User Authentication and Identification on Smartphones by Incorporating Capacitive Touchscreen

Mohamed Azard Rilvan
Department of Computer Science
Southern Connecticut State University
New Haven, CT
rilvanm1@southernct.edu

Kolby Isiah Lacy
Department of Electrical and Computer Engineering
Howard University
Washington, DC
kolby.lacy@bison.howard.edu

Md Shafaeat Hossain
Department of Computer Science
Southern Connecticut State University
New Haven, CT
hossainm3@southernct.edu

Bing Wang
Department of Electrical and Computer Engineering
University of Connecticut
Storrs, CT
bing@uconn.edu

***Abstract*—Smartphones, while providing users ease of access to sensitive information on the go, also present severe security risks if an attacker is able to gain access to them. To strengthen the user authentication and identification in a smartphone, we develop a biometric authentication and identification system which uses the capacitive touchscreen that is featured in all current smartphones. Our methodology focuses on using the touchscreen as a sensor to capture the image of a user's ear, thumb or four fingers. We extract the capacitive raw data from the touched body part to obtain a capacitive image, and then use it to capture geometric features (*e.g.,* length and width of a finger) and principal components. After that, we experiment with Support Vector Machine (SVM) and Random Forest (RF) classifiers to verify and also identify each user. We achieved the maximum authentication accuracy of 98.84% by four fingers with SVM, and maxinum identification accuracy of 97.61% by four fingers with RF.**

***Index Terms*—Biometric, authentication, identification, smartphones, capacitive touchscreen**

I. Introduction

There are currently over 2 billion smartphone users in the world. Because smartphones are now used for regular access to news, games, and private information, finding the best way to keep them secure from individuals that want to exploit this is a high priority. The goal is to make sure that whoever is in possession of the device is the owner, *i.e.,* identifying and authenticating a user. The most common forms of authentication for mobile devices are personal identification number (PIN) and password. A PIN, typically a four digit number, is considered to be weak since many people choose an easily guessable PIN in order to avoid forgetting it. A survey of four digit smartphone passcode conducted by [1] reveals that 1234, 0000, and 2580 are the top three passcodes which are among the 15% of total number of recorded passcodes. Another reason why a PIN is considered to be weak is because it is short and hence it can easily be leaked by shoulder surfing in a crowded place [11]. Similar to PIN, pattern passwords are also considered to be inadequate due to reasons such as users choosing easy to remember patterns for convenience and vulnerability to shoulder surfing.

Because of the above issues, researchers have suggested biometric based authentication. Fingerprint scanners and facial recognition are two types of biometric based authentication that have been implemented in newer phones. Facial recognition is not as convenient as other approaches. In addition, it may suffer from varying illumination conditions. Fingerprint scanners, on the other hand, are the most secure out of these techniques but they require additional hardware. Currently fingerprint scanners are inserted in a particular region of the phone which requires the user to scan their fingers into the home button on the front, sides of the phone or power button.

In this paper, we focus on capacitive touchscreen based authentication and identification. Unlike fingerprint scanners, this form of authentication/identification does not require additional sensors but instead utilizes the capacitive touchscreen that is currently in every smartphone. We use this capacitive touchscreen to extract capacitive values and create image of a body part from which we extract geometric features such as length and width of a finger, and principal components. We experiment with Support Vector Machine (SVM) and Random Forest (RF) to give an authentication/identification decision.

Capacitive touch screen technology is implemented in many smartphones and tablets and is an alternative to resistive touch screen technology. Capacitive screens work by detecting an additional amount of capacitance in the capacitors and registering a touch point. The screen is made up of an array of electrodes with a layer of glass acting as an insulator and as a dielectric [19]. When a person touches the screen, their

978-1-5090-5252-3/16/$31.00 2016 IEEE

finger becomes the second electrode. Each electrode is part of a proximity sensing device driven by alternating current (AC) signal. This signal emits a current through the screen capacitance which travels through the body capacitance and then comes back to the device through the case capacitance. The difference in potential from the screen capacitance to the case capacitance is measured and then is sent to the screen controller for processing.

The study [9] points out that one of the key benefits of using the touch screen to capture capacitance for user authentication is that the flat surface of the touchscreen provides a 1-1 mapping of the touched body part to the screen's sensor cells. Therefore this mapping would remain constant over the time and the dimensions of the touched body part will remain the same. Unlike camera based scanning, capacitive touchscreen does not require to take pictures from various angles or have concern of poor illumination conditions [14]. Most of the current smartphones come with larger touchscreen surface, which is more than four inches and hence provide the ability to scan ear, fingers and thumb.

We implemented our capacitive based authentication and identification system on a LG Nexus 5 smartphone running Android 5.0.1. We collected data from 21 participants, where each participant submitted 20 trials. Using SVM, we achieved authentication accuracies of 98.27%, 98.84%, and 97.70% for ear, four fingers, and thumb, respectively and identification accuracies of 82.73%, 87.50%, and 82.14% for ear, four fingers, and thumb, respectively. Using RF when the number of trees is 40, we achieved authentication accuracies of 98.15%, 98.24%, and 96.65% for ear, four fingers, and thumb, respectively and identification accuracies of 92.85%, 97.61%, and 74.40% for ear, four fingers, and thumb, respectively.

The rest of the paper is organized as follows. In Section II, we describe related work. In Section III, we explain our methodology. In Section IV, we describe the experimental setup and the analysis of our results. We conclude and give future directions in Section V.

II. Related Work

Beyond traditional approaches such as using password and PIN for user authentication, various other approaches have been investigated in the literature, including gait based ([6], [12], [20]) , behavioral [16], touch based ([4], [15], [21]), and capacitive based ([8], [9], [18]).

Gafurov *et al*. [6] have investigated gait based authentication, which is based around a person's way of walking and uses the accelerometers built in a mobile phone or on a separate device attached to a person as a means of identification by recognizing and classifying body motion. Gait is a more user friendly form of authentication because it only requires a user to walk to measure gait. However, this method is prone to many errors as a person may not always walk at the same pace or may even pause. Shi *et al*. [16] proposed a behavior based authentication system which relies on observation of the user's behavior through GPS or through interactions on a mobile device such as routes that are taken every day to work, calls to certain numbers, or application usage. [16] tested this by incorporating a scoring system in which actions that match the expected habit receive a good score, while actions that deviate from the expected receive a negative score. Once the score falls below a certain threshold the user is required to enter the pattern or PIN to the phone and the score is boosted to a certain score. Shen *et al*. [12] developed a method that implicitly authenticated a user based on the way that they unlocked the smartphone. They incorporated the motion sensor (accelerometer and gyroscope) by capturing data when a user was unlocking the phone while standing still, sitting, walking, or the phone was lying on top of a table. The results showed that this method could possibly be sufficient to use in a two-factor verification scenario. Attaullah *et al*. [4] created Touchstroke, which expands on the idea that uses the motion sensors as a way to classify the behavior of the user based on height, hand position, and movement through physical sensors as they input the password into the mobile device by adding a component that measures the timing of touch types. This addition provides an additional layer of security by noting that even if an adversary was able to mimic a users movement, they would also need to match the timing of the PIN input.

Three recent studies on capacitive based authentication are closely related to our work. Vu *et al.* [18] proposed a form of wireless communication called capacitive touch communication that can be used for user authentication on a smartphone. Specifically, a capacitive touch screen acts as a receiver and a small ring-like device (as a hardware identification token) acts as a transmitter. The hardware token transmits electrical signals on touch with the screen, either directly or indirectly through human skin. The authors experimented with injecting electrical signals that affected the capacitance measurement. This approach requires the users to wear the hardware identification token, while our approach does not need any additional hardware. Holz *et al*. [9] demonstrated how modified touch controller which captures human capacitance, could be used as sensors to authenticate a user as opposed to a fingerprint scanner. They used raw capacitance values to create an image of a user's ear, fist, fingers, or palm. Their algorithm includes three steps which are pre-processing, body part classification, and user identification. During pre-processing, the raw values are used to create a gray scale image. That image is then tested for features during the classification phase so that it can be recognized as one of the different images. In the final part, distance between images are calculated in order to identify and authenticate the user. Study [8] is an extension of the work done in [9]. Guo *et al*. decided to go with a hands flat pose so that they can extract more features, using a Nexus 5 smartphone running Android 5.0.1 and kernel modified to allow access to the Synaptics ClearPad 3350 touchscreen controllers interface. This interface allowed them to present the image on a 15×27 grid of pixels. From the capacitive image that was produced, they were able to extract features from users. From each image, they extracted a total of 550 features: each raw capacitance value as a feature, mean capacitance for each row and column, number of pixels with a value above

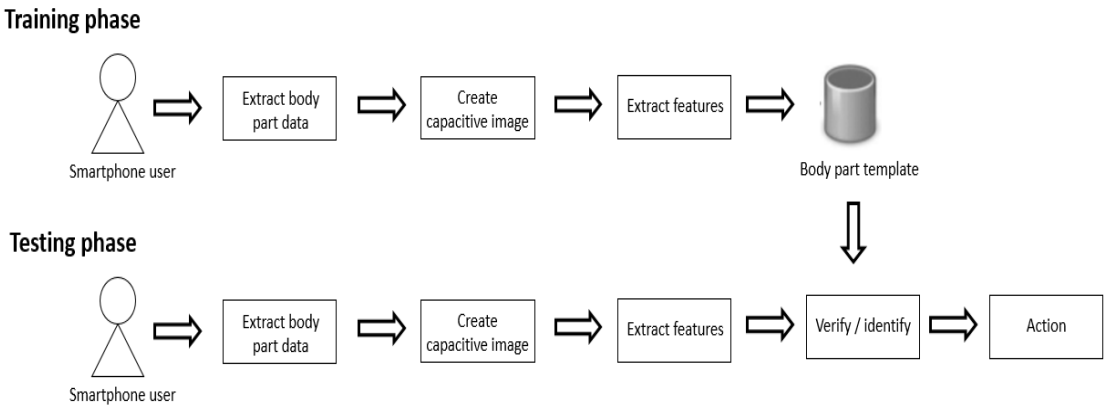


Fig. 1. Overview of user authentication/identification process.

15pF, sum of value for each finger, and various coordinate points. After feature selection, a subset of 150 features is used to train a support vector machine (SVM) classifier.

Our goal in this paper is to increase the accuracy of authentication and identification by using new geometric features and principal components of body part images (specifically, capacitive images of ear, thumb, and four fingers). Our study differs from ([8], [9]) in that we investigated using principal components as features for user authentication/identification, and demonstrated their benefits.

III. Methodology

Fig. 1 presents the overview of our user authentication and identification process. In the training phase, we extract body part data, create gray scale capacitive image, extract geometric features and principal components, and create body part templates. In the testing phase, similarly, we extract geometric features and principal components of the test samples and feed those features into a Support Vector Machine or Random Forest classifier to generate the verification/identification decision. Below, we describe several steps of Fig. 1 in more detail.

A. Capacitive Values Extraction

To extract capacitive values, kernel modifications are required. To modify the kernel we followed the tutorial described by [2], which provides the directions to modify the kernel to extract capacitive values for a smartphone running CyanogenMod.

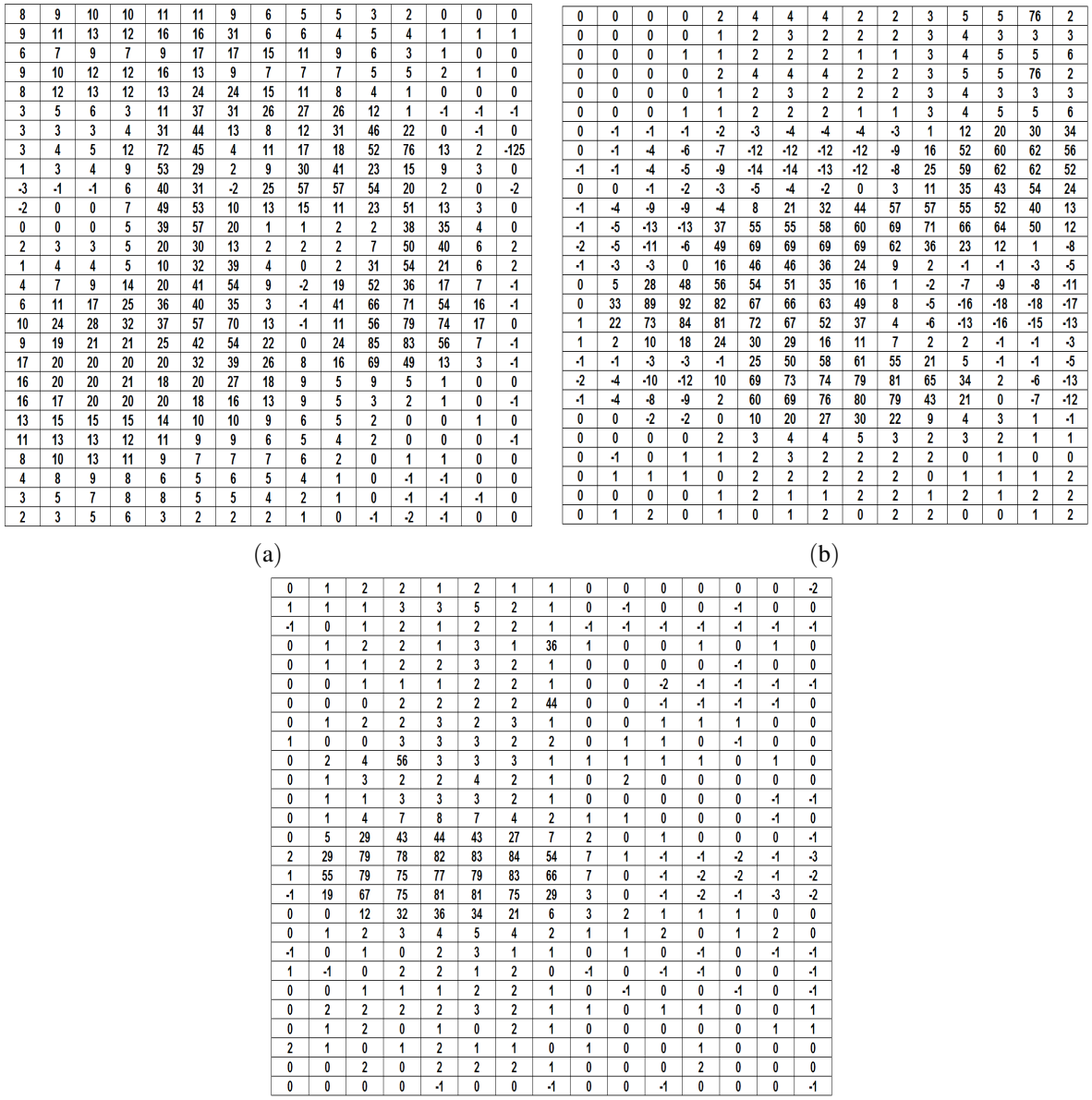
We implemented our capacitive based authentication and identification system on a LG Nexus 5 smartphone running Android 5.0.1. Nexus 5 contains a Synaptics ClearPad 3350 touchscreen controller, which follows a Register Mapped Interface (RMI) architecture. This interface is used to read and write the touch controller's registers which are 8 bit wide. Through rooting the Nexus 5 smartphone we gained access to RMI communications, to obtain the 8-bit 15×27 capacitive image at 30 frames per second (FPS). The address space of a register is divided into pages of related registers, where each page contains 256 registers. These registers hold data such as the touch position (x, y coordinates of the screen), and touch gestures (swipe, tap, scroll, *etc*.). The RMI contains a set of functions which defines the features of the touch controller. These functions are identified by an 8 bit integer. We use function 54 which allows to communicate with the I2C bus to record the capacitive values. To use function 54, we switch to register page 1, and get the data from function's get report command and read it to a 15×27 size matrix; and we switch back to the initial page which is page 0, so the touch function could recognize the touch gestures. Figures 2(a), (b) and (c) show an example of the 15×27 capacitive matrix for ear, four fingers, and thumb, respectively. A capacitive value less than 10 indicates an untouched part of the screen. Capacitive values that come from the sides of the body part are lower compared to those corresponding to the main area of the body part.

B. Creating Capacitive Images of Body Parts

After we extract the capacitive values from the touched body part, we compute an average frame of every 30 frames (which are extracted per second). We remove noise while computing the average frame. This average raw capacitive frame is then converted to a 15×27, 8 bit gray scale image. We normalize the capacitive values 0-255 range when we create the 8 bit gray scale image. Fig. 3 displays the 15×27 gray scale capacitive image created from the raw capacitive values. Visually, we can see the contours of the body parts, which will be used for feature extraction. We extract a body part image from the 15×27 gray scale capacitive image. The body part image is then resized to a 10×10 image.

C. Feature Extraction

We extract three geometric features: length, width, and area of a body part from each 15×27 gray scale capacitive image. The width of a row in a 15×27 body part image is the number of pixels that are greater than 0 in that row. The width of a body part image is the width of the widest row. Similarly, the length of a column in a 15×27 capacitive image is the number of pixels that are greater than 0 in that column. The length of



8	9	10	10	11	11	9	6	5	5	3	2	0	0	0
9	11	13	12	16	16	31	6	6	4	5	4	1	1	1
6	7	9	7	9	17	17	15	11	9	6	3	1	0	0
9	10	12	12	16	13	9	7	7	7	5	5	2	1	0
8	12	13	12	13	24	24	15	11	8	4	1	0	0	0
3	5	6	3	11	37	31	26	27	26	12	1	-1	-1	-1
3	3	3	4	31	44	13	8	12	31	46	22	0	-1	0
3	4	5	12	72	45	4	11	17	18	52	76	13	2	-125
1	3	4	9	53	29	2	9	30	41	23	15	9	3	0
-3	-1	-1	6	40	31	-2	25	57	57	54	20	2	0	-2
-2	0	0	7	49	53	10	13	15	11	23	51	13	3	0
0	0	0	5	39	57	20	1	1	2	2	38	35	4	0
2	3	3	5	20	30	13	2	2	2	7	50	40	6	2
1	4	4	5	10	32	39	4	0	2	31	54	21	6	2
4	7	9	14	20	41	54	9	-2	19	52	36	17	7	-1
6	11	17	25	36	40	35	3	-1	41	66	71	54	16	-1
10	24	28	32	37	57	70	13	-1	11	56	79	74	17	0
9	19	21	21	25	42	54	22	0	24	85	83	56	7	-1
17	20	20	20	20	32	39	26	8	16	69	49	13	3	-1
16	20	20	21	18	20	27	18	9	5	9	5	1	0	0
16	17	20	20	20	18	16	13	9	5	3	2	1	0	-1
13	15	15	15	14	10	10	9	6	5	2	0	0	1	0
11	13	13	12	11	9	9	6	5	4	2	0	0	0	-1
8	10	13	11	9	7	7	7	6	2	0	1	1	0	0
4	8	9	8	6	5	6	5	4	1	0	-1	-1	0	0
3	5	7	8	8	5	5	4	2	1	0	-1	-1	-1	0
2	3	5	6	3	2	2	2	1	0	-1	-2	-1	0	0

(a)

0	0	0	0	2	4	4	4	2	2	3	5	5	76	2
0	0	0	0	1	2	3	2	2	2	3	4	3	3	3
0	0	0	1	1	2	2	2	1	1	3	4	5	5	6
0	0	0	0	2	4	4	4	2	2	3	5	5	76	2
0	0	0	0	1	2	3	2	2	2	3	4	3	3	3
0	0	0	1	1	2	2	2	1	1	3	4	5	5	6
0	-1	-1	-1	-2	-3	-4	-4	-4	-3	1	12	20	30	34
0	-1	-4	-6	-7	-12	-12	-12	-12	-9	16	52	60	62	56
-1	-1	-4	-5	-9	-14	-14	-13	-12	-8	25	59	62	62	52
0	0	-1	-2	-3	-5	-4	-2	0	3	11	35	43	54	24
-1	-4	-9	-9	-4	8	21	32	44	57	57	55	52	40	13
-1	-5	-13	-13	37	55	55	58	60	69	71	66	64	50	12
-2	-5	-11	-6	49	69	69	69	69	62	36	23	12	1	-8
-1	-3	-3	0	16	46	46	36	24	9	2	-1	-1	-3	-5
0	5	28	48	56	54	51	35	16	1	-2	-7	-9	-8	-11
0	33	89	92	82	67	66	63	49	8	-5	-16	-18	-18	-17
1	22	73	84	81	72	67	52	37	4	-6	-13	-16	-15	-13
1	2	10	18	24	30	29	16	11	7	2	2	-1	-1	-3
-1	-1	-3	-3	-1	25	50	58	61	55	21	5	-1	-1	-5
-2	-4	-10	-12	10	69	73	74	79	81	65	34	2	-6	-13
-1	-4	-8	-9	2	60	69	76	80	79	43	21	0	-7	-12
0	0	-2	-2	0	10	20	27	30	22	9	4	3	1	-1
0	0	0	0	2	3	4	4	5	3	2	3	2	1	1
0	-1	0	1	1	2	3	2	2	2	2	0	1	0	0
0	1	1	1	0	2	2	2	2	2	0	1	1	1	2
0	0	0	0	1	2	1	1	2	2	1	2	1	2	2
0	1	2	0	1	0	1	2	0	2	2	0	0	1	2

(b)

0	1	2	2	1	2	1	1	0	0	0	0	0	0	-2
1	1	1	3	3	5	2	1	0	-1	0	0	-1	0	0
-1	0	1	2	1	2	2	1	-1	-1	-1	-1	-1	-1	-1
0	1	2	2	1	3	1	36	1	0	0	1	0	1	0
0	1	1	2	2	3	2	1	0	0	0	0	-1	0	0
0	0	1	1	1	2	2	1	0	0	-2	-1	-1	-1	-1
0	0	0	2	2	2	2	44	0	0	-1	-1	-1	-1	0
0	1	2	2	3	2	3	1	0	0	1	1	1	0	0
1	0	0	3	3	3	2	2	0	1	1	0	-1	0	0
0	2	4	56	3	3	3	1	1	1	1	1	0	1	0
0	1	3	2	2	4	2	1	0	2	0	0	0	0	0
0	1	1	3	3	3	2	1	0	0	0	0	0	-1	-1
0	1	4	7	8	7	4	2	1	1	0	0	0	-1	0
0	5	29	43	44	43	27	7	2	0	1	0	0	0	-1
2	29	79	78	82	83	84	54	7	1	-1	-1	-2	-1	-3
1	55	79	75	77	79	83	66	7	0	-1	-2	-2	-1	-2
-1	19	67	75	81	81	75	29	3	0	-1	-2	-1	-3	-2
0	0	12	32	36	34	21	6	3	2	1	1	1	0	0
0	1	2	3	4	5	4	2	1	1	2	0	1	2	0
-1	0	1	0	2	3	1	1	0	1	0	-1	0	-1	-1
1	-1	0	2	2	1	2	0	-1	0	-1	-1	0	0	-1
0	0	1	1	1	2	2	1	0	-1	0	0	-1	0	-1
0	2	2	2	2	3	2	1	1	0	1	1	0	0	1
0	1	2	0	1	0	2	1	0	0	0	0	0	1	1
2	1	0	1	2	1	1	0	1	0	0	1	0	0	0
0	0	2	0	2	2	2	1	0	0	0	2	0	0	0
0	0	0	0	-1	0	0	-1	0	0	-1	0	0	0	-1

(c)

Fig. 2. Samples of 15×27 raw capacitive matrices extracted from touch controller: (a) Ear, (b) Four fingers, (c) Thumb.

a body part image is the length of the longest column. The area of a body part image is calculated as the length of the body part times the width of the body part.

We did preliminary experiments only with the above three geometric features. However, the results were not satisfactory. With SVM the authentication accuracies were 65.19%, 67.79%, and 54.42% for ear, four fingers, and thumb, respectively. Then we applied PCA [17] on each 10×10 gray scale image to extract principal components, motivated by the successful results in several studies ([10], [7]) that apply PCA for face recognition. Principal components are the reduced dimensions which summarize and represent the entire image. We applied PCA with whitening. By applying PCA with whitening the correlation between the components are less and all the components have a similar variance. We jointly fed three geometric features and 20 principal components of each 10×10 image into the classifier. We used the Scikit-learn framework [13] to implement PCA, SVM, and RF. After we added principal components to our feature set, our results radically changed. We achieved authentication accuracies above 97% with SVM and above 96% with RF.

D. Authentication and Identification

We evaluate our methodology by running authentication and identification simulations. Through identification we distinguish a user using the captured body part from others. Identification claims an identity, while authentication is the act of verifying the identity. More specifically, authentication is

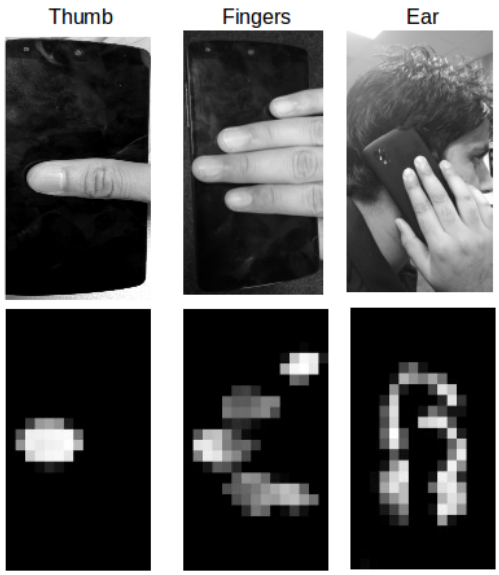


Fig. 3. 15×27 gray scale capacitive images created from the raw capacitive values. A body part image is extracted from each of these 15×27 capacitive images. The body part image is then resized to a 10×10 image which is used to extract principal components.

the process of determining that whether it is the actual user or an impostor; and identification is the process that seeks to gain knowledge about the subject and associates it with either a set of pre-defined or unknown identities [3]. For authentication simulations we use a binary classifier, and for identification simulations we label each user as a separate class.

We experiment with Support Vector Machine (SVM) and Random Forest (RF) classifiers in both authentication and identification. SVM and RF are standard machine learning classifiers used by several related research works and achieved very good performances ([8], [5]). SVM finds the optimal hyperplane that maximizes the minimal distance between the data sets and the hyperplane. In SVM, we used radial basis function (RBF) kernel because of its effectiveness in several machine learning applications. Random Forest is a meta learner which constructs decision trees on randomly selected samples. Each tree provides a classification and the forest selects the classification which contains the majority of the votes. For Random Forest we experimented with 10, 20, 30 and 40 trees.

E. Evaluation Metric

To evaluate the performance of our methodology, we generate confusion matrix and Receiver Operating Characteristic (ROC) curve for each of the authentication and identification simulations. From the confusion matrix, we calculate several performance measures, for example, accuracy, precision, false acceptance rate (FAR), and false rejection rate (FRR). The accuracy shows the proportion of the genuine and impostor predictions that are made correctly, and the precision shows the proportion of the genuine predictions that were made correctly. When a genuine user is predicted as an impostor, it is considered as false rejection (FR), while the opposite case when an impostor is predicted as a genuine user, it is considered as false acceptance (FA).

IV. Experiments and Results

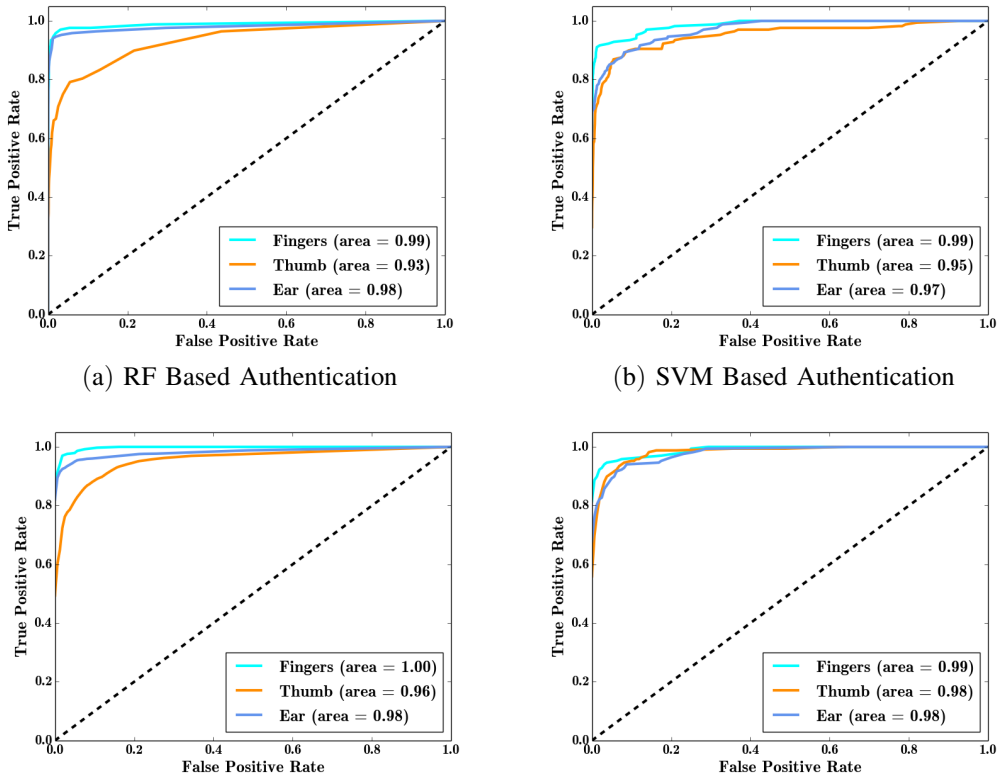
A. Data Collection

We collected data from 21 participants (16 being males and 5 being females) from the Southern Connecticut State University and the University of Connecticut. For each participant, after we demonstrated the body part placement we asked them to perform 20 trials for each body part in a single sitting, which took approximately 15 minutes. Overall we collected 420 trials for each body part. To record a sample, a participant placed his/her right thumb on the left center of the screen (for thumb), right four fingers as a flat position (for four fingers) or right ear on the center of the screen (for ear), as shown in Fig. 3. After a trial, a participant lifted his/her body part from the screen and then placed it on the screen again for the next trial.

B. Authentication Simulation

We ran authentication simulation for each type of body part (ear, thumb, or four fingers) separately. When authenticating one participant, the rest of the participants are considered as imposters. Consider authenticating one participant using one type of body part, specifically, ear. We have a total of 420 samples for ear (21 participants $\times$ 20 trials). The training set contains 60% of samples from each participant, and hence a total of 252 samples (60% $\times$ 20 trials $\times$ 21 participants), each marked with an annotation (indicating whether it is from the genuine user or an imposter user). The testing set contains the remaining 40% of samples from each participant, and hence a total of 168 samples (40% $\times$ 20 trials $\times$ 21 participants). Using the training set, we first learn classification models using SVM and RF, respectively. After that, we apply the classification model to the testing set for each of these two classifiers. The overall accuracy is the average of the authentication accuracy for all 21 participants. Applying a similar procedure, we obtain the authentication accuracy when using the other two types of body part (i.e., thumb and four fingers).

Tables I and II present the average performance of 21 participant authentication simulations for capacitive images of ear, four fingers, and thumb when using SVM and RF, respectively. We see that the performance of RF is insensitive to the number of trees that are being used. Using four fingers has achieved the highest accuracy compared to using ear or thumb for both SVM and RF. Though FARs and precisions of all body parts of RF seems to be better than SVM, the FRRs are much higher in RF than SVM. Figures 4(a) and (b) present the ROC curves obtained by RF based authentication and SVM based authentication, respectively. We achieve the maximum area under ROC curve (AUC = 0.99) by four fingers for both RF and SVM. We achieve the minimum area under ROC curve (AUC = 0.93) by thumb for RF.



(a) RF Based Authentication (b) SVM Based Authentication

(c) RF Based Identification (d) SVM Based Identification

Fig. 4. ROC Curves: (a) RF (40 trees) Based Authentication, (b) SVM Based Authentication, (c) RF (40 trees) Based Identification (d) SVM Based Identification.

TABLE I
PERFORMANCE OF SUPPORT VECTOR MACHINE (SVM) BASED AUTHENTICATION SIMULATIONS

	Four fingers	**Thumb**	**Ear**
Acc.	98.84%	97.70%	98.27%
Prec.	96.42%	89.23%	98.24%
FAR	0.27%	0.86%	0.06%
FRR	19.04%	30.95%	35.12%

C. Identification Simulation

Similar to authentication simulation, we ran identification simulation for each body part of a participant. Also, we randomly selected 12 samples which is 60% of the total samples of each body part of a person to create the training set. And, the rest 8 samples which is 40% of the total samples of a body part were used to create the testing set. We experimented with SVM and RF to classify 21 participants, where each participant was labeled as a separate class.

Tables III and IV present the average performance of 21 participant identification simulations for capacitive images of ear, four fingers and thumb for RF and SVM, respectively. RF experimented with 40 trees has achieved the best results for identification simulations of four fingers. Specifically, the FRR is 2.38% and the accuracy is 97.61%. The performance of RF improves when increasing the number of trees for all body parts. In Figures 4(c) and (d), we present the ROC

TABLE II
PERFORMANCE OF RANDOM FOREST (RF) BASED AUTHENTICATION SIMULATIONS FOR 10, 20, 30 AND 40 TREES

	Four fingers				**Thumb**				**Ear**			
	10	**20**	**30**	**40**	**10**	**20**	**30**	**40**	**10**	**20**	**30**	**40**
Acc.	98.44%	98.24%	98.27%	98.24%	96.57%	96.74%	96.65%	96.65%	97.87%	98.12%	98.01%	98.15%
Prec.	98.36%	96.74%	98.24%	98.64%	92.61%	98.35%	95.66%	97.35%	98.39%	90.03%	98.97%	99.05%
FAR	0.05%	0.02%	0.05%	0.02%	0.00%	0.00%	0.08%	0.02%	0.02%	0.00%	0.00%	0.00%
FRR	31.54%	36.30%	35.11%	36.30%	67.86%	68.45%	68.45%	69.64%	44.04%	39.28%	41.66%	38.69%

TABLE III
PERFORMANCE OF RANDOM FOREST (RF) BASED IDENTIFICATION SIMULATIONS FOR 10, 20, 30 AND 40 TREES

	Four fingers				Thumb				Ear			
	10	**20**	**30**	**40**	**10**	**20**	**30**	**40**	**10**	**20**	**30**	**40**
Acc.	90.47%	92.85%	95.23%	97.61%	66.07%	67.26%	70.83%	74.40%	84.52%	91.07%	91.66%	92.85%
Prec.	91.97%	93.41%	95.98%	97.88%	69.47%	71.29%	72.96%	76.80%	85.73%	92.74%	92.76%	94.25%
FAR	0.47%	0.35%	0.23%	0.11%	1.69%	1.63%	1.45%	1.28%	0.77%	0.44%	0.42%	0.35%
FRR	9.52%	7.14%	4.76%	2.38%	33.92%	32.73%	29.16%	25.59%	15.47%	8.92%	8.33%	7.14%

TABLE IV
PERFORMANCE OF SUPPORT VECTOR MACHINE (SVM) BASED IDENTIFICATION SIMULATIONS

	Four fingers	**Thumb**	**Ear**
Acc.	87.50%	82.14%	82.73%
Prec.	88.60%	83.85%	82.97%
FAR	0.62%	0.89%	0.86%
FRR	12.50%	17.85%	17.26%

curves obtained by RF based identification and SVM based identification, respectively. We achieve the maximum area under ROC curve (AUC = 1.00) by four fingers for SVM. We achieve the minimum area under ROC curve (AUC = 0.96) by thumb for RF.

D. Discussion

Our study indicates that for both authentication and identification, the accuracy achieved by using four fingers is higher than using thumb or ear. This is perhaps not surprising since each finger contains distinct features and when four fingers attached together, it lead to higher authentication and identification accuracies. The accuracy when using ear is slightly lower than when using four fingers, both are much higher than the accuracy when using thumb. We also observe that identification accuracies tend to be lower than authentication accuracies. This may be because the identification procedure considers a large number of classes (i.e., 21 in our scenario) while the authentication procedure only considers two classes. Investigating how to further improve identification accuracy is left as future work.

Compared to the results in [8] (which extends the study in [9]), our study achieves similar authentication accuracy. We did not run the algorithms in [8] on our dataset because [8] did not provide details on how features are being selected. The identification results of our study and [8] are not directly comparable since we classify over 21 participants while [8] considers a small group of participants. We will also investigate identification among a small group of participants (e.g., 4 participants as in [8]) in future work.

Our study has the following limitations. First, the number of participants is small and all participants are from a similar age group (our participants are 21 college students). Investigation of a larger population and other age groups may provide further insights on the effectiveness of our approach, which is left as future work. Secondly, our study does not consider the sensitivity of the proposed technique over time. As future work, as in [8], we are interested in collecting samples for participants at a later point of time, and investigate whether the classification accuracy is sensitive to time. Last, our study does not investigate the performance of our approach in the presence of environmental disturbances. Techniques based on capacitive touchscreen may be affected by environmental factors (e.g., other high-power electrical devices or sweat on hand). The sensitivity of our techniques to such environmental disturbances is left as future work.

V. CONCLUSION AND FUTURE WORK

To strengthen the user authentication and identification on a smartphone, we presented a capacitive touchscreen based biometric system which authenticates and identifies a user by capturing the capacitive values and generating a capacitive image of a touched body part. We used geometric features and principal components of the capacitive image and applied Support Vector Machine (SVM) and Random Forest (RF) classifiers to verify and also identify the users. Evaluation results show that our approach performs well across the data collected from 21 participants. With SVM, we achieved authentication accuracies of 98.27%, 98.84%, and 97.70% for ear, four fingers, and thumb, respectively and identification accuracies of 82.73%, 87.50%, and 82.14% for ear, four fingers, and thumb, respectively. With RF (40 trees), we achieved authentication accuracies of 98.15%, 98.24%, and 96.65% for ear, four fingers, and thumb, respectively and identification accuracies of 92.85%, 97.61%, and 74.40% for ear, four fingers, and thumb, respectively. Results show that the strength of capacitive based sensing to authenticate or identify a user is reasonably high.

As future work, we will investigate other machine learning algorithms and a larger dataset. We will also address the limitations described in Section IV D.

ACKNOWLEDGMENTS

The first two authors were funded by NSF sponsored Trustable Computing Systems REU program at the University of Connecticut (UConn). We would like to thank the anonymous reviewers for their insightful comments. We would also like to thank Shweta Ware (UConn) for her help with SVM.

REFERENCES

[1] "Most common iphone passcodes." [Online]. Available: http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes

[2] "Raincheck." [Online]. Available: https://ubicomplab.cs.washington.edu/raincheck/index.html

[3] S. P. Banerjee and D. L. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," *Journal of Pattern Recognition Research*, vol. 7, no. 1, pp. 116–139, 2012.

[4] A. Buriro, B. Crispo, F. Del Frari, and K. Wrona, "Touchstroke: smartphone user authentication based on touch-typing biometrics," in *International Conference on Image Analysis and Processing*. Springer, 2015, pp. 27–34.

[5] H. Drira, B. B. Amor, M. Daoudi, A. Srivastava, and S. Berretti, "3D dynamic expression recognition based on a novel deformation vector field and random forest," in *Pattern Recognition (ICPR), 2012 21st International Conference on*. IEEE, 2012, pp. 1104–1107.

[6] D. Gafurov, K. Helkala, and T. Søndrol, "Biometric gait authentication using accelerometer sensor," *Journal of computers*, vol. 1, no. 7, pp. 51–59, 2006.

[7] E. Gumus, N. Kilic, A. Sertbas, and O. N. Ucan, "Evaluation of face recognition techniques using PCA, wavelets and SVM," *Expert Systems with Applications*, vol. 37, no. 9, pp. 6404–6408, 2010.

[8] A. Guo, R. Xiao, and C. Harrison, "Capauth: Identifying and differentiating user handprints on commodity capacitive touchscreens," in *Proceedings of International Conference on Interactive Tabletops & Surfaces*. ACM, 2015, pp. 59–62.

[9] C. Holz, S. Buthpitiya, and M. Knaust, "Bodyprint: Biometric user identification on mobile devices using the capacitive touchscreen to scan body parts," in *Proceedings of ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 3011–3014.

[10] K. I. Kim, K. Jung, and H. J. Kim, "Face recognition using kernel principal component analysis," *IEEE signal processing letters*, vol. 9, no. 2, pp. 40–42, 2002.

[11] T. Kwon and J. Hong, "Analysis and improvement of a pin-entry method resilient to shoulder-surfing and recording attacks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 278–292, 2015.

[12] M. F. Nowlan, "Human identification via gait recognition using accelerometer gyro forces," *Yale Computer Science. http://www. cs. yale. edu/homes/mfn3/pub/mfn_gait_id. pdf (accessed November 12, 2013)*, 2009.

[13] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg *et al.*, "Scikit-learn: Machine learning in python," *Journal of Machine Learning Research*, vol. 12, no. Oct, pp. 2825–2830, 2011.

[14] P. J. Phillips, J. R. Beveridge, B. A. Draper, G. Givens, A. J. O'Toole, D. S. Bolme, J. Dunlop, Y. M. Lui, H. Sahibzada, and S. Weimer, "An introduction to the good, the bad, & the ugly face recognition challenge problem," in *International Conference on Automatic Face & Gesture Recognition*. IEEE, 2011, pp. 346–353.

[15] C. Shen, T. Yu, S. Yuan, Y. Li, and X. Guan, "Performance analysis of motion-sensor behavior for user authentication on smartphones," *Sensors*, vol. 16, no. 3, p. 345, 2016.

[16] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," in *International Conference on Information Security*. Springer, 2010, pp. 99–113.

[17] M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of cognitive neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.

[18] T. Vu, A. Baid, S. Gao, M. Gruteser, R. Howard, J. Lindqvist, P. Spasojevic, and J. Walling, "Distinguishing users with capacitive touch communication," in *Proceedings of international conference on Mobile computing and networking*. ACM, 2012, pp. 197–208.

[19] W. C. Westerman and J. G. Elias, "Capacitive sensing arrangement," Jul. 27 2010, US Patent 7,764,274.

[20] Y. Zhang, G. Pan, K. Jia, M. Lu, Y. Wang, and Z. Wu, "Accelerometer-based gait recognition by sparse representation of signature points with clusters," *IEEE Transactions on Cybernetics*, vol. 45, no. 9, pp. 1864–1875, 2015.

[21] N. Zheng, K. Bai, H. Huang, and H. Wang, "You are how you touch: User verification on smartphones via tapping behaviors," in *International Conference on Network Protocols*. IEEE, 2014, pp. 221–232.