experimental results revealed that the five novel features proposed are effective. Possible applications and limitations of the proposed approach are discussed.

Keywords: Histogram-based features, Nonintrusive authentication, Smartphone, Touch screen sensor.

1 Introduction

Advances in information and communication technology have enabled smartphones to be used not only as telecommunication tools but also as endpoint devices in various applications, such as accessing emails and social networks [1-3]. The new applications of smartphones have raised security concerns regarding the identification of smartphone users when they access sensitive information stored in the phone or at remote sites [4-8]. Furthermore, recent surveys have reported that smartphone penetration has increased fourfold in 5 years (since 2007) [9], increasing the risk that smartphones are exposed to attacks.

Most current security protection mechanisms on smartphones are based on PIN codes, passwords, and biometric methods such as fingerprint recognition [10-11] and face recognition [12-14]. Fingerprint and password entry are intrusive; that is, they require explicit interaction with users. According to recent surveys [15-16], 60% ~ 80% of users disable these verification features to avoid the inconvenience these features cause. In addition, using mobile devices to access **sensitive information** with password-based authentication mechanisms involves the risk of shoulder surfing [17-22]. Therefore, to enhance the security level of mobile devices, **nonintrusive** authentication mechanisms must be developed [4-5][7].

Recently, biometric modalities such as gait [23-25] and voice modalities [14][25] have been applied in the nonintrusive authentication of smartphone users. Gait-based authentication mechanisms are useful when the user is in motion (e.g., walking). Voice is another modality that is suitable for nonintrusive authentication when the user is talking to others by using a smartphone. Conti et al. [26] proposed using both an accelerometer and an orientation sensor to authenticate a smartphone user answering or placing a phone call. None of the aforementioned approaches can be used to authenticate a smartphone user accessing sensitive information, which is one of the primary **smartphone applications** according to recent surveys [1-3].

Seo and Kim proposed an authentication method based on the input patterns of users to prevent mobile e-finance incidents [27]. However, because a proprietary GUI is required to collect a user's behavioral biometric data, this method may not be feasible for other apps. Shi et al. [28] and Feng et al. [29] nonintrusively authenticated a smartphone user who operated a smartphone through touch-gesture-related dynamics features. The main advantage of their systems is that they offer instant authentication. However, some types of distinctive touch-gesture-related features, such as the position of a touch gesture, cannot be characterized as dynamics features. The histogram-based approach [30-32] involves constructing authentication models by learning the distributions of features and has no limitation related to the type of feature. Therefore, this paper proposes a histogram-based approach to authenticate users that involves touch gestures.

The proposed approach involves 16 histogram-based features, namely five novel features related to the habitual touch positions of a user and 11 features derived from previous studies [28-30][33-34]. These 16 features belong

*Corresponding author: Deron Liang; E-mail: drliang@csie.ncu.edu.tw
DOI: 10.6138/JIT.2015.16.5.20131015

to three categories of touch gesture features, namely, trajectory, motion, and the characteristics of a touch screen (pressure and size). The objective is to capture the characteristics of the flick touch gesture of a user from various aspects. According to a thorough review of relevant research, this is the first publicly reported study that used the habitual touch positions of a user to construct an authentication model for smartphone users. For each smartphone user, 16 normalized histograms are established to represent the distributions of the 16 touch gesture features. The dissimilarity between the flick-touch gestures of two smartphone users is defined according to the weighted sum of the K-L divergences [35-36] between the corresponding histogram-based features of the two users. A user is identified as the genuine user if the dissimilarity between the flick-touch gestures of the user and the genuine user is small; otherwise, the user is identified as an imposter.

An app was implemented to collect the touch gestures of 51 participants. Experimental results revealed that the equal error rate (EER) of the proposed approach was approximately 4.37% ~ 5.13% when the histogram-based features were calculated based on 30 flicks, and the EER decreased to approximately 2.35% ~ 2.99% when the features were based on 60 flicks. The accuracy of the proposed approach was close to that of approaches involving the use of physiological biometrics such as fingerprints, the face, and the voice [10-11][14][25] and as high as that of methods based on behavioral biometrics such as keystrokes, mouse dynamics, gait, and dynamic-feature-based touch gestures [4][28-30][37-38]. The purpose of devising the proposed approach was to develop a complementary mechanism for improving smartphone security. For example, users can use strong biometrics or passwords explicitly for first-time authentication. Subsequently, the proposed approach can be applied in continual reverification.

The remainder of this paper is organized as follows. Section 2 describes the proposed approach. Section 3 presents the experimental results. Possible applications and limitations of the proposed approach are discussed in Section 4. Concluding remarks are provided in the final section.

2 Structural Modeling

2.1 Proposed Flick-Touch-Gesture-Related Features

Touch gestures may be categorized into the following types: flick, spread, pinch, and drag. Flick gestures are used to access data and operate a smartphone. Spread and pinch gestures are used to zoom in and zoom out on the touch screen. Drag gestures are used to move icons, files, and folders. Because flick-touch gestures are frequently used in smartphone apps [2-3], they were applied in authentication in this study.

According to the studies described in [28-29][34], people clearly tend to operate their smartphones in distinct manners. The straightness of flick trajectories, the velocity and acceleration of flick gestures, the touch pressure, and the touch size have been validated as features that can be used for authentication purposes. In this study, users were observed to have habitual touch positions on the touch screen when performing flick-touch gestures, and features related to the habitual touch positions may be used as behavioral biometric features.

Table 1 lists raw data on a flick; each record consists of six fields: the action type, x- and y-coordinates of the touch position in pixels, touch pressure, touch size, and time stamp. The action type and time stamp are used to identify the start and end of a flick. The trajectory of a flick can be formed by connecting adjacent touch positions.

Table 2 lists the 16 flick-gesture-related features adopted, including 11 trajectory-related features, three motion-related features, and two characteristics of the touch screen (touch pressure and touch size). The touch pressure and touch size are related to the strength and agility of a flick and were normalized based on the setting established in smartphone factories. Features 1 to 5 are the proposed novel features representing the habitual touch positions of smartphone users. Features 6 to 14 were proposed in [28-29][33-34], and Features 15 and 16 were used in [28-29][34]. A graphical illustration of Features 2 to 11 and Features 15 and 16 is shown in Figure 1.

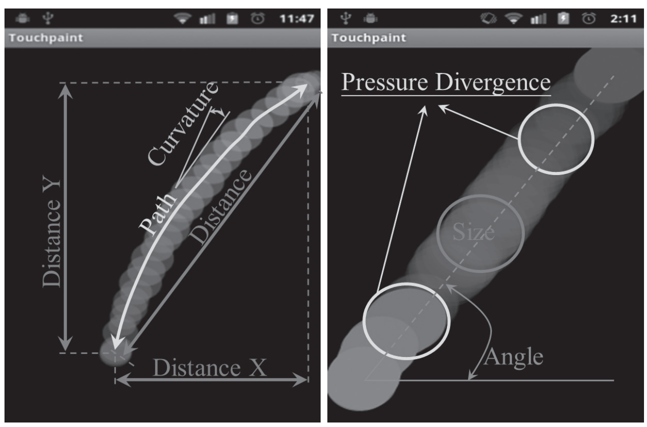


Figure 1 An Illustration of Features 2 to 11 and Features 15 and 16

A histogram-based representation [30-32] based on the frequencies of a feature in different ranges of feature values is used to represent the distribution of a feature in a sequence of flick gestures. The details on the histogram-based feature representation are described in the following paragraphs.

Table 1 Raw Flick Data

Type of motion	Touch				Time stamp
	X-axis	Y-axis	Pressure	Size	
...	...	...	...	...	...
Down	379.22	683.9117	0.6	0.1	1358839609887
Move	344.36	626.8816	0.6	0.1	1358839609939
Move	326.6	594.2988	0.6	0.1	1358839609962
Move	304.81	558.8608	0.6	0.133333	1358839609981
Move	280.37	525.4977	0.6	0.1	1358839610002
Move	256.16	495.7088	0.6	0.1	1358839610025
Move	204.88	435.0411	0.75	0.133333	1358839610053
Move	162.93	397.9022	0.75	0.1	1358839610072
Move	110.12	352.6057	0.75	0.133333	1358839610091
Move	69.609	318.8223	0.4625	0.066667	1358839610107
Up	69.609	318.8223	0.4625	0.066667	1358839610136
...	...	...	...	...	...
Down	275	713.1718	0.141176	0.141176	1352280110963

Table 2 Proposed Flick-Gesture-Related Features

Feature type	No	Feature name	Metrics	Range of data		Bin size	Range of bin		Units
				From	To		From	To	
A	1	*Touch-Position*	Pixel	400 × 800		40 × 40	1	240	%
	2	*Start-X*	Pixel	0	480	40	1	12	%
	3	*Start-Y*	Pixel	0	800	40	1	20	%
	4	*End-X*	Pixel	0	480	40	1	12	%
	5	*End-Y*	Pixel	0	800	40	1	20	%
	6	*Ang-T*	Degree	-180	180	10	1	36	%
	7	*Curv-T*	Degree/pixel	0	7.5	0.15	1	50	%
	8	*Dist-X*	Pixel	0	500	10	1	50	%
	9	*Dist-Y*	Pixel	0	810	30	1	25	%
	10	*Dist-T*	Pixel	0	1,000	50	1	20	%
	11	*Path-T*	Pixel	0	1,200	50	1	24	%
B	12	*Elapsed-time*	ms	0	2,000	40	1	50	%
	13	*Velocity*	Pixel/ms	0	50	1	1	50	%
	14	*Acceleration*	Pixel/ms^2	-0.75	0.75	0.015	1	200	%
C	15	*Touch-Pressure*	Manufacturer	0	1	0.005	1	200	%
	16	*Touch-Size*	Manufacturer	0	1	0.05	1	20	%

Note. Type A: Trajectory-Related Features; Type B: Motion-Related Features; Type C: Characteristic Feature of Touchscreen.

2.1.1 Trajectory-Related Features

In this study, the resolution of the touch screen was 480 × 800 pixels. The touch screen was partitioned into 12 × 20 blocks to account for the distribution of the flick trajectory. Feature 1, namely *Touch-Position*, represents the frequency of the flick trajectory passing through the corresponding block and was represented by a 240-bin histogram, in which each bin corresponded to one of the 240 blocks on the touch screen. Features 2 and 4, which are related to the distributions of the horizontal positions of the start and end points of the flick trajectory, were represented by two 12-bin histograms and. Features 3 and 5 were represented by

20-bin histograms and similarly defined for the vertical positions of the start and end points of the flick trajectory. Figure 2 shows a comparison between the distributions of the flick trajectories of two different users based on Feature 1, with the flick trajectories of the two users exhibiting distinct distributions.

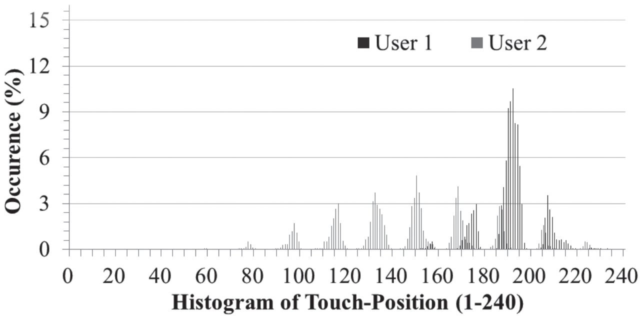


Figure 2 The 240-Bin Histograms of the Flick Trajectories of Two Users

Features 6 and 7, namely *Ang-T* and *Curv-T*, are related to the distributions of the slope and curvature of the flick trajectory and were represented by a 36-bin and a 50-bin histogram, respectively. Detailed definitions of *Ang-T* and *Curv-T* have been provided in [39] and [40], respectively. Features 8 to 10, namely *Dist-X*, *Dist-Y*, and *Dist-T*, are related to the distributions of the horizontal, vertical, and Euclidean distance between the start and end positions of the flick trajectory, and the features were represented by a 50-bin histogram, 27-bin histogram, and 200-bin histogram, respectively. Feature 11, namely *Path-T*, is related to the distribution of the trajectory length of the flick gesture and was represented by a 60-bin histogram.

2.1.2 Motion-Related Features

Features 12 to 14 are related to the distributions of the flick time, flick speed, and flick acceleration, respectively, and can be directly calculated using raw data. Features 12 and 13 were represented by 50-bin histograms, and Feature 14 was represented by a 100-bin histogram. Figure 3 shows a comparison between the distributions of the flick time of two users based on Feature 12; the distribution of the flick time of User 1 was concentrated on fast flicks, whereas the distribution of the flick time of User 2 was spread out and exhibited two modes. Thus, users exhibit characteristic flick motions.

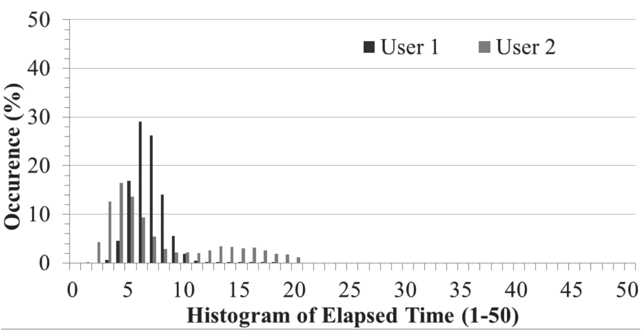


Figure 3 Distributions of the Flick Time of Two Users

2.1.3 Characteristics of a Touch Screen

Features 15 and 16 were based on the characteristics of the touch screen, which are related to the strength and agility of the flick gesture of a user. Feature 15, namely *Touch-Pressure*, was represented by a 200-bin histogram describing the distribution of the touch pressure. Feature 16, namely *Touch-Size*, was represented by a 20-bin histogram describing the distribution of the touch size. Figures 4 and 5 depict the distributions of the touch pressure and the touch size of two users based on Features 15 and 16, revealing that User 1 was more agile than User 2.

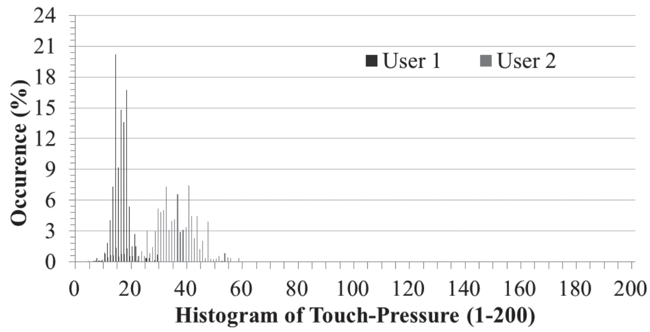


Figure 4 Distributions of the Touch Pressure of Two Users

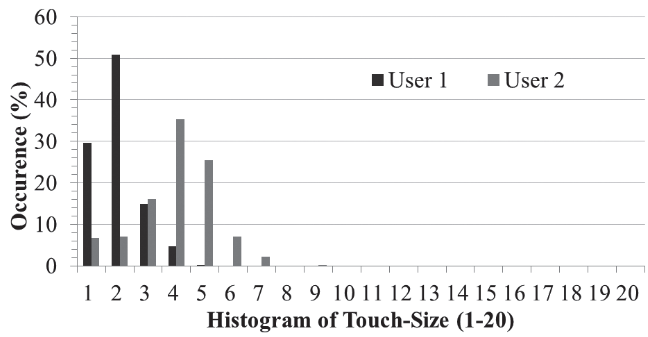


Figure 5 Distributions of the Touch Size of Two Users

2.2 System Modeling of the Proposed Approach

In this study, the dissimilarity between two histogram-based features $\mathbf{X}_1 = [\mathbf{f}_{11}...\mathbf{f}_{1d}]$ and $\mathbf{X}_2 = [\mathbf{f}_{21}...\mathbf{f}_{2d}]$ of the flick gesture was the weighted sum of symmetrized K-L divergences [35-36]:

$$D(\mathbf{X}_1, \mathbf{X}_2) = \sum_{i=1}^{d} w_i \left(D_{KL}(\mathbf{f}_{1i} \,\|\, \mathbf{f}_{2i}) + D_{KL}(\mathbf{f}_{2i} \,\|\, \mathbf{f}_{1i})\right) \quad (1)$$

where d denotes the number of features, $w_i \geq 0$, $i = 1...d$, are feature weights, and $D_{KL}(\mathbf{f} \,\|\, \mathbf{g})$ is the K-L divergence between two distributions $\mathbf{f}$ and $\mathbf{g}$ with $\sum_i \mathbf{f}(i) = 1$ and $\sum_i \mathbf{g}(i) = 1$ defined as

$$D_{KL}(\mathbf{f}\,\|\,\mathbf{g}) = \sum_i \ln\left(\frac{\mathbf{f}(i)}{\mathbf{g}(i)}\right)\mathbf{f}(i) \tag{2}$$

In the learning phase, a set of flick samples of the genuine user is provided to learn the histogram-based feature of the flick gesture of the user, which is regarded as the authentication model of the genuine user. In addition, samples from imposters are provided to calculate the feature weights as follows:

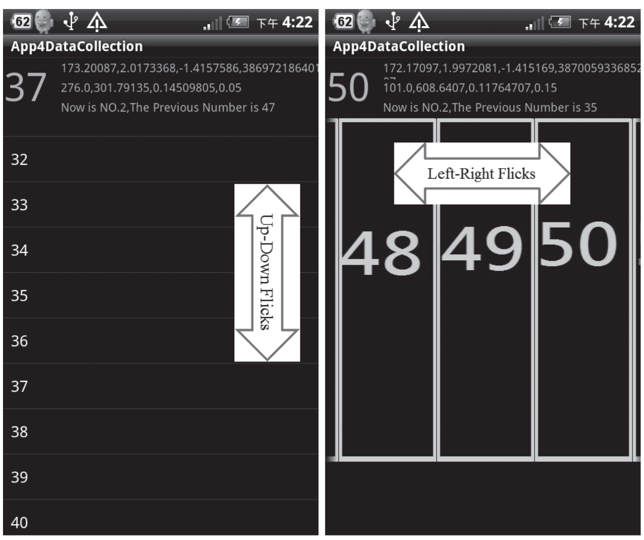
$$w_i = \frac{\sum_u \sum_v \left\{ D_{KL}(\mathbf{f}^g_{ui}\,\|\,\mathbf{f}^i_{vi}) + D_{KL}(\mathbf{f}^i_{vi}\,\|\,\mathbf{f}^g_{ui}) \right\}}{\min\limits_{u\neq v} \left\{ D_{KL}(\mathbf{f}^g_{ui}\,\|\,\mathbf{f}^g_{vi}) + D_{KL}(\mathbf{f}^g_{vi}\,\|\,\mathbf{f}^g_{ui}) \right\}} \tag{3}$$

where $\mathbf{f}^g_{ui}$ denotes the histogram for the ith feature of the uth sample of the genuine user, and $\mathbf{f}^i_{vi}$ is analogically defined as the sample of imposters. The feature weight w_i is the ratio of the dissimilarity between the user and imposters to the minimum dissimilarity between individual strokes of the user. A user is classified as an imposter if the dissimilarity between the histogram-based feature of the flick gesture of the user and the authentication model of the genuine user is greater than a prespecified threshold; otherwise, the user is classified as the genuine user.

3 Experimental Results

3.1 Data Collection

An app was developed on the HTC™ Sensation XL [41] by using the Android™ 2.3 platform [42] to collect users' left-right and up-down flick actions, because these two types of flick actions are often used to access data, as Figure 6 shows. When a user's finger touches the screen of the smartphone, the app continually collects touch-based readings at a sampling rate of 50 Hz until her or his fingers leave the screen.



(a) Up-Down Flicks (b) Left-Right Flicks

Figure 6 App Used for Data Collection

To simulate a realistic situation, a total of 51 participants, specifically 33 men and 18 women with various levels of smartphone experience and ages ranging from 18 to 40 years, participated in this experiment. To ensure that the participants operated the smartphone in a consistent manner, all participants sat on the same chair and operated the same smartphone, as shown in Figure 7.

Figure 7 Experimental Setup for Data Collection

Two data sets were collected: one for up-down flicks and the second for left-right flicks. The participants produced a total of 210,000 flick samples. The collected data were stored on the smartphone. Each participant generated approximately 2,000 up-down flick samples and 2,000 left-right flick samples. Flick actions shorter than 100 ms were disregarded because they were considered too short to convey information useful for authentication. Approximately 3% of the collected touch gestures were short flicks and were thus disregarded.

3.2 Experimental Design

The main objectives of the experiments were to verify the feasibility of the proposed approach and to evaluate the effectiveness of the five novel features proposed. Three experiments were conducted based on the collected data sets with respect to three feature subsets: Set-16, Set-5, and Set-11. Set-16 comprised all 16 features defined in Section 2. Set 5 was a subset of Set-16 and consisted of the five novel features proposed, and Set-11 comprised the other 11 features in Set-16.

To perform the experiments, a suitable size for the training set used to construct the authentication model of the genuine user was determined by using learning curves. In the pre-test, we evaluated varying thresholds several rounds. The results show that the varying thresholds to performance is insensitive. As shown in Figure 8, the pretest results revealed that a training set consisting of 450 flick samples was suitable.

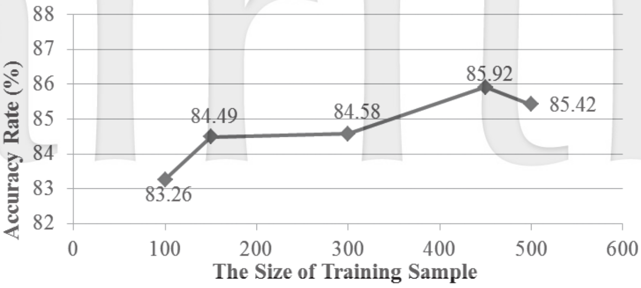


Figure 8 Learning Curve for the Touch Screen (5 flicks)

In our experiments, the false acceptance rate (FAR), and the false rejection rate (FRR) were estimated based on the results of five rounds. In each round, every participant played the role of the genuine user once and the other participants were imposters. An authentication model for the genuine user was learned from a training set containing 450 flick samples. The test set contained 1000 samples of the histogram-based features of the imposters (20 samples per imposter) and 500 samples of the histogram-based features of the genuine user.

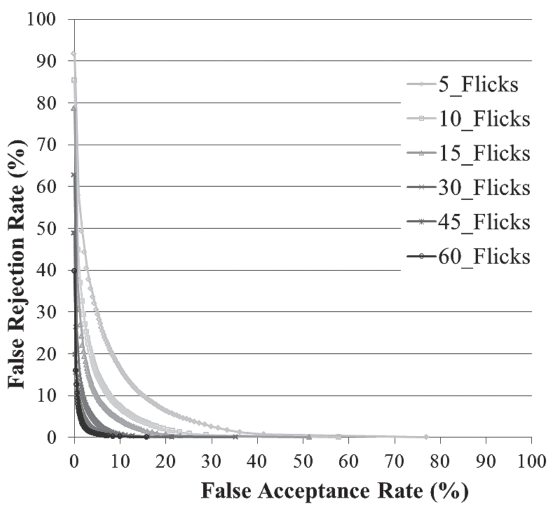
3.3 Results

The results in Figure 9(a) and (b) show the detection error tradeoff curve of the proposed approach with respect to the data sets of the up-down flicks and the left-right flicks based on Set-16; the performance when the histogram-based features based on 5, 10, 15, 30, 45, and 60 flicks were applied is shown. The performance increased substantially from 5 flicks to 30 flicks. After 30 flicks, the improvement was marginal. The proposed approach yielded an EER lower than 4.75% when the number of flicks exceeded 30, and the EER was approximately 2.67% when the number of flicks was 60 (approximately 1 min). As Table 3 shows, the performance of the proposed approach was close to that of approaches based on physiological biometrics such as fingerprints, the face, and the voice [10-11][14][25] and at least as accurate as approaches based on behavioral biometrics such as keystrokes, mouse dynamics, and touch gestures [4][28-30][37-38].

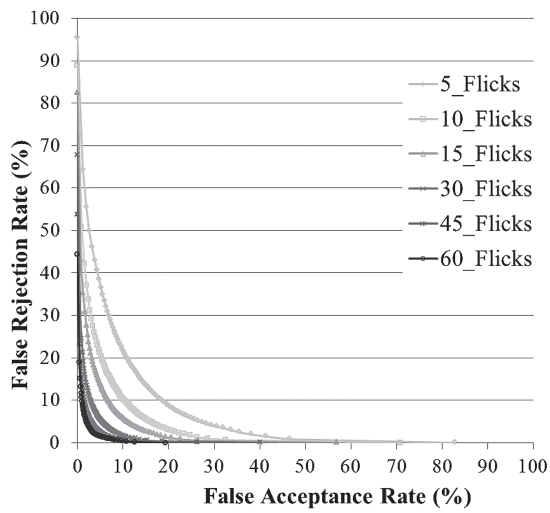
Table 3 Performance of Various Biometric Characteristics

Biometrics	Performance, %	Participants
Physiological		
IRIS [13-14]	EER = 0.0259	456 (eyes)
Fingerprint [10-11][25]	EER = 3.2	110 (fingers)
Palmprint [14][44]	EER = 0.19	392 (palms)
Face [14]	EER = 6	13,872 (images)
Voice [14][25]	EER = 2.9 to 41.6	32
Behavioral		
Signature [45]	EER = 0.99 to 1.07	94
Keystroke [4][37]	EER = 4; FAR = 0.01	154, 32
Mouse [30][38]	EER = 2.461; FAR = 2.464	22, 15 ~ 22
Gait [23-25]	EER = 5 to 9	21
Touch Gestures [28-29]	EER = 0.13; FAR = 4.66	40

Tables 4 and 5 show the EERs for the up-down flicks and the left-right flicks based on the three feature sets. The EER for Set-11 was 1.7 times higher than that for Set-16 on average. This observation indicates that, without the five novel features proposed, the accuracy of the proposed



(a) Up-Down Flicks



(b) Left-Right Flicks

Figure 9 Experimental Results for Up-Down/Left-Right Flicks Based on the Touch-Gesture-Related Histogram Features

Table 4 Performance of Three Applied Feature Sets Based on Up-Down Flicks

Features / Flicks	EER % (Experiment I) Set-16 (Set-11 ∪ Set-5)	EER % (Experiment II) Set-11 (11 features)	EER % (Experiment III) Set-5 (5 features)
5	12.68	19.27	16.96
10	8.64	15.41	12.98
15	7.02	13.62	11.01
30	4.37	10.04	8.06
45	3.12	7.82	6.55
60	2.35	6.24	5.35

Table 5 Performance of Three Applied Feature Sets Based on Left-Right Flicks

Features / Flicks	EER % (Experiment I) Set-16 (Set-11 ∪ Set-5)	EER % (Experiment II) Set-11 (11 features)	EER % (Experiment III) Set-5 (5 features)
5	14.29	17.66	21.77
10	10.16	13.70	17.41
15	7.93	11.16	15.07
30	5.13	7.34	11.83
45	3.75	5.82	9.77
60	2.99	4.79	8.29

approach decreases considerably, evidencing that the five novel features proposed are effective.

Because the smartphone used in this experiment is rectangular, and the height of this smartphone is greater than the width, the length of the trajectory of an up-down flick is usually longer than the trajectory length of a left-right flick. Consequently, up-down flicks could contain more behavioral information than left-right flicks. This is the reason why Set-5, which is a set of trajectory-related features, benefits from up-down flicks.

Table 6 shows the computing time of the proposed approach. In general, the computing times for determining the histogram-based features of a user and for authenticating the user by using Equation (1) were proportional to the number of flicks and the number of features. When 60 flicks were used, the computing time for Set-16 was 62.70 ms, indicating that the proposed approach is computationally efficient. In comparison with the computing times for Set-11 and Set-16, the computation overheads of the five novel features proposed were 3.08 ms and 25.07 ms for five flicks and 60 flicks, respectively, indicating that the five novel features proposed are computationally inexpensive.

Table 6 Average Computing Time

Feature sets / Flicks	5	10	15	30	45	60
Set-11						
T_1	3.00	5.92	8.88	17.77	26.65	36.00
T_2	1.63	1.63	1.63	1.63	1.63	1.62
T_3	4.63	7.55	10.51	19.40	28.28	37.63
Set-16						
T_1	5.00	8.62	12.92	25.85	38.77	60.00
T_2	2.70	2.70	2.70	2.70	2.70	2.70
T_3	7.71	11.32	15.63	28.55	41.47	62.70

Note. Units: Millisecond. T_1: The computing time used to form the histogram-base features. T_2: The computing time used to recognize a user. T_3: The total computing time ($T_1 + T_2$).

Table 7 shows the response times when various numbers of flicks were used. The response time depended on the user. In general, 3 ~ 40 s were required to perform 5 ~ 60 flicks on the app designed for this experiment. In other words, the proposed system could authenticate the user after more than five flicks, and this nonintrusive and continuous authentication function could be enabled in approximately 3 s on average.

Table 7 Average Response Time

Flicks	5	10	15	30	45	60
Time (sec)	2.88	5.75	8.55	18.37	28.25	38.77

4 Discussion

4.1 Possible Applications of the Proposed Approach

Private data, such as emails, documents, contact lists, and social networks, are the most coveted targets for cyber attackers. In smartphone apps, users often access data through left-right or up-down flicks; this behavior inspired the use of the five novel features related to the habitual touch positions of smartphone users. However, the proposed approach is not suitable for apps in which left-right or up-down flicks are not used to access data, such as Candy Crush Saga.

Although physiological biometrics are more useful than behavioral biometrics [24][43], as Table 3 shows, the proposed behavioral biometric method can improve the security level of intrusive authentication systems through continuous authentication and access control. For example, physiological biometrics or password entry may be used when a user is denied access by the proposed system.

For applications in which convenience is more important than security, the proposed system can be adjusted by controlling the system parameters to achieve a low or zero FRR (e.g., a zeroFRR), which is the minimum FAR with respect to the zero FRR. The zero FRR of our system for 30 flicks was approximately 40%, suggesting that the proposed system can provide an additional level of security in which approximately 60% of attackers can be detected without interrupting the user.

4.2 Limitations of the Proposed Approach

Under ideal conditions for the proposed approach, the genuine user always operates a smartphone in a specific manner. However, in practice, the proposed approach exhibits limitations, namely a mimic problem, a regular behavior problem, a posture problem, and a problem of users having similar habits.

- Regarding the mimic problem, it is crucial to verify whether impersonation attacks executed by trained hostile users and hostile users who can easily mimic other users as well as attacks attributable to users whose operate styles are relatively easy to mimic can be resisted (in other words, whether there are any users of "lamb" or "wolf" type, as defined by Doddington et al. [46]). The mimic problem is not addressed in this paper and should be investigated in future research.
- A smartphone user may have different operation behaviors when not using his or her regular hand to operate the smartphone. In such a situation, behavior-based authentication systems must learn the irregular behaviors of the genuine user. For simplicity, this problem is not addressed in this paper.
- A user may flick the touch screen in a manner different from that in which flicks were recorded in the authentication model (e.g., walking or lying on the bed or sofa). In this case, the performance of the proposed approach may be poor. Therefore, a crucial premise of the proposed approach is that the user operates the smartphone in a pose similar to that recorded in the authentication model.
- In reality, it is possible to have similar habits for smartphone users with same age, position, education degree, etc. Therefore, it may be more difficult to distinguish them. In this paper, the experiments are designed to simulate a realistic situation where intruders have different smartphone experiences. Now, we do not have clues to validate whether these factors will affect the performance of a behavior-based authentication system. To validate this hypothesis, we will design experiments in our future work.

5 Concluding Remarks

This paper proposes a nonintrusive authentication approach involving the touch screen of a smartphone. The proposed approach involves adopting 16 histogram-based features, including five novel features related to the habitual touch positions of a user. The contribution of this paper is threefold. First, according to a thorough review of research, this is the first publicly reported study in which an authentication model for smartphone users was constructed using their habitual touch positions on the touch screen. Second, the touch-gesture-related approach is at least as accurate as approaches involving behavioral biometrics such as gait, mouse dynamics, and keystrokes. Third, this study proposed five novel effective features and demonstrated their importance to the touch-gesture-based authentication system. In the future, more sophisticated classifiers with advanced feature extraction schemes will be used to improve the proposed system.

References

[1] Gartner, Inc., *Gartner Says Number of Mobile Payment Users Worldwide to Increase 70 Percent in 2009*, 2009, http://www.gartner.com/it/page.jsp?id=995812

[2] Gartner, Inc., *Gartner Identifies the Top 10 Consumer Mobile Applications for 2012*, 2009, http://www.gartner.com/it/page.jsp?id=1230413

[3] O2 News Centre, *Making Calls Has Become Fifth Most Frequent Use for a Smartphone for Newly-Networked Generation of Users*, 2012, http://news.o2.co.uk/Press-Releases/Making-calls-has-become-fifth-most-frequent-use-for-a-Smartphone-for-newly-networked-generation-of-users-390.aspx

[4] Nathan L. Clarke and Steven Furnell, *Authenticating Mobile Phone Users Using Keystroke Analysis*, *International Journal of Information Security*, Vol.6, No.1, 2007, pp.1-14.

[5] Nathan L. Clarke, Sevasti Karatzouni and Steven Furnell, *Flexible and Transparent User Authentication for Mobile Devices*, *Proc. 24th IFIP TC 11 International Information Security Conference, SEC 2009*, Pafos, Cyprus, May, 2009, pp.1-12.

[6] Mohammad Najmud Doja and Naveen Kumar, *User Authentication Schemes for Mobile and Handheld Devices*, *INFOCOMP Journal of Computer Science*, Vol.7, No.4, 2008, pp.38-47.

[7] Steven Furnell, Nathan L. Clarke and Sevasti Karatzouni, *Beyound the PIN: Enhancing User Authentication for Mobile Devices*, *Computer Fraud & Security*, Vol.2008, No.8, 2008, pp.12-17.

[8] Oleksiy Mazhelis, Jouni Markkula and Jari Veijalainen, *An Integrated Identity Verification System for Mobile Terminals*, *Information Management & Computer Security*, Vol.13, No.5, 2005, pp.367-378.

[9] Lars Kamp, *Mobility Trends that Will Define the Next Decade, Mobile World Congress 2012, Accenture Mobility*, 2009, http://www.slideshare.net/scapecast/accenture-mobility-mwc-2012-bubble-over-barcelona-lars-kamp

[10] Dario Maio, Raffaele Cappelli and Anil K. Jain, *FVC2000: Fingerprint Verification Competition*, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol.24, No.3, March 2002, pp.402-412.

[11] Yong-Liang Zhang, J. Yang and Hong-Tao Wu, *Sweep Fingerprint Sequence Reconstruction for Portable Devices*, *Electronics Letters*, Vol.42, No.4, 2006, pp.204-205.

[12] Aravind Ruthala, Karthick Santhanam, Prashant Sanjay and Santosh Chilkunda, *Face Recognition on Android*, 2010, https://sites.google.com/site/androidfacerecognition/Home

[13] Donald M. Monro, Soumyadip Rakshit and Dexin Zhang, *DCT-Based Iris Recognition*, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol.29, No.4, 2007, pp.586-595.

[14] Lawrence O'Gorman, *Comparing Passwords, Tokens, and Biometrics for User Authentication*, *Proceedings of the IEEE*, Vol.91, No.12, 2003, pp.2021-2040.

[15] Smart Credit, *Consumer Reports Survey on Mobile Phones and Security*, 2011, http://blog.smartcredit.com/2011/09/02/consumer-reports-survey-on-mobile-phones-and-security/

[16] Carole Theriault, *Survey Says 70% Don't Password Protect Mobiles*, 2011, http://nakedsecurity.sophos.com/2011/08/09/free-sophos-mobile-security-toolkit/

[17] Andrea Bianchi, Ian Oakley and Dong-Soo Kwon, *Obfuscating Authentication through Haptics, Sound and Light*, *Proc. of CHI'11 Extended Abstracts on Human Factors in Computing Systems*, Vancouver, Canada, May, 2011, pp.1105-1110.

[18] Alain Forget, Sonia Chiasson and Robert Biddle, *Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords*, *Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI'10)*, Atlanta, GA, April, 2010, pp.1107-1110.

[19] Saranga Komanduri and Dugald R. Hutchings, *Order and Entropy in Picture Passwords*, *Proc. Graphics Interface (GI'08)*, Windsor, Canada, May, 2008, pp.115-122.

[20] Taekyoung Kwon, Jong-Hyup Lee and Joo-Seok Song, *On the Privacy-Preserving HCI Issues*, *Proc. of UAHCI 2009*, San Diego, CA, July, 2009, pp.544-549.

[21] Volker Roth, Kai Richter and Rene Freidinger, *A PIN-Entry Method Resilient Against Shoulder Surfing*, *Proc. 11th ACM Conference on Computer and Communications Security*, Washington, DC, October, 2004, pp.236-245.

[22] Furkan Tari, A. Ant Ozok and Stephen H. Holden, *A Comparison of Perceived and Real Shoulder-Surfing Risks between Alphanumeric and Graphical Passwords*, *Proc. of SOUPS'06*, Pittsburgh, PA, July, 2006, pp.56-66.

[23] Mohammad O. Derawi, Patrick Bours and Kjetil Holien, *Improved Cycle Detection for Accelerometer Based Gait Authentication*, *Proc. Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'10)*, Darmstadt, Germany, October, 2010, pp.312-317.

[24] Davrondzhon Gafurov, Kirsi Helkala and Torkjel Søndrol, *Biometric Gait Authentication Using Accelerometer Sensor*, *Journal of Computers*, Vol.1, No.7, 2006, pp.51-59.

[25] Elena Vildjiounaite, Satu-Marja Makela, Mikko Lindholm, Vesa Kyllonen and Heikki Ailisto, *Increasing Security of Mobile Devices by Decreasing User Effort in Verification*, *Proc. Second International Conference on Systems and Networks Communications (ICSNC'07)*, Cap Esterel, France, August, 2007, pp.80-85.

[26] Mauro Conti, Irina Zachia-Zlatea and Bruno Crispo, *Mind How You Answer Me!: Transparently Authenticating the User of a Smartphone When Answering or Placing a Call*, *Proc. 6th ACM Symposium on Information, Computer, and Communications Security (ASIACCS'11)*, Hong Kong, China, March, 2011, pp.249-259.

[27] Hojin Seo and Huy-Kang Kim, *User Input Pattern-Based Authentication Method to Prevent Mobile E-Financial Incidents*, *Proc. Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW)*, Busan, Korea, May, 2011, pp.382-387.

[28] Weidong Shi, Jun Yang, Yifei Jiang, Feng Yang and Yingen Xiong, *SenGuard: Passive User Identification on Smartphones Using Multiple Sensors*, *Proc. IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Shanghai, China, October, 2011, pp.141-148.

[29] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunary, Yifei Jiang and Nhung Nguyen, *Continuous Mobile Authentication Using Touchscreen Gestures*, *Proc. 12th IEEE Conference on Technologies for Homeland Security (HST'12)*, Waltham, MA, November, 2012, pp.451-456.

[30] Ahmed Awad E. Ahmed and Issa Traore, *A New Biometric Technology Based on Mouse Dynamics*, *IEEE Transactions on Dependable and Secure Computing,* Vol.4, No.3, 2007, pp.165-179.

[31] James Hafner, Harpreet S. Sawhney, Will Equitz, Myron Flickner and Wayne Niblack, *Efficient Color Histogram Indexing for Quadratic Form Distance Functions*, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol.17, No.7, 1995, pp.729-736.

[32] Ediz Saykol, Uğur Güdükbay and Özgür Ulusoy, *A Histogram-Based Approach for Object-Based Query-by-Shape-and-Color in Multimedia Databases*, *Image and Vision Computing*, Vol.23, No.13, 2005, pp.1170-1180.

[33] Chien-Ceng Lin, Chin-Chun Chang and Deron Liang, *A New Non-intrusive Authentication Approach for Data Protection Based on Mouse Dynamics*, *Proc. 2012 International Symposium on Biometrics and Security Technologies (ISBAST'12)*, Taipei, Taiwan, March, 2012, pp.9-14.

[34] Chien-Ceng Lin, Chin-Chun Chang, Deron Liang and Ching-Han Yang, *A Preliminary Study on Non-intrusive User Authentication Method Using Smartphone Sensors*, *Applied Mechanics and Materials*, Vol.284-287, 2013, pp.3270-3274.

[35] Solomon Kullback, *Letter to the Editor: The Kullback-Leibler Distance*, *The American Statistician*, Vol.41, No.4, 1987, pp.340-341.

[36] Solomon Kullback and Richard Leibler, *On Information and Sufficiency*, *The Annals of Mathematical Statistics*, Vol.22, No.1, 1951, pp.79-86.

[37] Francesco Bergadano, Daniele Gunetti and Claudia Picardi, *User Authentication through Keystroke Dynamics*, *ACM Transactions on Information and System Security*, Vol.5, No.4, 2002, pp.367-397.

[38] Kenneth Revett, Hamid Jahankhani, Sérgio Tenreiro de Magalhães and Henrique M. D. Santos, *A Survey of User Authentication Based on Mouse Dynamics*, *Communications in Computer and Information Science*, Vol.12, 2008, pp.210-219.

[39] Wikipedia, *Angle*, http://en.wikipedia.org/wiki/Angle

[40] Wikipedia, *Curvature*, http: http://en.wikipedia.org/wiki/Curvature

[41] HTC Inc., *Smartphone*, http://www.htc.com/us/products

[42] Google Inc., *Android™ Platform*, http://developer.android.com/index.html

[43] Ruud M. Bolle, Jonathan H. Connell and Nalini K. Ratha, *Biometric Perils and Patches*, *Pattern Recognition*, Vol.35, No.12, 2002, pp.2727-2738.

[44] Xiangqian Wu, Kuanquan Wang and David Zhang, *Palmprint Texture Analysis Using Derivative of Gaussian Filters*, *Proc. 2006 International Conference on Computational Intelligence and Security (CIS'06)*, Guangzhou, China, November, 2006, pp.751-754.

[45] Alisher Kholmatov and Berrin Yanikoglu, *Identity Authentication Using Improved Online Signature Verification Method*, *Pattern Recognition Letters*, Vol.26, No.15, 2005, pp.2400-2408.

[46] George Doddington, Walter Liggett, Alvin Martin, Mark Przybocki and Douglas Reynolds, *Sheep, Goats, Lambs and Wolves a Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation*, *Proc. 5th International Conference on Spoken Language Processing*, Sydney, Australia, November/December, 1998, pp.1351-1354.

Biographies

Chien-Cheng Lin is currently attending the National Taiwan Ocean University, Taiwan, pursuing a PhD in computer science and engineering. He also earned his MS in computer science there in 2003. His research interests include fault-tolerance, information security, and digital forensics.

Chin-Chun Chang received the BS degree and the MS degree in computer science in 1989 and 1991, respectively, and the PhD degree in computer science in 2000, all from National Chiao Tung University, Hsinchu, Taiwan. From 2001 to 2002, he was a faculty of the Department of Computer Science and Engineering, Tatung University, Taipei, Taiwan. In 2002, he joined the Department of Computer Science and Engineering, National Taiwan Ocean University, Keelung, Taiwan, where he is currently an associate professor. His research interests include computer vision, machine learning, and pattern recognition. He is a member of the IEEE.

Deron Liang received a BS degree in electrical engineering from National Taiwan University in 1983, and an MS and a PhD in computer science from the University of Maryland at College Park in 1991 and 1992 respectively. He is on the faculty of Department of Computer Science & Information Engineering, and serves as Director of Software Research Center, National Central University, Taiwan since 2008. Dr. Liang's current research interests are in the areas of software fault-tolerance, system security, and system reliability analysis. Dr. Liang is a member of ACM and IEEE.