CapAuth: Identifying and Differentiating User Handprints on Commodity Capacitive Touchscreens

Anhong Guo **Robert Xiao** **Chris Harrison**
Human-Computer Interaction Institute
Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213
{anhongg,brx,chris.harrison}@cs.cmu.edu

ABSTRACT
User identification and differentiation have implications in many application domains, including security, personalization, and co-located multiuser systems. In response, dozens of approaches have been developed, from fingerprint and retinal scans, to hand gestures and RFID tags. In this work, we propose CapAuth, a technique that uses existing, low-level touchscreen data, combined with machine learning classifiers, to provide real-time authentication and even identification of users. As a proof-of-concept, we ran our software on an off-the-shelf Nexus 5 smartphone. Our user study demonstrates twenty-participant authentication accuracies of 99.6%. For twenty-user identification, our software achieved 94.0% accuracy and 98.2% on groups of four, simulating family use.

Author Keywords
Touchscreen input; mobile devices; capacitive sensing; user identification; user differentiation; groupware.

ACM Classification Keywords
H.5.2. Information interfaces and presentation (*e.g.*, HCI): User Interfaces: Input devices and strategies.

INTRODUCTION

Understanding *who* is interacting with a computing device has many implications and applications. It is most often used for authentication [1,5,10], where only certain users are permitted to use the system or privileged functionality. It can also be used for personalization [9,12], where different users can have custom settings, browser bookmarks, email accounts, favorite applications and so on. Furthermore, knowing who is performing what action is also tremendously valuable in co-located computer supported collaborative work [2,13] and games [4], for example, on large interactive tabletops.

Recently, Bodyprint [6] demonstrated how unmodified, commodity touchscreens can be used to identify and authenticate users. This is done by capturing a capacitive "image" of various body parts when they are pressed to the touchscreen, for example the ear. We extend this paradigm with a new "hands-flat" pose, which reveals more distinguishing user features, enabling higher recognition accuracies. During evaluation, Bodyprint used a single round of data collected in one sitting, and ran a post hoc cross-fold analysis. We extend this feasibility study to additionally validate stability over time, where users attempt to authenticate at a later time. We also extend the study to account for real world issues, such as hand moisture level and accuracies amongst small groups of users.

ITS '15, November 15-18, 2015, Funchal, Portugal
 ISBN 978-1-4503-3899-8/15/11···$15.00
DOI: http://dx.doi.org/10.1145/2817721.2817722

IMPLEMENTATION

Modern projected capacitive touchscreens work by detecting changes in a projected electric field caused by a proximate finger. The touch controller collects capacitance measurements across the touch-sensing grid (Figure 1), which are taken together to form a *capacitive image*. This image is generally used inside the touch controller to resolve the pixel position of touch contacts, which are subsequently reported to the operating system.

We developed our proof-of-concept CapAuth implementation on a Nexus 5 smartphone running Android 5.0.1, with a Linux kernel specially modified to provide access to the Synaptics ClearPad 3350 touchscreen controller's debugging interface. We use this interface to obtain the 16-bit 15×27 capacitive image at 25 FPS. Each pixel of the image corresponds to a 4.1mm×4.1mm square on the screen. The pixel values are the picofarad (pF) differences between the baseline measurement and current measurement. CapAuth uses the capacitive image to derive a series of features designed to capture material (*e.g.*, varying dielectric effects from skin thickness) and geometric (*e.g.*, heights of fingers) variations between the hands of different users.

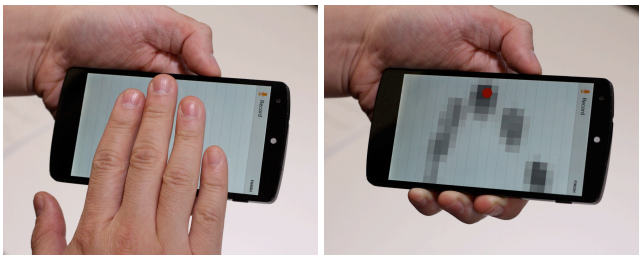

Figure 1. Capacitive image on Nexus 5. Left: hand position on the screen. Right: resulting capacitive image.

Features

We compute the following set of 550 features from the capacitive image: each raw data point as an independent feature, mean values of the capacitive image / each row / each column, length of each finger, number of pixels with a value of over 15pF for each finger, sum of value of each finger, coordinates of the 9 points (overall centroid / four fingertips / centroids of each finger), and the distances and angles of each of the two points among the 9 points. Using feature selection, we found that a subset of 150 features was sufficient for reasonably accurate classification.

Classification Algorithm

The full feature set is used to train quadratic-kernel support vector machine (SVM) classifiers using the Weka machine-learning toolkit [3]. For authentication, we use a binary classifier specific to each user, which distinguishes between that user and all other users. For identification, we train a multi-class, one-to-one classifier, which uses binary classifiers trained to distinguish each pair of users. Each binary classifier output is treated as a vote for that user, and the votes are tallied to form the final classifier output.

Correct Hand Placement

We use a separate process for ensuring that users place their hands on the screen in a standard fashion; consistency is important for reliable user differentiation. A separate binary SVM classifier is trained to distinguish between correct and incorrect hand placements. This classifier uses the same feature set described in the previous section.

This classifier is exposed to users through a basic visualization. Our application starts with a grey screen with a suggestive handprint rendered on screen (Figure 2). Improper placements cause the screen to turn red, indicating the user should reposition their hand. The screen turns green when an acceptable handprint is detected.

Classifier Confidence

In our real-time classifier running on the phone, we use the binary classifier vote tallies to compute a confidence score for each class, outputting the class corresponding to the highest confidence score. In the event of a tie, the classifier outputs a null result meaning "not confident", after which the user interface will prompt the user to "try again".

RELATED WORK

Many systems in the literature aim to extract biometric data from touchscreens; see *e.g.*, Blažica *et al.* [1] for a survey. However, most such systems use camera-based setups to image the user's hand at high resolution, in contrast to our low-resolution capacitive image. Fiberio [5] uses a high-resolution camera to capture fingerprints. HandsDown [12] uses a diffuse-illumination interactive tabletop and hand contours for user identification (see *e.g.*, [7,11] for more discussion on hand geometry-based approaches). MTi [1] uses the coordinates of the five finger tips for user identification. Mock *et al.* [8] used an FTIR screen and blob-geometry analysis for user identification from typing.

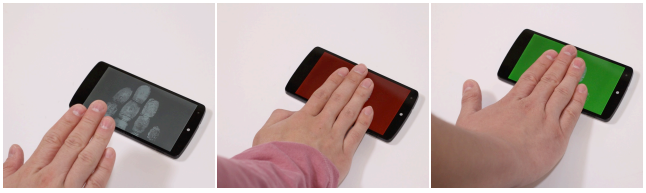

Figure 2. CapAuth classification. Left: initial state. Middle: unauthorized user (red). Right: authorized user (green).

Carpus [9] used a high-resolution overhead camera and the back of users' hands as identifiers. Capacitive Fingerprinting [4] used a special sensor attached to an infrared touch panel to measure the swept-frequency impedance of a user. Vu *et al.* [14] authenticated users on a capacitive touchscreen by using a finger-worn ring device to inject a pattern of false events onto the screen. Finally, "Biometric-Rich Gestures" [10] used five-finger touch gestures and movement of palm and fingertips for authentication. In contrast to these methods, our approach uses low-resolution commodity touchscreens found in nearly every "smart" device today, without needing user or device augmentation.

As discussed previously, we extend work presented in Bodyprint [6], which authenticated users via various body parts (*e.g.*, ear, fist, and hand grips) pressed against a conventional capacitive touchscreen. Compared with Bodyprint, we demonstrate improved accuracy (99.6% authentication precision with 5.5% false rejection rate), live classification, accuracy persistence and moisture robustness, all with more users (20 participants).

EVALUATION

We recruited 20 participants, gender balanced, with a mean age of 26.0. Our primary study consisted of five sessions of handprint data collection, each separated by a short break to avoid over-fitting to transient physical properties of the hand and repetitive (and thus similar) placement of the hand by the user. In total, the study took approximately 30 minutes and participants received $10 for their time.

Following a brief demonstration of proper hand placement on our Nexus 5 prototype, participants proceeded to record one session of data. Participants placed their right hand down onto the screen in a natural fashion and pressed the physical volume button (located on the side of the device) to record one handprint trial. Participants were asked to lift their hands from the screen between trials before replacing them, adding variety to the collected data. Fifty handprints were collected in each session. In total, four sessions were collected in the manner, producing 4000 handprint instances (20 participants × 4 sessions × 50 trials).

One additional and special session collected *improper* hand placements, which we use to train our "correct hand placement classifier". In this session only, users were instructed to put their hands on the screen in a way that did not match the onscreen guide. This produced 1000 improper handprints (20 participants × 1 session × 50 trials).

Thus in total, there was five data collection sessions. In the breaks between these sessions, participants were asked to perform an activity. After round one, they completed a survey. After round two, they traced an outline of their hand on paper. After round three, they completed another survey, and in the last break, they washed and dried their hands. We included this hand-washing step to see if altering the moisture level (and likely the capacitance) of the hands would affect classification.

We also asked 10 of our participants to return for a follow-up study several days later (3 female, mean age 25.2, mean gap of 8.0 days). Using *all* handprint data collected from procedure above (20 participants), our Nexus 5 was initialized with participant-specific authentication and identification classifiers. Each participant then collected handprints following the same procedure as before. However, this time, classification was performed in *real-time* on the phone for a "live" experimental result. Of note, the interface was the same as the first study, which lacked graphical feedback (thus preventing participants from adjusting their hand pose to match classification results).

RESULTS

Beyond immediate authentication and identification accuracies, we also designed our study to provide insights into a variety of peripheral questions relevant to our method.

Authentication

To assess authentication accuracy, we ran a simulation consisting of 1000 handprint-events for each of our 20 participants (*i.e.*, 20,000 rounds). In each round of the simulation, we randomly combined 3 (out of 4) sessions of data from each participant and used this to train an "authorized" class. At the same time, we used 3 randomly selected sessions of data from each of the remaining 19 participants for an "unauthorized" class. We then trained a binary classifier on this data. The unused session from each of the twenty participants was used for testing. Thus, the classifier was trained on 2850 negative and 150 positive instances, and tested on 950 negative and 50 positive instances.

Overall, our technique achieved twenty-participant authentication accuracies of 99.6% (SD=0.76%). More specifically, 94.5% of the time, the "authorized" participant was correctly logged into the system. And 5.5% of the time, the system falsely rejected that participant, which would prompt the user to "try again" in real world applications. On the other hand, an unauthorized user was falsely accepted only 0.1% of the time. See Table 1 for the confusion matrix.

Identification

To assess identification accuracy, we ran another 1000 round classification simulation. In each round, we randomly combined 3 (out of 4) sessions of data from each participant and used this as a training set. Each participant was labeled as a separate class (*i.e.*, a twenty-class classifier). The single unused session of data from all twenty participants was used for testing. We forced our classifier to make a best guess, even when it was "not confident". Overall, our technique achieved a mean twenty-participant identification accuracy of 94.0% (SD=2.7%); see Table 2.

Not Authenticated	Authenticated	←Classified as
99.9%	0.1%	Not Authenticated
5.5%	94.5%	Authenticated

Table 1. Confusion matrix for authentication simulations.

Small Groups

We also conducted a post hoc experiment simulating family units of size four. In each of the 1000 simulation rounds, we randomly picked 4 (out of 20) participants to form a "family", and constructed an identification classifier for that family. We randomly combined 3 (out of 4) sessions of data from each of the four family members and used this for training. The unused session of data for each member was used for testing the classifier.

Overall, our technique achieved four-participant identification accuracies of 98.2% (SD=3.95%). The histogram in Figure 3 shows the family member identification accuracy result as percentages of rounds (*i.e.*, simulated families). More than 40% of the families achieved 100% accuracy, and 90% of families achieved exceeded 95% accuracy.

Correct Hand Placement

To assess the accuracy of our hand placement classifier, we ran 1000 simulation rounds. In each round of the simulation, we chose a stratified sample consisting of 70% of correct and improper hand placements to use as training data. We then trained a binary classifier (*i.e.*, the classifier returned "correct" or "incorrect" hand placement as its output). The remaining (30%) data was used for testing the classifier. Overall accuracy was 99.7% (SD=0.15%), demonstrating robust rejection of incorrect hand placements, which is an important pre-check before attempting authentication or identification.

Hand Washing

In our user study, we asked participants to wash and dry their hands in the restroom before the last session. This was

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20
P1	99.5	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
P2	1.0	98.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0	0.0	0.0
P3	1.0	0.0	98.9	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
P4	1.0	0.0	0.0	98.5	0.0	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
P5	2.9	0.0	0.0	0.0	96.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.2	0.0	0.0	0.1	0.0
P6	11.5	0.0	0.0	0.0	0.0	87.6	0.0	0.0	0.2	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.1	0.0	0.5	0.0
P7	0.5	0.0	0.0	0.0	0.0	0.4	98.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.2	0.4	0.0	0.0	0.0	0.0
P8	2.6	0.0	0.0	0.0	0.0	0.0	0.0	97.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
P9	16.5	0.0	0.4	0.0	0.0	0.4	0.0	0.0	82.2	0.4	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
P10	1.7	0.0	0.0	0.0	0.0	0.8	0.0	0.0	0.0	97.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
P11	1.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	97.8	0.0	0.0	0.3	0.0	0.0	0.0	0.0	0.0	0.0
P12	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	97.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
P13	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	99.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
P14	1.0	0.3	12.1	0.0	0.1	0.0	0.0	0.2	0.1	0.0	0.5	0.0	0.1	85.7	0.0	0.0	0.0	0.0	0.0	0.0
P15	30.8	4.0	0.0	0.8	0.0	0.1	0.1	0.0	0.1	0.4	0.0	0.3	0.0	0.0	61.9	0.0	0.2	1.4	0.0	0.0
P16	5.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	93.4	0.4	0.3	0.0	0.0
P17	3.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0	95.9	0.0	0.0	0.0
P18	1.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0	1.2	0.0	0.0	0.0	97.0	0.0	0.0
P19	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	97.8	0.0
P20	0.2	0.0	0.0	0.4	0.0	0.0	0.0	0.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	99.1

Table 2. Confusion matrix for identification simulations.

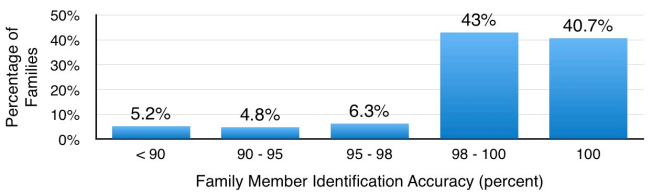

Figure 3. Histogram of family member identification accuracy.

included to see if altering the moisture of the hands would affect classification accuracy. Like our other experiments, we randomly combined 3 (out of 4) sessions of data from each participant, and used this as a training set. The unused sessions were used for testing.

For authentication, the accuracy for the session after hand washing (99.5%, SD=1.06%) had no significant difference in accuracy from the other three (pre-wash) sessions (99.7%, SD=0.52%). For identification, the accuracy for the session after hand washing is slightly worse: 91.7% (SD=20.9%) compared to 95.4% (SD=9.38%) for the pre-wash sessions, though this is not statistically significant.

Stability Over Time & Live Accuracy

As described previously, to study the robustness of classification over time, we invited ten of our participants to return after several days (mean gap of 8.0 days). We then evaluated authentication and identification accuracies "live" (trained using the data collected days earlier).

The new authentication accuracy was 98.0% (SD=2.62%), slightly down from 99.6%. However, identification accuracy was up: 96.5% (SD=4.70%) vs. 94.0% previously. Neither result was statically significant, suggesting that CapAuth may be stable overtime.

Questionnaire Data

We collected various demographic and qualitative information, including age, height, weight, and thirstiness to see if there was any affect on classification accuracy. We also computed a BMI estimate using this data. However, we found no significant correlations, though we warn that our participant pool is too small to draw any strong conclusions.

DISCUSSION AND CONCLUSION

Our results indicate that CapAuth is not well suited for high-security applications, nor use cases desiring user differentiation among large groups of users (*e.g.*, ten or more people). However, CapAuth can accurately identify users within smaller groups at 98.2% accuracy, such as families, suggesting its use as a simple user differentiation mechanism for shared devices where security is not paramount. This could be used to *e.g.*, provide parental control on a family tablet, or to enable tracking of individual users on a shared workspace touch table.

Similarly, authentication accuracies, even in large groups (20 or fewer people), is reasonably high (99.6% and 98.0% from our two studies). While acceptable for *e.g.*, family use, this result is still not sufficiently secure for security applications (which typically require accuracies in excess of 99.9%). However, even in high-security settings, CapAuth could prove useful as a two-factor authentication method.

Finally, one limitation of this technique is its potential susceptibility to environmental effects. Similar to the difficulty of detecting faces under varying illumination conditions, our system may not function as well under varying electrical conditions (*e.g.*, grounding to a charger, proximity to high-power electrical devices) as these could affect the capacitive image. Similarly, liquid on the screen (*e.g.*, raindrops) and certainly gloves, rings, watches and other accessories could affect accuracies.

ACKNOWLEDGEMENTS

This research was generously supported by Qualcomm, Google and the David and Lucile Packard Foundation.

REFERENCES

1. Blažica, B., Vladušič, D. and Mladenić, D. (2013). MTi: A method for user identification for multitouch displays. *Int. J. of Human-Computer Studies, 71*(6), 691-702.
2. Gutwin, C., Greenberg, S., Blum, R., Dyck, J., Tee, K. and McEwan, G. Supporting Informal Collaboration in Shared-Workspace Groupware. *J. UCS, 14*(9), 2008, 1411-1434.
3. Hall, M. *et al.* The WEKA Data Mining Software: An Update. *SIGKDD Explor.*, 11,1. 2009.
4. Harrison, C., Sato, M. and Poupyrev, I. Capacitive fingerprinting: exploring user differentiation by sensing electrical properties of the human body. In *Proc. UIST '12.* 537-544.
5. Holz, C. and Baudisch, P. Fiberio: A touchscreen that senses fingerprints. In *Proc. UIST '13.* 41-50.
6. Holz, C., Buthpitiya, S. and Knaust, M. Bodyprint: Biometric User Identification on Mobile Devices Using the Capacitive Touchscreen to Scan Body Parts. In *Proc. CHI '15.* 3011-3014.
7. Jain, A., Ross, A. and Pankanti, S. A prototype hand geometry-based verification system. In *Proc. AVBPA '99.* 166-171.
8. Mock, P., Edelmann, J., Schilling, A. and Rosenstiel, W. User identification using raw sensor data from typing on interactive displays. In *Proc. IUI '14.* 67-72.
9. Ramakers, R., *et al.* Carpus: a non-intrusive user identification technique for interactive surfaces. In *Proc. UIST '12.* 35-44.
10. Sae-Bae, N., Ahmed, K., Isbister, K. and Memon, N. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In *Proc. CHI '12.* 977-986.
11. Sanchez-Reillo, R., Sanchez-Avila, C., & Gonzalez-Marcos, A. (2000). Biometric identification through hand geometry measurements. *IEEE Trans. Pattern Anal. Mach. Intell.* 22(10), 1168-1171.
12. Schmidt, D., Chong, M. K. and Gellersen, H. HandsDown: hand-contour-based user identification for interactive surfaces. In *Proc. NordiCHI '10.* 432-441.
13. Stewart, J., Bederson, B. B. and Druin, A. Single display groupware: a model for co-present collaboration. In *Proc. CHI '99.* 286-293.
14. Vu, T., *et al.* Distinguishing users with capacitive touch communication. In *Proc. Mobicom '12.* 197-208.
15. Zheng, N., Bai, K., Huang, H. and Wang, H. You are how you touch: User verification on smartphones via tapping behaviors. In *Proc. IEEE ICNP '14.* 221-232.