Pre-Interaction Identification By Dynamic Grip Classification

Mohammad Faizuddin Mohd Noor*, Simon Rogers†1 and John Williamson†2

*Malaysian Institute of Information Technology
Universiti Kuala Lumpur
Kuala Lumpur, Malaysia
mfaizuddin@unikl.edu.my

†School of Computing Science
University of Glasgow
Scotland, United Kingdom
[1]Simon.Rogers@glasgow.ac.uk
[2]JohnH.Williamson@glasgow.ac.uk

ABSTRACT

We present a novel authentication method to identify users as they pick up a mobile device. We use a combination of back-of-device capacitive sensing and accelerometer measurements to perform classification, and obtain increased performance compared to previous accelerometer-only approaches. Our initial results suggest that users can be reliably identified during the pick-up movement before interaction commences.

CCS Concepts

•Computing methodologies → **Support vector machines; •Human-centered computing** → **Gestural input; •Hardware** → *Sensors and actuators;* **•Security and privacy** → Authentication;

Keywords

Back-of-device; capacitive; accelerometer; machine learning

1. INTRODUCTION

Reliable and unobtrusive measures for identifiying and authenticating users on mobile devices are of increasing important as such devices become pervasive in everyday life. The main goal of user authentication in smartphones is to ensure that only the rightful owner is granted access. Traditional authentication mechanisms such as personal identification numbers (PIN) and password have been widely used to protect from adversaries such as thieves and impostors. There are a number of reasons why securing personal data is of paramount importance on mobile devices. For instance, users are now able to read and send emails, take pictures, record videos, do on-line shopping, perform bank transactions and access cloud services using their device.

However, users are notoriously bad at producing and using secure passwords and guessing common combinations such as year of birth, car registration number is an effective strategy to break them. This effect is compounded on mobile devices, where the tendency for simple passwords is reinforced by the difficulty in entering text using a small keyboard or keypad. For example, even though some smartphones offer re-authentication facility after recovering from stand-by, users tend to disable this feature because the time taken to re-authenticate is very large in proportion to the time the task they are trying to do takes (e.g. to check email).

There are also cases where simple identification is more important that secure authentication, and heavyweight mechanisms such as passwords are inappropriate. For example, in a family where there is a single ebook reader shared among members of the family, if the user can be reliably identified, then the appropriate library of texts and current reading state can be restored. Requiring users to enter a password to identify themselves on each use would seriously impair the usability of the device.

Many new authentication mechanisms have been proposed to overcome the problems of the traditional PIN and password. On mobile devices, the use of onboard sensors for authentication has been of central interest; commercial devices now come with an array of rich sensors as standard (inertial sensors, microphones, cameras, touch sensors, pressure sensors, proximity sensors). Transparent biometric authentication use aspects of a user's physical make-up and characteristic features of a user's behaviour are used as identifiers. These identification methods identify users as they engage in their primary task, without requiring specific actions directed at authentication.

In this paper we present a preliminary study on the use of touch and inertial sensing data for authentication techniques that can be used as a device is picked up; identification occurs before a user begins the first interaction with the device, so that it becomes a truly transparent process. We show that a combination of accelerometer and back-of-device capacitive touch sensors can reliably identify users before they have finished picking up the device.

2. RELATED WORK

The use of gestural motion in building identification system has been widely studied over the past decade. This approach is especially applicable to mobile devices due to their small size and limited interaction capabilities and the wide availability of standard sensing hardware in mobile platforms. Gesture based identification in mobile device has a long history in HCI [5, 8, 1].

Previous work has specifically shown that a user can be authenticated while performing a specific action such as when placing or answering a call [4]. This approach suggests that every user has a unique motion signature when placing or answering phone call. [4] used a Dynamic Time Warping similarity algorithm comparing accelerometer timeseries of users' hand movement data while placing or answering a call, and achieved False Acceptance Rates (FA) of 2.5% and False Rejection Rates (FR) of 8%.

Other studies demonstrated that valuable context information can be obtained from the grip pattern of a mobile devices. Kim et al. [10] demonstrated a technique to recognise grip patterns associated with several common mobile tasks such as making a call, text messaging and playing games. These techniques used a capacitive sensor film attach underneath the mobile phone housing to capture the grip data. Besides the capacitive sensor, they also investigated whether movement data acquired using a 3-axis accelerometer, is useful in the recognition process. They used Naive Bayes, Minimum Distance Classifier (MDC) and Support Vector Machines (SVM) classifier to perform the recognition. Their technique yielded promising results with classification accuracy of above 90% in classifying intended task using both capacitive and accelerometer data. The use of capacitive sensor also been successful in recognising grasp in tangible interfaces by measuring the way people hold and manipulate the object rather than discriminating the way people grasp an object [15, 16].

Besides capacitive sensors, previous work has also shown that users can be identified using the pressure applied while holding or gripping an object. The Smart Gun project, for instance, has used a piezo-resistive sensor sheet embedded in the grip of a prototype gun to measure the static pressure of the hand-grip when the gun is being held in order to identify its owner [13]. They used Support Vector Machines (SVM) and Likelihood-Ratio Classifier (LRC), and reported their technique to have an Equal Error Rate (ERR) average of 3.5% using LRC and 5.7% using SVM. While this result may not be sufficient for guns, which are only ever used in life threatening situations, this technique could be adapted to work with mobile devices where performance is less critical. In [3], the use of grip pressure sensor has shown to be able to differentiate between car drivers from the way they grasp and grip the steering wheel.

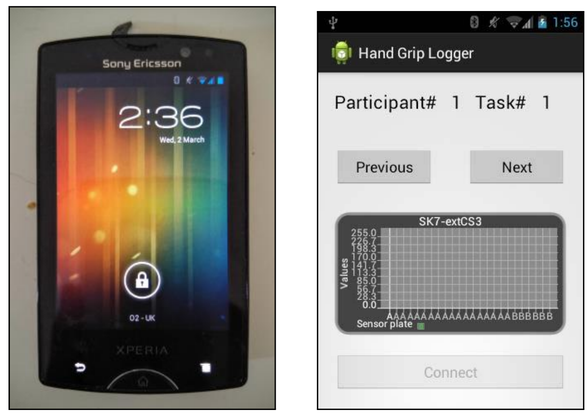
3. EXPERIMENT

We are interested in investigating whether dynamic sensing of grip contact can aid in the identification of users during the call answering process. To do so, we recreated Conti et. al. [4]'s experiment [4] by adding back-of-device (BoD) hand grip information. In particular, we are interested in investigating whether dynamic sensing of grip contact can aid in the identification of users during the call answering process. Furthermore, this also allows us to compare performance between hand grip and hand movement methods as well as to investigate if performance gain can be achieved if both inputs are used to build the identity predictor.

In order to capture hand grip contact we developed a prototype system which consists of a Sony Xperia Mini Pro (SK7i) smartphone connected via Bluetooth to a SHAKE SK7 sensor pack (see Figure 3)[1] that interfaces an external array of 24 capacitive sensors that detect proximity of the hand to the rear and sides of the case. Apart from BoD sensors, the SK7 is also equipped with various other sensors, including accelerometer, gyroscope and magnetometer. The total size of this prototype is 25 mm (H) x 150 mm (L) x 65 mm (W). The prototype is shown in Figure 1.

The 24 capacitive sensor values (with 8 bit dynamic range) and 3 accelerometer values (in the $\pm 2g$ range, with 12 bit dynamic range) were transmitted from the SK7 to the phone via Bluetooth with a sample rate of 50 Hz. An application was developed on the phone to perform the experiment and record the data for subsequent offline analysis.

3.1 User study



(a) Sony Xperia Mini Pro (b) Logging application

Figure 2: (a) Sony Xperia Mini Pro (b) Screenshot of data logging application.

Figure 3: SHAKE SK7 sensor pack

For this study, 12 participants consisted of 6 males and 6 females, aged between 25 and 35 years old (mean=26.91, sd=2.15) were recruited locally after formal ethical approval been granted. Each participant recorded data over 6 separate sessions, 3 with their left hand and 3 with their right. Each left/right session was separated by a 3-minute break to minimise repetition effects – a condition where users becoming skilled after making similar action repetitively [11]. Therefore by separating the task into sessions, we are not capturing only a single hand grip/movement pattern but a range of plausible hand grip patterns.

[1]http://code.google.com/p/shake-drivers/

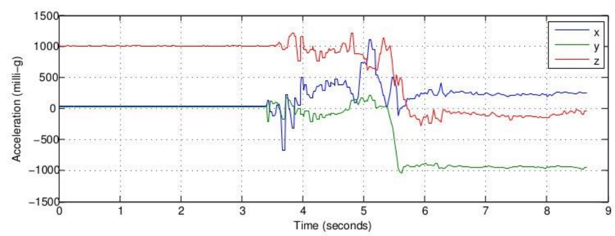
(a)

(b)

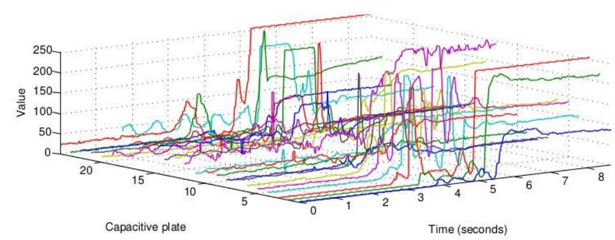
Figure 1: Individual component of the prototype (b) when fully-assembled (SHAKE SK7 is hidden underneath the front cover).

To acquire sensor data, we developed an Android application on the Sony Xperia Mini Pro smartphone (see Figure 2). The application communicates with another application that we wrote on a PC to trigger a phone call on the smartphone. This allows us to coordinate the data acquisition process without the need to rely on the real GSM network. The BoD sensors were calibrated prior to every data acquisition session. This was done using simple two-point calibration of the capacitive sensors, that is by measuring untouched and touched each sensor's capacitance values.

Each session required the participants to perform 10 answering actions while seated in front of a desk. Each action started with the phone ringing. On hearing this, the user picked up the phone (with whichever hand they were using in this session) and lifted the phone to the same ear (i.e. if a right-hand session, the phone was lifted to the right ear). They were then asked to hold the phone there for at least 3 seconds. Data logging started when the phone rang and finished when the phone vibrated. From each call answering action, we recorded timestamps, acceleration along *x, y* and *z*-axis and 24 BoD capacitive sensor values. All data were stored in the external storage of the phone for subsequent offline analysis. Examples of recorded signals for one call answering action can be seen in Figure 4.



(a) Accelerometer



(b) BoD

Figure 4: Signals from accelerometer and BoD for one phone answering action using right hand selected randomly from one user.

3.2 Analysis methods

Similar to the approach proposed by Conti et. al. [4], we used classifiers to identify to which group (authorised/non-authorised) the observation (phone answering action) belongs to. This represents a standard setting where some training data from a particular user would be compared with a pooled set of training data from other users.

We began by pre-processing our data by converting the time series into fixed length feature vectors. This was done by first removing the empty signal at the beginning (data logged between the phone ringing and the users' first touch) by deleting all data until the total output from the capacitive sensors reached 150 which is approximately 3 seconds after the trial starts (flat section of the timeseries in Figure 4).

The remaining data for each sensor was then split into K equal length blocks and the mean value of the sensor within this block was extracted as a feature. For example, for $K = 6$, each sensor time series would be converted into $K = 6$ mean values, resulting in a total of $24 \times 6 = 144$ capacitive features and $3 \times 6 = 18$ accelerometer features. All features were normalised to have mean zero and standard deviation one prior to the next step of analysis.

3.3 Classification

Metrics	1	2	3	4	5	6	7	8	9	10	11	12	Mean
	Participants												
AUC													
$Right_{cap}$	0.96	1.00	0.88	1.00	0.96	0.96	1.00	1.00	0.94	1.00	1.00	1.00	**0.97**
$Left_{cap}$	1.00	1.00	1.00	1.00	1.00	0.95	1.00	0.91	0.95	1.00	1.00	1.00	**0.98**
$Right_{acc}$	0.95	1.00	0.96	1.00	1.00	0.95	1.00	0.87	0.89	1.00	0.98	0.99	**0.97**
$Left_{acc}$	0.71	1.00	1.00	0.83	1.00	0.95	0.99	0.90	0.94	0.95	1.00	1.00	**0.94**
Accuracy													
$Right_{cap}$	0.97	1.00	0.93	0.97	0.99	0.93	0.98	1.00	0.90	1.00	1.00	1.00	**0.97**
$Left_{cap}$	1.00	1.00	0.97	0.99	1.00	0.92	1.00	0.99	0.93	0.98	1.00	1.00	**0.98**
$Right_{acc}$	0.94	0.88	0.98	0.99	0.99	0.84	0.99	0.83	0.83	1.00	0.96	0.91	**0.93**
$Left_{acc}$	0.66	1.00	0.97	0.84	1.00	0.89	0.98	0.87	0.88	0.89	1.00	1.00	**0.91**
FRR													
$Right_{cap}$	0.30	0.00	0.20	0.00	0.10	0.10	0.00	0.40	0.30	0.00	0.10	0.00	**0.11**
$Left_{cap}$	0.00	0.00	0.20	0.00	0.00	0.00	0.00	0.10	0.00	0.20	0.00	0.00	**0.04**
$Right_{acc}$	0.10	0.00	0.20	0.00	0.10	0.10	0.00	0.40	0.30	0.00	0.10	0.00	**0.93**
$Left_{acc}$	0.30	0.00	0.00	0.70	0.00	0.00	0.10	0.10	0.10	0.50	0.00	0.00	**0.15**
FAR													
$Right_{cap}$	0.00	0.00	0.05	0.04	0.00	0.07	0.00	0.00	0.11	0.00	0.00	0.00	**0.02**
$Left_{cap}$	0.00	0.00	0.01	0.01	0.00	0.09	0.00	0.00	0.07	0.00	0.00	0.00	**0.02**
$Right_{acc}$	0.05	0.14	0.00	0.01	0.00	0.16	0.01	0.14	0.15	0.00	0.04	0.10	**0.07**
$Left_{acc}$	0.35	0.00	0.04	0.09	0.00	0.12	0.01	0.14	0.12	0.06	0.00	0.00	**0.08**

Table 1: Comparison of performance for left and right hands with capacitive sensors alone, and accelerometer alone. The performance metrics are AUC, accuracy, false reject rate (FRR), false accept rate (FAR).

The goal of authentication in this study is to classify user of interest from the rest of users in our dataset. This is essentially a binary classification problem where we define data from user of interest as positive class and the rest of the user as negative class. To perform classification, we have used SVM classifier provided by MATLAB libSVM toolbox [2]. In all experiments, the data are split into independent training and test sets. Here we use both first and second session as training set and the third session as test set.

Support Vector Machine (SVM) is a discriminative classifier formally defined by a separating hyperplane that is, given labeled training data, SVM outputs an optimal hyperplane that categorises new unseen data [14] The use of SVM in solving user identification problem is prevalent and this is justified by their previous use in [6, 12, 10] and their general state-of-the-art performance for data classification (in particular for large numbers of features, as is the case here). Gaussian (rbf) kernel functions was used throughout this study with the following form:

$$K(\mathbf{x}_1, \mathbf{x}_2) = \exp\left(-\frac{\gamma}{D}\sum_{d=1}^{D}(x_{1d} - x_{2d})^2\right)$$

where x_{nd} is the d-th feature of the n-th object (the data derived from the n-th pick-up action) and D is the total number of features.

Because of the large discrepancy in number of features between the capacitive and acceleration features, separate kernels were built for each. Putting them into the same kernel would make it difficult to assess the relative contribution to performance from each data type, and would also possibly result in the influence of the acceleration features being drowned out by the larger number of capacitance values. When using both feature types, the kernels were combined additively (for a review of multiple kernel learning, see e.g. [7]) as follows:

$$K = aK_{accelerometer} + (1 - a)K_{BoD}$$

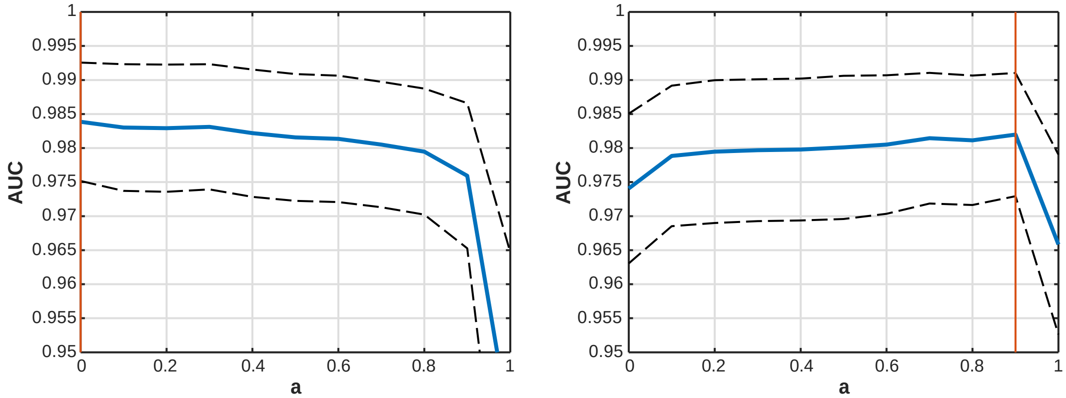
where $0 \leq a \leq 1$ with 0 represents only BoD capacitive kernel and 1 represents only accelerometer kernel. This is guaranteed to produce a correct (i.e. symmetric, positive, semi-definite) kernel, K.

In all SVM models, 2 kernel parameters C and γ need to be optimised with an additional kernel weight parameter a when using multiple kernel learning. Here all parameters were selected via k-fold cross-validation on the respective training data set using logrithmic grid-search. The parameters are then chosen based on the highest classification accuracy given by C and γ combination. Similarly, parameter a is selected based on the best C and a combination, where a ranging from 0 to 1. It is worth mentioning that prior to all experiments, all features were centered to have mean 0 and scaled to have standard deviation 1 to avoid numerical instability.

4. RESULT

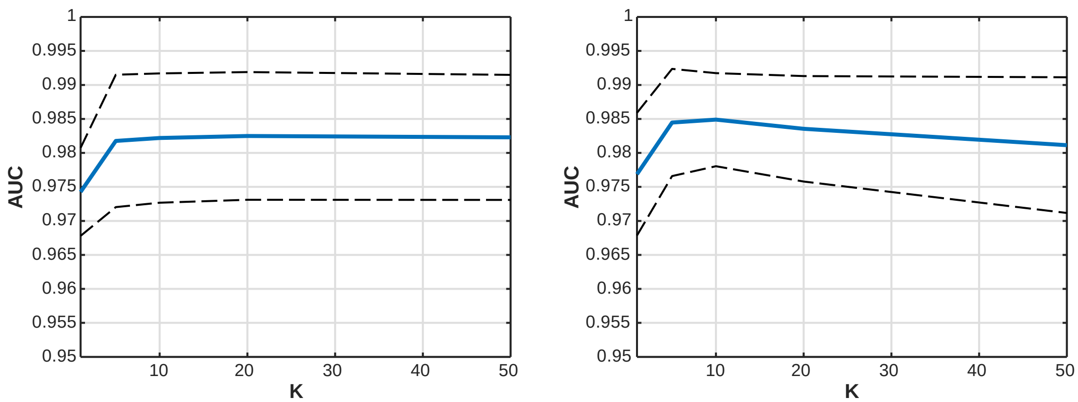
Classification task in the context of this study is a binary classification problem where the goal is to identify user of interest from a pool of users. In all experiments, we compare the results for both accelerometer and back-of-device from both tasks. We use Area Under the Curve (AUC) along its respective False Accept, False Reject and Error Equal rates to estimate the performance of classifiers. Baseline is computed by randomising the test data labels and we use random subsampling method to balance between positive and negative classes.

False Accept Rate (FAR) and False Reject Rate (FRR) are two measures widely used in to evaluate performance of authentication system. False Accept Rate is a fraction of unauthorised user being misclassified as rightful user whereby False Reject Rate is a fraction of rightful user being mis-



(a) Left (b) Right

Figure 5: Classification performance (AUC) averaged across users including ± standard error as the kernel weighting parameter is varied from just capacitive data (left, $a = 0$) to just accelerometer data (right, $a = 1$). Solid vertical red lines correspond to the optimal a value.



(a) Left (b) Right

Figure 6: Classification performance (AUC) averaged across users including ± standard error, as the number of blocks is varied from static ($K = 1$) to dynamic ($K = 50$). Performance plateaus appears at $K = 6$ for both hands.

classified as unauthorised user. Error Equal Rate (EER) on the other hand indicates that the proportion of false acceptances is equal to the proportion of false rejections. Ideally, the lower of these values, the higher the accuracy of the authentication system.

We begin by reporting the performance of the classifier in distinguishing between a particular user and data from all other users. To identify a user, we used a One-vs-All (OVA) classification strategy where we treat data from a particular user (user of interest) as belonging to the positive class and data from the other 11 users as belonging to the negative class. To train the classifiers, we used 20 samples for the user of interest taken from the first two sessions and 80 random samples from other users also from the first two sessions. To test, we used 10 samples from the user of interest from session 3 and 80 random samples from session 3 of other users. This is to reflect the typical phone use case where calibration data is collected at some point (sessions 1 and 2) and then the user uses the phone sometime in the future (session 3).

4.0.1 One-vs-All

In all SVMs, the margin parameter C was set to 10^3 (making this a hard-margin SVM [14]). The kernel parameter γ was set through a Leave-One-Out Cross Validation (LOOCV) procedure on data for each user (from the first two sessions of a particular hand) and 20 random samples drawn from the other eleven users (with the same hand). We use area under the ROC curve (AUC), accuracy and false accept rate (FAR) which is the proportion of misclassifying a sample from another user as coming from the user of interest, and false reject rate (FRR) which is the proportion of misclassifying a sample from user of interest as coming from another user. To compute statistical significance of results, we use the non-parametric Wilcoxon Signed Rank Test with threshold of 0.05. In all classifications, $K = 6$ blocks were used.

Classification results for each user are shown in Table 1. From the table, we see that performance is typically high (AUC > 0.9). In general the capacitive models slightly outperform those trained on accelerometer data – indicated by higher accuracy and a lower number of false rejects and false accepts.

4.0.2 Composite input

To investigate whether combining two sensor inputs could improve the performance of the individual sensor spaces we used a composite kernel as described previously. Figure 5 shows classification AUC as a function of a, the kernel weighting parameter. Note that $a = 0$ corresponds to just capacitive sensing and $a = 1$ to just accelerometer sensing. For left hand the curve decreases gradually as a increases up to $a = 0.9$ before decreasing as a approaches 1. For right hand, the AUC curve increases gradually from $a = 0$ to $a = 0.1$ and gradually increasing up to $a = 0.9$ before the AUC drops when the kernel contains only accelerometer data ($a = 1$). Whilst sensor combination for left hand shows no performance improvement (highest AUC is given by $a = 0$), the right hand however shows that the gain can be achieved through sensor combination, however the gain is not statistically significant.

From the results, it suggests that classifiers constructed using combination of capacitive and accelerometer data could give better performance, particularly when using right hand data (optimal $a = 0.9$). This indicates that the capacitive and accelerometer data contribute independent information about user identity.

4.0.3 Feature dimension

Finally, in Figure 6 we show how the classification performance varies as we increase the number of blocks (K) which is the fixed length segmentation of the timeseries where the feature is extracted, from 1 to 50. This is based on combining both data types, with the optimal value of a from Figure 5. The performance increases rapidly and then plateaus before dropping slowly as K is increased. This is to be expected – simply taking the mean for each sensor over time ($K = 1$) is unlikely to be optimal. Similarly, increasing K above some value is likely to result in different parts of the answering action ending up in different blocks (and hence different features) for examples from the same person, causing a slight decrease in performance.

4.1 Discussion

Although we managed to achieve mean classification AUC and accuracy of all above 0.9, it should be noted that the sample size here (12 participants) is too small for us to be able to make comments as to how this technique might work in an actual implicit identification system. Nevertheless, it does allow us to compare classification performance between accelerometer and capacitive sensors.

In One-v-All classification setting, it shows that users can be identified with similar level of performance using hand grip and motion data. This suggests that both sensors can be used interchangeably to identify users' unique hand grip and motion patterns from the phone pick-up action. This can be useful in some phone answering scenarios such as answering while walking/on the move where hand grip is more consistent compared to hand motion. Moreover the results also show that the performance for right and left hands are nearly similar suggesting that this technique may generalise for right and left handed users.

The phone answering tasks that we used in this study were constrained to only two pick-up motions: picking-up with the right hand and bringing it to the right ear and picking-up with the left hand and bringing it to the left ear. It is therefore interesting to explore how other possible pick-up motions (e.g. picking up the phone using left hand and bringing it to the right ear) would impact the classification performance.

Despite improving performance when using composite classifiers, the mean improvement however was marginal and not statistically significant. This indicates that the addition of hand grip or hand motion information to the kernel may not necessary lead to an improvement. Nevertheless, from Figure 5, it is clear that single kernel classifiers could already produce very high classification AUC using either hand grip or hand motion data and thus composite classifiers might not be needed.

5. CONCLUSION

In this work, we investigated whether hand grip sensed via BoD capacitive sensors can be used to distinguish users. We chose user distinguishing methods based on 1) hand movement [4] as direct comparison. We recreated the experiments used by both methods and augmenting them with hand grip input. Our results show that hand grip contains valuable information that can be used to distinguish users.

In our experiment, we collected phone pickup action from 12 participants using a prototype mobile phone. From this, we extracted 3 features from the accelerometer input and 24 features from the BoD input. We then trained user classifiers using Gaussian RBF kernel SVM for each input and combination of both. We clearly show that a combination of BoD grip sensing and accelerometer motion signatures can be used to identify users in the few seconds between making contact with a device and lifting it to interact.

BoD sensors may not yet mainstream presently, however some commercial devices (e.g. the Doogee DG800 or the Oppo N1) already provide BoD touch sensors to enhance touchscreen interaction. These sensors may have sufficient resolution to capture hand grip for identification purposes. We anticipate BoD sensors with wider sensing surface to be included in commercial devices in the near future to allow grip-based interaction such in [9] which can be effectively used for grip-based implicit authentication.

In summary, these results form a concrete contribution to building a rich, multi-sensor mobile phone identification system. While hand grip alone may be insufficient to perform secure authentication, it can form part of an array of contributing virtual sensors in a hybrid continuous authentication system or as a lightweight identification model. The performance obtained in our experiments also suggest that these techniques could be readily applied to non-critical identification tasks (such as user identification with communal devices like remote control) or could feed into a larger authentication system as evidence for user identity.

6. REFERENCES

[1] A. Akl, C. Feng, and S. Valaee. A Novel Accelerometer-Based Gesture Recognition System. IEEE Transactions on Signal Processing, 59(12):6197–6205, dec 2011.

[2] C.-C. Chang and C.-J. Lin. LIBSVM. ACM Transactions on Intelligent Systems and Technology, 2(3):1–27, apr 2011.

[3] R. Chen, M. F. She, X. Sun, L. Kong, and Y. Wu. Driver recognition based on dynamic handgrip pattern

on steeling wheel. Proceedings - 2011 12th ACIS International Conference on Software Engineering, Artificial Intelligence Networking and Parallel Distributed Computing, SNPD 2011, pages 107–112, jul 2011.

[4] M. Conti, I. Zachia-Zlatea, and B. Crispo. Mind how you answer me!: transparently authenticating the user of a smartphone when answering or placing a call. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pages 249–259, 2011.

[5] E. Farella, S. O'Modhrain, L. Benini, and B. Riccó. Gesture signature for ambient intelligence applications: a feasibility study. Pervasive Computing, pages 288–304, 2006.

[6] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication. IEEE Transactions on Information Forensics and Security, 8(1):136–148, jan 2013.

[7] M. Gönen and E. AlpaydÄśn. Multiple Kernel Learning Algorithms. Journal of Machine Learning Research, 12:2211–2268, 2011.

[8] J. Guna, I. Humar, and M. Pogacnik. Intuitive gesture based user identification system. 2012 35th International Conference on Telecommunications and Signal Processing (TSP), pages 629–633, jul 2012.

[9] Y. Higuchi and T. Okada. User Interface Using Natural Gripping Features. NTT Docomo Technical Journal, 15(3):17—-24, 2014.

[10] K. Kim, W. Chang, S. Cho, and J. Shim. Hand grip pattern recognition for mobile user interfaces. IAAI'06 Proceedings of the 18th conference on Innovative applications of artificial intelligence, 2:1789–1794, 2006.

[11] G. D. Logan. Repetition priming and automaticity: Common underlying mechanisms? Cognitive Psychology, 22(1):1–35, jan 1990.

[12] A. Serwadda and V. V. Phoha. When kids' toys breach mobile phone security. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13, pages 599–610, New York, New York, USA, 2013. ACM Press.

[13] X. Shang and R. Veldhuis. Grip-Pattern Recognition in Smart Gun Based on Likelihood-Ratio Classifier and Support Vector Machine. Image and Signal Processing, pages 289–295, 2008.

[14] N. Shawe-Taylor, John and Cristianini. Analysis, Kernel methods For Pattern Analysis. Cambridge University Press, 2004.

[15] B. T. Taylor and V. M. Bove. The bar of soap: a grasp recognition system implemented in a multi-functional handheld device. Proceedings of ACM CHI 2008 Conference on Human Factors in Computing Systems, 2:3459–3464, 2008.

[16] Wimmer and Boring. HandSense: discriminating different ways of grasping and holding a tangible user interface. Proceedings of TEI 2009, pages 16–19, 2009.