Enabling Finger-touch-based Mobile User Authentication via Physical Vibrations on IoT Devices

Xin Yang, *Student Member, IEEE*, Song Yang, *Student Member, IEEE*, Jian Liu, *Member, IEEE*, Chen Wang, Yingying Chen, *Fellow, IEEE*, and Nitesh Saxena, *Member, IEEE*

Abstract—This work enables mobile user authentication via finger inputs on ubiquitous surfaces leveraging low-cost physical vibration. The system we proposed extends finger-input authentication beyond touch screens to any solid surface for IoT devices (e.g., smart access systems and IoT appliances). Unlike passcode or biometrics-based solutions, it integrates passcode, behavioral and physiological characteristics, and surface dependency together to provide a low-cost, tangible and enhanced security solution. The proposed system builds upon a touch sensing technique with vibration signals that can operate on surfaces constructed from a broad range of materials. New algorithms are developed to discriminate fine-grained finger inputs and supports three independent passcode secrets including PIN number, lock pattern, and simple gestures by extracting unique features in the frequency domain to capture both behavioral and physiological characteristics including contacting area, touching force, and etc. The system is implemented using a single pair of low-cost portable vibration motor and receiver that can be easily attached to any surface (e.g., a door panel, a stovetop or an appliance). Extensive experiments demonstrate that our system can authenticate users with high accuracy (e.g., over 97% within two trials), low false positive rate (e.g., less 2%) and is robust to various types of attacks.

Index Terms—User authentication; finger-input; physical vibration; ubiquitous surfaces

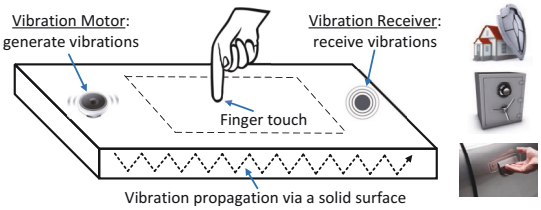
1 Introduction

The process of authentication verifies a user's identity and is frequently deployed at almost every corner of our daily lives. Recently, the flourishing mobile IoT facilitates wide deployment of *smart access systems*, which are defined as those used for keyless controlling access to corporate facilities/apartment buildings/hotel rooms/smart homes/vehicle doors, require the authentication process to play a broader role in numerous daily activities beyond the common form authentication on touch screen devices, such as mobile phones. A market report shows that the deployment of smart security access systems is expected to grow rapidly at an annual rate of 7.49% and will reach a market value of $\$9.8$ billion by the year of 2022 [1].

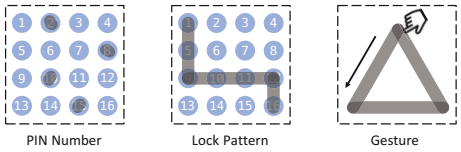
Traditional authentication solutions in smart security access systems are based on passwords (i.e., texts and graphical patterns) [2], [3], [4], [5], [6] and physiological biometrics (e.g., fingerprints, iris patterns, and face) [7], [8], [9], [10]. However, these approaches either suffer from password theft or shoulder surfing, or require installation of expensive equipment and stir privacy concerns of the users. Other solutions supported by intercom, camera, card, or fingerprint, however, involve expensive equipment, complex hardware installation, and diverse maintenance needs. The trend of employing low-cost low-power tangible user interfaces (TUI) to support user authentication in smart IoT and mobile systems has gained industry attentions recently. For example, token devices (e.g., smart ring, glove or pen) could be utilized for associating identities of their touch interactions [11], [12], and an ultra-thin sensing pad can be deployed in automobiles to perform driver authentication [13]. Moreover, isometric buttons appearing on new models of smart microwave ovens and stove tops and rotary inputs (e.g., used by iPod) can replace the regular physical buttons to provide better functionality and flexibility [14]. These new approaches appear promising of conducting mobile user authentication and operating appliances/devices in smart IoT systems leveraging capacitive sensing. However, these techniques require that the touched surface possesses electric conductivity and an electric field that produces/stores electrical energy, which largely limits the wide deployment of such solutions.

Along this direction, we start a new search in developing a low-cost and portable general user authentication approach, which can be easily integrated into mobile and IoT devices and has the capability to work with any solid surface for smart IoT access control systems. The convenience of executing mobile user authentication via touching any surface is enticing. For instance, with the rapid development of IoT and connected vehicles, a user can just place his palm against the driver side window to unlock and access the vehicle. This has already been visualized in the popular movie "Mission Impossible 5", in which the featured BMW muscle car can be unlocked instantly when the lead

- *X. Yang, S. Yang, and Y. Chen are with the Department of Electrical and Computer Engineering, Rutgers University, Piscataway, NJ 08854. E-mail: {xinyang, sy540}@winlab.rutgers.edu; yingche@scarletmail.rutgers.edu.*
- *J. Liu is with the University of Tennessee, Knoxville, TN 37996. E-mail: jliu@utk.edu.*
- *C. Wang is with Louisiana State University, Baton Rouge, LA 70803. E-mail: chenwang1@lsu.edu.*
- *N. Saxena is with the University of Alabama at Birmingham, Birmingham, AL 35294. E-mail: saxena@uab.edu.*
- *Y. Chen is the corresponding author.*



(a) Finger touching on a vibrating surface



(b) Three types of secrets

Fig. 1. Illustration of a finger touching on a solid surface under physical vibration, and three independent types of secrets for pervasive user authentication.

actor pressed his palm against the side window. Moreover, many appliances in smart homes require access control for advanced safety, such as prohibiting children and seniors from operating risky appliances (e.g., stovetop, oven, and dryer). Additionally, various IoT devices, such as smart TV, air conditioner, and smart speaker, have a growing need for providing customized services, including adjusting room temperature/lighting conditions and recommending TV content. A low-cost solution of tangible user authentication enabled on any solid surface could eliminate the need of installing touch screens on such electronic devices and make the customized services easy to deploy.

In this work, we introduce a new authentication system grounded on low-cost, low-power tangible user interface, which has the flexibility and mobility to be deployed on ubiquitous surfaces. Our system leverages physical vibration to support authentication for emerging IoT devices and smart access security systems and is portable to be deployed on various mobile applications. Builds upon a touch sensing technique using vibrations, the proposed system is robust to environmental noise and can operate on a broad range of surface materials. As shown in Figure 1(a), when a vibration motor actively excites a surface resulting in the alteration of the shockwave propagation, the presence of the object or finger in contact with the surface can thus be sensed by analyzing the vibrations received by the sensor. By relying on a single low-cost sensor that generates vibration signals in a relatively high frequency band (i.e., over $16kHz$), the system is hardly audible or distracting to the user, and is less susceptible to environmental interference from acoustic (i.e., mainly within a lower frequency band [15]) or radio-frequency noise. More importantly, vibration propagation is highly dependent on the surface material and shape in specific scenarios. Thus the designed system provides enhanced security by integrating location/surface uniqueness through such low-cost and tangible vibration-based user-interface. The user-specific identity information is embedded in both the behavioral biometrics as well as the surface being touched, making the system hard to be forged by attackers. The proposed system provides users to choose from three different forms of secrets including PIN, lock pattern, and gesture to gain secure access as shown in Figure 1(b).

In our conference paper [16], we developed a preliminary system that achieves reasonable authentication performance on a 3×3 simple grid layout with 9 grid points using Support Vector Machine (SVM). In this work, we design and implement a more comprehensive system with enhanced authentication capability to support 4×4 advanced grid layout with 16 grid points. The enhanced system could facilitate various practical applications. For instance, a virtual PIN pad with standard T9 layout can be deployed on any solid surface, with 10 grid points reserved for digits and the rest for "star", "pound", "delete" and "confirm"; palm recognition and handwriting authentication could also be achieved thanks to the enhanced sensing resolution. In addition, our preliminary work uses SVM-based classifier which shows low scalability to authenticate users on the advanced grid layout. This is because SVM converts multi-class classification to multiple binary classification tasks, making it difficult and slow to optimize the model [17]. Toward this end, we develop a novel deep neural network (DNN) that intrinsically supports identifying enormous classes and outperforms SVM on complicated tasks [18], [19]. Through integrating the developed deep learning model, extensive experiments are performed to further validate the authentication performance and versatility of the proposed system. We implemented two prototypes that could adapt to diverse scenarios by exploiting the SVM or DNN accordingly: 1) We provide a lightweight prototype based on SVM for deployment on resource-constrained mobile devices and IoT systems with simple grid layout; 2) A more comprehensive prototype based on DNN offers more accurate user authentication on the advanced grid layout for accuracy-sensitive applications with more computing resources.

The authentication process can be enabled on any solid surface beyond touch screens and without the constraint of limited screen size. The proposed system is compact and portable, making it ideal to be deployed on smart IoT and mobile devices, such as smart appliances, apartment entrance, and automobiles. It is resilient to side-channel attacks and various adversarial activities even when the adversaries are aware of the passcode secret. It can authenticate the legitimate user and reject attacks well because of the following insights: 1) our study shows that vibration signals have the capability to perform cm-level location discrimination; and 2) unique features are embedded in a user's finger pressing at different locations on a solid surface. Such unique features reflect the characteristics of the user's finger touching on the medium (e.g., a door panel or a desk surface) including locations of touching, contacting area, touching force, and etc., making them capable to discriminate different touching locations of the same user and different users when touching on the same location. Thus, the system enables users to finger-input (i.e., touch or write) on solid surface and is robust to passcode theft or passcode cracking by integrating 1) passcode, 2) behavioral and physiological characteristics (e.g., touching force and contacting area), and 3) surface dependency (e.g., house door or office desk) together to provide enhanced security. We summarize our main contributions as follows:

- We develop the first real-time vibration-signal-based finger-input authentication system, which can be deployed on any solid surface for mobile applications and

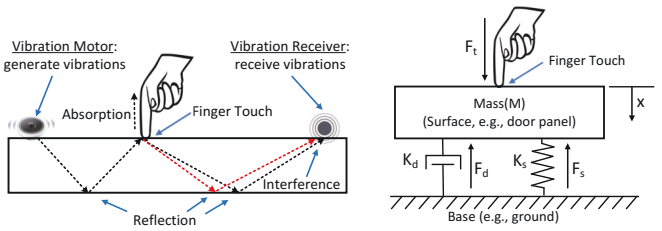
IoT access control systems.

- Our system captures intrinsic human physical characteristics presenting at specific location/surface for authentication through extracting unique features (e.g., frequency response and cepstral coefficient) in the frequency domain.
- The system is flexible to support three types of secrets (i.e., PIN, lock pattern, and gesture) and works with different grid layouts and surfaces to meet diverse application requirements by developing novel techniques of virtual grid point derivation, feature-based dynamic time warping (DTW), and earth mover's distance (EMD)-based distribution analysis.
- We implement portable system prototypes with a single pair of low-cost vibration motor and receiver that involve minimum installation and maintenance cost, together with an Android app that enables real-time profiling and verification.
- Extensive experiments show that our SVM-based prototype can effectively verify legitimate users on a simple grid layout with over 95% accuracy within two trials and less than 3% false positive rate. The new prototype enhanced by DNN achieves over 97% accuracy and less than 2% false positive rate on an advanced grid layout.

Our preliminary work has been published in ACM CCS 2017 [16]. In this journal paper, we have made revision with comprehensive additions to the design, implementation, and evaluation of the approach. Specifically, we proposed a vibration profile extraction mechanism based on deep learning. This mechanism aims to enhance the authentication performance when using either PIN number or lock pattern. Moreover, we implemented an end-to-end prototype of the real-time user authentication system by using a pair of low-cost piezoelectric sensors and developed an Android app. In addition to the 3×3 small grid layout presented in the conference paper, we further evaluated our system on a larger 4×4 grid layout with more virtual grid points to validate the system's scalability. Furthermore, we extended our study to investigate the authentication performance on various surface sizes and different material types in addition to the wooden table and door panel originally reported in the conference paper.

2 Related Work

User authentication becomes a critical step under the growing privacy concerns. Traditional user authentications utilize text-based passwords [2]. To ensure that a user's password cannot be easily guessed, the user has to memorize long strings of random characters, making it inconvenient [4]. Graphical passwords are proposed to ease the memory burden by letting users choose their pre-selected images from random choices of pictures [3], [4], [6] or Cued Clicked Points (CCP) in a sequence of images [20]. Additionally, grid lock pattern based approaches [5], [21] have been widely adopted to keep the user's mobile devices protected. Recent graphical authentication methods can resist shoulder surfing attacks by utilizing the Convex Hull Click Scheme [22] or the eye-gaze version of CCP [23]. However, these strategies eventually perform the authentication based on the knowledge of the passwords (e.g., text-based, image-based and lock pattern-based) and cannot tell whether the password is entered by the legitimate user.



(a) Vibration signal propagation characteristics (b) Vibration model under finger touch

Fig. 2. Illustration of the propagation characteristics of vibration signals on a solid surface.

To ensure that the secret inputs used for authentication are physically from the legitimate user, biometrics-based schemes (e.g., fingerprints [8], iris patterns [7], retina patterns [9], and face [10]) have been drawn considerable attention recently. However, physiological biometrics are sensitive personal information, which may involve privacy concerns, thus are not widely accepted. To reduce the privacy concerns, a compromised approach is to authenticate users based on their behavioral characteristics, including unique keystroke dynamic [24], mouse movements [25], and gait patterns [26]. Although these approaches are less sensitive in terms of privacy, they are designed for continuous user verification during the period that the user operates the keyboard, moves a mouse or takes a walk, rather than one-time authentication.

To provide authentication to the emerging smart access systems needed by corporate facilities, apartment buildings, hotel rooms, and smart homes, techniques involving intercom [27], camera [28], access card [29] and fingerprint [8] have been explored. For example, KinWrite [28] uses Kinect, a vision-based platform, to capture the user's 3D handwriting patterns for authentication. These approaches usually involve expensive hardware, complex installation process, and diverse maintenance efforts. Recent studies successfully combine 2D handwriting and behavior features such as corresponding writing pressure, writing speed, and correlation between multiple fingers on touch screens to provide enhanced security [30], [31], [32]. The limitation is that the authentication relies on touch screens, which may suffer from smudge attacks [33] and are not always available in smart access systems. Toward this end, we propose to extend the authentication process beyond touch screens to any solid surface leveraging vibration signals. Our proposed system will have the authentication capability in a broad array of applications including entry access (e.g., smart building, car doors) and supporting customized services in appliances and devices at smart homes. The authentication process combines password and human physical traits, and supports three types of secret including PIN, lock pattern, and gesture input for emerging smart access systems.

3 Physical Vibration Propagation

Physical vibration transfers the initial energy through a medium by a mechanical wave. It experiences attenuation along the propagation path and reflection/diffraction when the signal hits the boundary of two different media. Figure 2(a) illustrates the reflection and diffraction of a vibration signal propagating in a solid surface when a

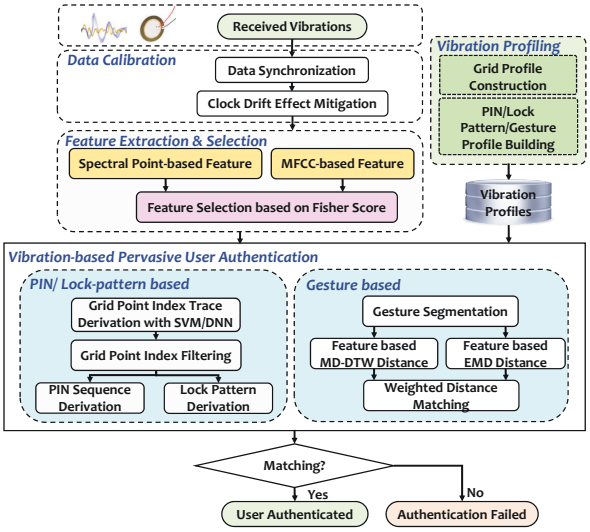


Fig. 3. Overview of the system architecture.

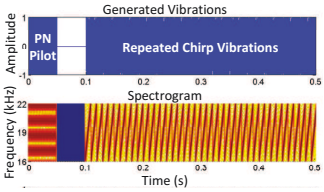


Fig. 4. Example of generated vibrations between $16kHz$ and $22kHz$.

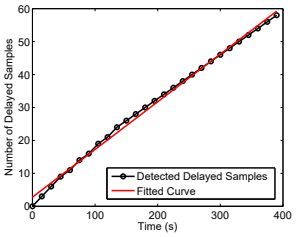


Fig. 5. Illustration of clock drift effect mitigation.

finger touches the area in between the vibration motor and receiver. As described in our conference paper [16], the vibration signal is affected by the finger touching location and traverses different paths before reaching the vibration receiver. Thus, the touching location information is embedded in the various interference effects captured by the receiver. Specifically, we consider a spring-mass-damper system, as shown in Figure 2(b), to model the vibration effect on the object under an external force caused by the finger touch. We leave the detailed analysis of the model in our conference paper [16]. This model shows the displacement of medium is dependent on the external force. Therefore, the finger touching force could be captured by analyzing the received vibration signals and utilized as a biometric-associated feature in our system.

In addition, Dong *et al*. [34] experimentally demonstrate that the vibration energy absorbed into the human finger-hand-arm system is different under different vibration frequencies. In our empirical study we find that the frequency response of the same user finger-press presents higher correlation than that of different users when they touch the same location on a surface. This important observation suggests that the vibration propagation properties are strongly influenced by unique human physical traits such as contacting area, touching force and etc., which can assist ubiquitous user authentication together with passcode on any surface beyond touch screens.

4 Approach Overview

4.1 System Overview

As illustrated in Figure 3, when the vibration motor generates low annoyance vibrations, the system starts taking inputs of vibration signals from the vibration receiver. The system first performs *Data Calibration* (Section 5.2) including data synchronization and clock drift effect mitigation to synchronize the received vibration signals and eliminate the clock drift effects caused by the inconsistent sampling frequency.

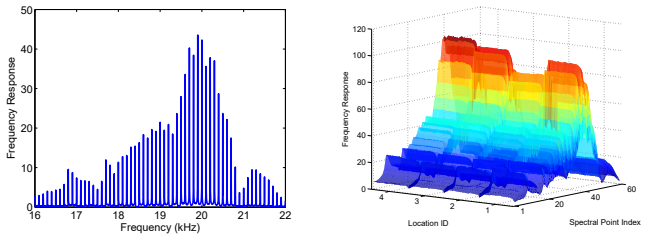
The system then extracts and selects vibration features (Section 5) in the frequency domain from the synchronized vibration signals within a sliding window. We find that *Spectral Point-based Feature* (i.e., frequency amplitude of each spectral point) and *MFCC-based Feature* (Mel-frequency cepstral coefficient [35]) reflect the intrinsic physical traits embedded in the user's finger inputs. The system further performs *feature selection* based on the Fisher Score [36] on top of the Spectral Point-based and MFCC-based features by selecting a subset of features exhibiting more discriminative power among different touching locations as well as maintaining feature consistency within each touching location.

The extracted vibration features are used by two phases in the system: *profiling* and *authentication*. In the profiling phase, the features are extracted and captured while a user first enrolls in the system and presses his finger at different grid points on the touching surface. These features are labeled and saved to build the user's profile in *Grid Profile Construction*.

During the authentication phase, the received vibration signals are utilized to extract vibration features. The extracted features then serve as inputs to *Grid Point Index Trace Derivation* via a classifier based on Supporting Vector Machine (SVM) for a simple grid layout or deep neural network (DNN) for an advanced grid layout trained by the grid profiles. The classifier compares the extracted features with the stored ones in the profile. The derived grid point trace would then be put into *Grid Point Index Filtering* (Section 6.3) to eliminate the incorrectly classified grid point indices and obtain the ones corresponding to the finger presses in the grid point index trace. Next, the filtered grid point trace would be recovered to the PIN sequence/lock pattern via *PIN Sequence Derivation* or *Lock Pattern Derivation* (Section 6.4). The recovered PIN number/lock pattern is then compared with the local stored PIN/lock pattern information for the final authentication.

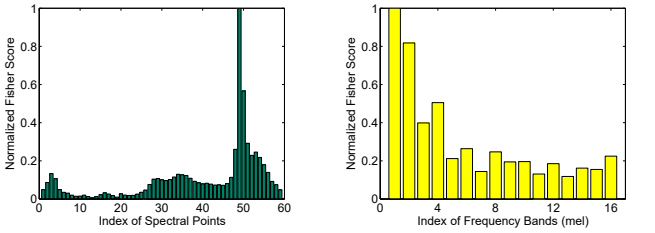
Independently, the proposed system also enables the user to perform simple gestures (e.g., drawing a circle on the surface) for authentication without the restrictions of pressing/passing the grid points on the authentication surface. Different from the fixed grids in PIN/lock pattern based authentication, using gestures provides more flexibility. However, even for the same user, the finger gesture could be inconsistent at different times. Thus our system needs to tolerate the inconsistency while preserving individual diversity.

In particular, during the gesture-based authentication, the system first identifies the signal segment containing the gesture operation via *Gesture Segmentation*. In the profiling phase, the extracted feature sequence (i.e., Spectral Point-based and MFCC-based features) from the gesture segments are saved to build the user's profile. To measure the simi-



(a) Spectral points at every $100Hz$ interval (b) Distinguishable spectral points when a finger presses 4 different locations

Fig. 6. Illustration of the frequency response of the received vibrations in a $0.2s$ time window. And the frequency response is depicted at spectral points when a finger presses 4 different locations of a desk.



(a) Fisher score of spectral point based features (b) Fisher score of MFCC based features

Fig. 7. Fisher score of the feature candidates (a) spectral point based and (b) MFCC based.

larity of generated features in the authentication phase to the gesture profiles, we address the gesture inconsistency problem by considering both time warped feature sequences and the distribution of the features. This is achieved by calculating both MD-DTW (Multi-Dimensional Dynamic Time Warping) Distance [37] and EMD (Earth Mover Distance) [38] of the extracted feature sequences. The weighted distance combination in *Weighted Distance Matching* obtains the combined distance from both techniques. Finally, the system makes decision as user authenticated or access denied by checking a threshold to the calculated distances between input gestures and the stored profiles.

5 Vibration Signal Design and Feature Extraction & Selection

5.1 Vibration Signal Design

To facilitate finger-input based user authentication via physical vibration, the vibration signals used in our system need to contain a broad range of frequencies to increase the diversity of vibration features in the frequency domain. Specifically, we generate repeated chirp vibration signals to linearly sweep frequency within the range from $16kHz$ to $22kHz$, which are hardly audible to most human ears [39]. Figure 4 illustrates an example of the generated vibration signal and its corresponding spectrogram. In particular, there is a short pseudo-noise (PN) sequence preamble played before the repeated chirp vibrations, which is used for the signal synchronization. We leave the details in Section 5.2. After transmitting PN pilot, with a $50ms$ pause, the vibration motor repeatedly transmits the chirp vibration signal to keep its continuous sensing capability while performing authentication. The length of each chirp vibration signal is set to T=$10ms$, which provides high time resolution to enable continuously finger-input sensing.

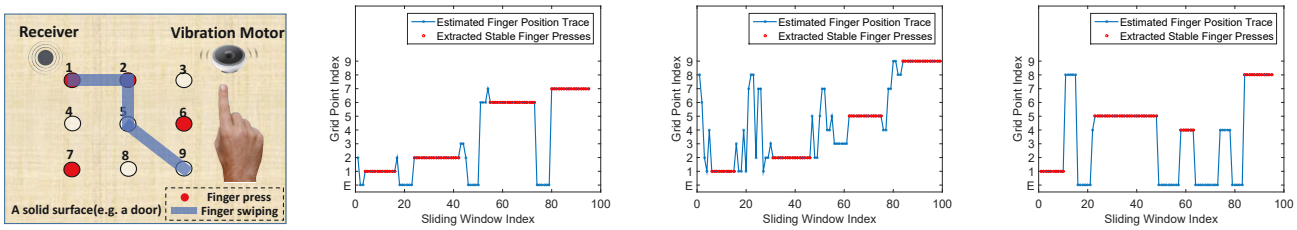
5.2 Vibration Signal Calibration

Vibration Signal Synchronization. The timing of the system's vibration motor and receiver needs to be synchronized so that each sliding window used for vibration feature extraction contains the same part of the chirp signals without time delay. We address this issue by leveraging the ideal autocorrelation properties of adding a pseudo-noise (PN) sequence preamble (i.e., 2400 samples) [40] at the beginning of the generated chirp vibration signals as Figure 4 shows. We then synchronize the received vibrations using cross-correlation between the PN sequence of the received vibration signals and the known generated PN sequence.

Clock Drift Effect Mitigation. The Analog to Digital Converter (ADC) is usually configured to convert the analog voltage signals produced by the sensor into digitized signals at a fixed sampling frequency driven by different application requirements. However, we experimentally find the sampling rate may not be a fixed value over time due to the imperfect clock, and a small gap exists between the actual sampling rate and the configured sampling rate. To eliminate the clock drift effect, we estimate the sampling rate offset during a short calibration phase at the beginning. Specifically, the vibration motor periodically sends a short vibration chirp with a fixed time interval (e.g., 2s). The time intervals between these chirps should be a fixed value as well if there is no clock drift. We use cross-correlation to measure the sample delays of the received vibration chirps over time as illustrated in Figure 5. We observe that the number of delayed samples increases linearly over time, indicating the actual sampling rate is slightly larger than the configured value but remains relatively fixed. We then use a least-squares based approach to fit a quadratic curve to the measured delayed samples, and obtain the slop k to shift the starting point S_p of each received vibration chirp to $S_p = S_p - \lfloor kt \rfloor$, where t is the time interval between the current vibration chirp and the first received vibration chirp.

5.3 Spectral Point-based Feature Extraction

In order to extract unique vibration features from the received vibrations to discriminate the finger touches on different surface locations and distinguish different users touching a same surface location, we first analyze the received vibration signals in the frequency domain using a $200ms$ sliding window. Figure 6(a) presents an example of the Fast Fourier Transform (FFT) of a time series of the received vibration signals, ranging from $16kHz$ to $22kHz$, in a sliding window. The transmitted chirp vibration signal has fundamental frequencies that are all multiples of the frequency $1/T$ Hz, where T is the time duration of each chirp vibration signal (e.g., $T = 0.01s$ in this work). We find that the amplitudes of some designated frequency components in the signals (i.e., peak values in Figure 6(a)), called *spectral points*, are most sensitive to the minute changes caused by finger touching or swiping. These spectral points are more sensitive to the finger touches and could be utilized to differentiate different surface locations finger presses or finger moving along. For example, in our preliminary experiments, the vibration signals are collected when a user's



(a) User presses a PIN sequence "1267" and swipes a lock pattern "$1-2-5-9$" on a 3×3 grid

(b) Estimated finger position trace in terms of grid point index when the user enters the PIN sequence "1267"

(c) Estimated finger position trace in terms of grid point index when the user swipes the lock pattern "$1-2-5-9$"

(d) Example of an attacker entering the legitimate user's PIN sequence "1267" on the same grid of the same desk surface

Fig. 8. Example of PIN sequence/lock pattern derivation in sliding windows when entering a PIN sequence/lock pattern on a solid surface.

finger presses at four different locations of a solid surface (i.e., wooden table) equipped with our vibration motor and receiver. We observe obvious distinguishable patterns of the frequency amplitude at these 60 spectral points (i.e., $\frac{22000-16000}{100} = 60$) between different locations, which are shown in Figure 6(b). Furthermore, the spectral points in the frequency domain may not be exactly spaced at $100Hz$ due to imperfect sampling module. We thus design a threshold-based strategy (i.e., minimum distance between two neighboring peaks and minimum height of each detected peak) to find peaks of the frequency response to extract each spectral point feature.

5.4 MFCC-based Feature Extraction

The Mel-frequency cepstral coefficient (MFCC) is widely used to represent the short-term power spectrum of acoustic or vibration signals [35] and can represent the dynamic features of the signals with both linear and nonlinear properties. While the MFCCs are able to distinguish people's sound differences in speech and voice recognition, we find that they can also characterize the vibration signals transmitting via the medium of a solid surface on which the user's finger touches, because the user's behavioral and physiological characteristics (e.g., touch area and pressure) and the touching position can cause different changes to the vibration propagation. We thus extract the MFCC-based features to characterize the different vibration signatures when the user touches or writes at different positions on the surface. In particular, we calculate the MFCCs of the received vibration signals in each sliding window. The number of filterbank channels is set to 32, and 16-th order cepstral coefficients are computed in each $20ms$ Hanning window, shifting $2ms$ each time. We leave the details of correlation-based effectiveness verification for the MFCC-based feature in our conference paper [16].

5.5 Feature Selection based on Fisher Score

From our experiments, we observe that not all extracted features including both spectral points and MFCC are unique enough to discriminate different touching locations and distinguish different users touching the same location. The discrimination power is dependent on the extracted features at specific frequencies or Mel-frequency bands. We therefore propose to select features based on Fisher Score [36] to find a subset of features which are more distinct between classes (i.e., touching locations per user) and consistent within a class. The fisher score of the r-th feature candidate is defined as follows:

$$F_r = \frac{\sum_{i=1}^{c} n_i(\mu_i - \mu)^2}{\sum_{i=1}^{c} n_i \delta_i^2}, \quad (1)$$

where n_i is the number of instances in class i. And μ_i and δ_i^2 denote the mean and variance of class i, $i = 1, ..., c$, corresponding to the r-th feature candidate. μ denotes the mean of r-th feature candidates in the whole data sets.

To analyze the feature difference between different frequency bands, we consider each spectral point or MFCCs at each frequency band as an individual feature candidate. Figure 7 shows the normalized fisher scores of both the spectral point based and MFCC based features that we use to perform user authentication. In this work, we empirically choose top 30 spectral point based features, and top 8 MFCC based features which are more sensitive to the finger pressing and swiping.

By applying the feature selection method based on Fisher Score, we could enhance the performance of the SVM-based grid point index derivation method introduced in Section 6 via eliminating features that are less distinguishable to the touching locations and user identities. Moreover, for the DNN-based grid point index derivation that can automatically adjust the weights of features, feature selection can reduce the size of the spectral point and MFCC based features to accelerate the model profiling and grid point index derivation processes. Therefore, the Fisher Score-based feature selection could generate compact and effective features to satisfy both the SVM and DNN based grid point index derivation methods and enable efficient computation on mobile IoT devices.

6 Authentication Using PIN Numbers and Lock Patterns

6.1 Deriving Grid Point Index Traces Based on SVM

The system takes the received vibration signals as input when the user enters PIN sequence/lock pattern. In particular, we apply a sliding window to the vibration signals and derive vibration features (e.g., spectrum-based feature and MFCC-based feature) in every sliding window. We then apply a machine learning-based grid point classifier based on the Support Vector Machine (SVM) using LIBSVM [41] to estimate the finger-press positions by leveraging the user's personal grid profile. The resulted grid point index trace is actually an estimated finger-press position trace which reflects the finger position changes among the grid

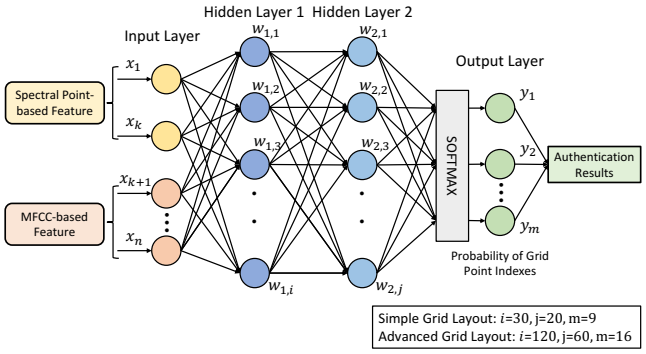


Fig. 9. Demonstration of the deep neural network-based classifier.

point indices in the entire PIN sequence/lock pattern input duration. Note that when we derive grid point index trace, it involves user's behavior and physical characteristics. Based on the derived grid point index trace, we can recognize the user's PIN sequence/lock pattern input and verify their identities. An example of PIN sequence/lock pattern derivation is given in Figure 8, as explained in our conference paper [16], where the legitimate user inputs PIN sequence "1267" and lock pattern "1-2-5-9" as Figure 8(a) shows. Our system correctly recognizes the user's PIN sequence as in Figure 8(b) and lock pattern as in Figure 8(c). The attacker's input is mistakenly recognized, thus rejected by the system as shown in Figure 8(d).

6.2 Deriving Grid Point Index Traces Based on Neural Network

The SVM-based classifier gives reasonable predictions when authenticating users on the simple grid layout. However, many real-world applications such as the virtual PIN pad, virtual keyboard, and handwriting authentication, bring eager demands for more authentication grid points. As we extend the preliminary system on the advanced grid layout, we observe the authentication accuracy of the SVM-based system decreases below the threshold to support the user authentication. This is because SVM gains multi-class classification capabilities [42], [43], [44] by converting multi-classification problems into many binary classification problems [45], [46]. Therefore, the authentication efficiency decreases as more grid points are added. Toward this end, we leverage deep learning techniques that intrinsically support multi-class classification to enhance the authentication capability of the developed system. Meanwhile, given that SVM has low computational overhead and is effective for a lightweight deployment, we preserve the SVM-based system as an alternative for lightweight systems with restricted computational resources on the simple grid layout.

Specifically, we design a four-layer deep neural network as demonstrated in Figure 9. To find the suitable structure of the neural network, we start with a basic three-layer DNN model and gradually adjust the number of neurons and layers to seek the balance between authentication accuracy and model complexity. Through many rounds of trials, we find that a four-layer DNN could achieve high authentication accuracy and is sufficiently lightweight to fit in mobile IoT devices. This neural network takes both the spectral point-based feature and MFCC-based feature as inputs. We then apply two fully connected hidden layers to extract unique vibration characteristics. To accommodate both simple and advanced grid layouts, we empirically deploy 30 neurons in *Hidden Layer 1* and 20 neurons in *Hidden Layer 2* for the simple grid layout; whereas for the advanced grid layout, the deployed neurons are increased to 120 and 60 respectively. We use $tanh$ as the activation function for $HiddenLayer1$ and $sigmoid$ for $HiddenLayer2$. After that, the softmax layer outputs the predicted grid point index. We use mean square error (MSE) as the loss function to estimate the deviation between the inference results and ground truth for model optimization. The derived neural network converges within 200 iterations in the training stage, which only takes around 5 seconds on a consumer laptop equipped with a quad-core Intel Core i5 processor.

When deploying the DNN-based authentication system in real-time, user profiles are usually collected over a limited time period (i.e., 5 seconds) for better user experiences. However, DNN requires enormous training samples to build effective models. Therefore, we need to address the overfitting issue caused by the limited finger-input samples. Particularly, an overfitted model requires the user to perform highly identical finger input as in the profiling stage. Although the system security is enhanced by requiring strict input consistency, as a trade-off, even the legitimate user can be denied by the system due to the increased false negative rate. To address the overfitting issue without compromising the system integrity, we apply neuron pruning techniques [47] to properly restrict the fitting capability and accelerate the inference process. Particularly, we utilize the magnitude-based weight pruning API provided in TensorFlow [48] to set the values of up to 50% of weights as zeros. The pruned DNN model holds high sparsity as the computations related to the zero-weight neurons could be skipped at the inference stage. As a result, the pruned DNN model could further accelerate the inference speed and is more resistant to overfitting due to its simplified structure [49]. Moreover, we add dropout layers that randomly invalidate 20% of neurons and apply early stopping strategy to prevent the model from converging to a local optimum. Our fine-tuned deep neural network can effectively extract the user's grid profiles from the captured finger-input events. At the inference stage, the continuous vibration signals are processed based on small sliding windows (i.e., $200ms$) to further reduce the computational cost. We observe that on regular Android smartphones (e.g., Google Nexus 6), our pre-trained DNN model could achieve near real-time user experiences with negligible latency.

6.3 Grid Point Index Filtering

In practice, the derived grid point index traces contain incorrectly classified grid point indices caused by the varying finger touching area and force when the finger is just detaching or pressing on the surface (e.g., the noises in Figure 8(b)), or the swiping finger is far from any of the predesigned profiled virtual keys (e.g., the noisy indices in Figure 8(c)). Therefore, we develop a grid point index filter to determine the segments that have consecutive same grid point indices, which could provide more reliable results for identifying the PIN sequence/lock pattern. The grid point index filter consists of three steps: 1) calculating the difference between every two consecutive grid point indices

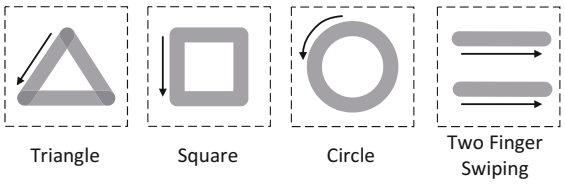


Fig. 10. Illustration of the four pre-defined finger gestures for gesture-based authentication.

in the trace; 2) searching for the starting and ending points of the consecutive differential grid point indices (i.e., 0s) to extract *finger-press segment*, indicating the finger positions of the firm finger presses right on or near virtual keys; 3) removing the grid point indices from the trace that are out of the finger-press segments. The red dots in Figure 8(b) and Figure 8(c) are filtered grid point indices for the PIN sequence and lock pattern derivation, respectively.

6.4 PIN Sequence/Lock-pattern Derivation

Next, we further confirm each finger-press segment based on their length of time and remove the incorrect finger location estimations to derive the PIN sequence/lock pattern. The intuition is that when users enter their PIN sequences or draw their lock patterns, the finger pressing process will last for certain amount of time. The grid point index segments shorter than this amount of time are highly possible to be incorrect finger location estimations. We empirically determine the threshold of minimum finger-press duration (i.e., $300ms$) to remove the finger-press segments with shorter time duration. Finally, given the length of the user's PIN sequence/lock pattern, the system finds the same number of the longest finger-press segments as the valid finger-press segments and derives the PIN sequence/lock pattern by mapping the segments' grid point indices to virtual keys.

6.5 Grid Profile Construction

Our PIN/Lock-pattern based authentication requires constructing the user's profile corresponding to every grid point, which enables successful identification of the input virtual keys during authentication. Specifically, the system records a short time period (e.g., 1 to 5 seconds per grid point) of received vibration signals when the user presses at each grid point. The recorded vibration signals are used to derive the vibration features in sliding windows. The feature in each sliding window is labeled with corresponding grid point index. In addition, we also build a profile when no finger touches the surface and label it as "E" (i.e.,"empty") to discriminate whether a finger presses on the surface.

7 Authentication Using Gestures

7.1 Gesture Segmentation

Our system defines four simple finger gestures as shown in Figure 10: swiping a single finger along three patterns including a triangle, square and circle, and swiping two fingers horizontally. To facilitate the gesture-based authentication, our system needs to first detect the occurrence of the user's gesture. Specifically, the system first extracts vibration features from spectral points and MFCC, then calculates vibration feature differences between the received vibration signals and those in the profile when no finger touches on the surface. When the user inputs a gesture, the

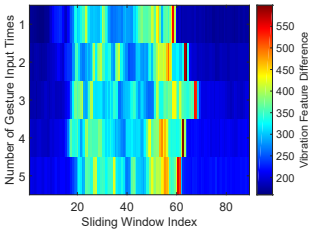


Fig. 11. Illustration of gesture segmentation when a user inputs gestures for five times.

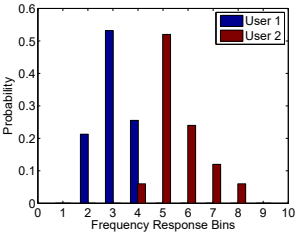


Fig. 12. Histogram of frequency response at a spectral point for two users swiping a same gesture.

finger swipes on the surface, causing the vibration features to differ largely from those when there is no finger touching. Figure 11 shows an example of calculated vibration feature differences when the user inputs square gestures on the surface for five times. We observe that the vibration feature difference rises as the finger swipes on the surface and drops when the finger releases from the surface. We thus normalize the vibration feature differences and segment each gesture via a threshold.

7.2 Distance Calculation of Feature Sequence

User authentication using such simple gestures is much harder due to lack of unique secrecy to discriminate different users. Moreover, the gesture inconsistency (i.e., swiping speed, duration, and trajectory of the same user's gestures) would lead to varying density of locations within the swiped pattern. To solve this, we resort to two techniques that complete the authentication process in high accuracy to cope with the challenges. The Dynamic Time Warping (DTW) [37] is exploited to deal with gesture inconsistency, and the earth mover's distance (EMD) [38] technique is employed to preserve individual diversity because the feature distribution of the same user should have a higher similarity than that from different users.

Specifically, we first derive a time series of vibration features based on the vibration signals in segmented gestures using a sliding window. The DTW technique stretches and compresses required parts to allow a proper comparison between two data sequences. Therefore, it is useful to compare the vibration feature traces extracted from two segmented gestures. The extracted vibration features report both frequency amplitude and MFCC coefficients, which are discussed in Section 5. To perform multidimensional sequence alignment, our system applies Multi-Dimensional Dynamic Time Warping (MD-DTW) [37], in which the vector norm is utilized to calculate the distance matrix according to:

$$d(v_i, v'_j) = \sum_{p=1}^{P} (v_i(p) - v'_j(p))^2, \tag{2}$$

where $V = v_1, v_2, ..., v_T$ and V'=$v'_1, v'_2, ..., v'_T$ are two vibration feature traces for gesture discrimination, and P is the number of dimensions of the sequence data (i.e., the number of extracted features within each window). A least cost path is found through this matrix and the MD-DTW distance is the sum of the matrix elements along the path.

Besides time warped feature sequence, we find that the histogram of the spectral point based features preserve individual diversity and can be used to distinguish different users when even the same gesture is swiped. Figure 12

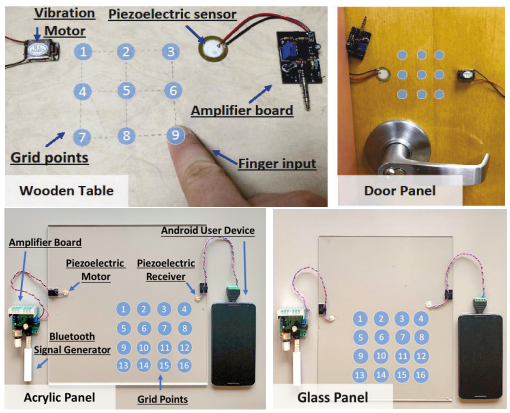
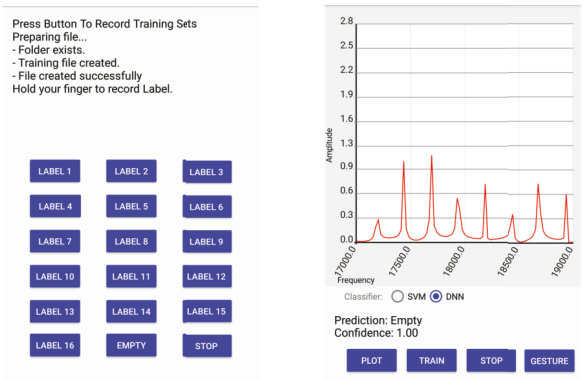


Fig. 13. Four prototypes of our system on the wooden table, door panel, acrylic, and glass panel.



(a) Profiling module of the Android app

(b) Authentication module of the Android app

Fig. 14. User interface screenshots of the Android app.

shows the feasibility study results where two users swipe their fingers following an exactly same circle gesture pattern on a desk surface. The histogram of frequency response (quantized to 10 bins) at a specific spectral point during their swiping presents distinct distributions that can clearly distinguish these two users. We thus take the advantage of the EMD-based distribution difference to preserve the individual diversity during the gesture-based authentication. Specifically, we normalize the EMD distance and MD-DTW distance to be integrated for final authentication. If the integrated distance to the gesture profiles is larger than a threshold, our system regards the swiped gesture as an unknown gesture and fails the authentication. Otherwise, we consider the swiped gesture is from the user whose profile results in the minimum integrated MD-DTW and EMD distance.

7.3 Gesture Profile Construction

Unlike grid point profile construction, the proposed system does not need to construct profiles for each grid point for the gesture-based authentication. Instead, when constructing the gesture profile for a particular user, the system collects the vibration signals while the user swipes a finger following a predefined gesture. In particular, we use the sequence of the vibration features extracted from the segmented signals for building individual gesture profile. Though the profile only contains simple gestures, such profile contains the user's unique behavior and physiological characteristics and is sufficient to perform user authentication. We also build a profile when there is no finger touching on the surface to determine the presence of finger touching.

8 Performance Evaluation

8.1 Prototype Implementation

Test Surface. We evaluate the performance of the user authentication and system scalability using PIN and lock patterns on both the simple 3×3 grid layout and the advanced 4×4 grid layout. The grid is drawn on a solid surface in a typical office environment. The distance between the adjacent grid points is $3cm$. In practice, the grid arrangement could be flexibly extended as needed. We build our prototypes on four different types of surfaces. The prototype setups are illustrated in Figure 13. We used (1) wood surfaces, including a wooden table with the testing region resided below the vibration motor and receiver and a wood sheet ($30.48cm \times 15.24cm \times 1.91cm$) with the testing region resided between the vibration sensors; (2) a door panel with the testing region resided in between the motor and receiver; (3) acrylic panels ($30.48cm \times 30.48cm \times 0.32cm$ and $30.48cm \times 30.48cm \times 0.64cm$) with the testing region resided in between the sensors; and (4) a glass panel ($30.48cm \times 30.48cm \times 0.24cm$) with the testing region resided in between the sensors.

Vibration Generator and Receiver. To further scale down the size and cost of our system, we replace the vibration motor and receiver used in our conference paper (i.e., the linear resonant actuator and bulky piezoelectric sensor) with a pair of low-cost, highly compact piezoelectric sensors ($9mm$ diameter). The new pair of sensors could be easily attached to any solid surface. Moreover, the high frequency of the generated vibrations, i.e., 18-$22kHz$, and the ultra-low vibration strength provided by the piezoelectric sensors make the generated surface vibrations imperceptible to humans. We use a low-cost Bluetooth pairing device wired to the vibration motor to capture the designed signals transmitted from the user's device. The received signals will be amplified by a connected low-power amplifier, then converted to physical vibrations via the piezoelectric vibration motor. Note that our system has the flexibility to be further integrated into existing environments, and can easily add on wireless support, such as WiFi, to achieve wireless user authentication.

Android Authentication App. Our system can be used either as a standalone system or be integrated into mobile devices. The system can work with any devices that lack touchscreens, such as IoT devices or embedded systems, to enable user authentication. In our implementation, the Android phone is an emulation of a device on which the system could be implemented in the real-world. The developed Android app allows transceiving vibration signals, constructing grid/gesture profiles, and performing real-time authentication on a single device. Specifically, the Android app consists of two modules: *profiling* and *authentication*. The user interface of profiling module is shown as Figure 14(a). To start capturing the grid point profile, the user can follow the instructions displayed on the screen and tap the grid point button intended to record, then press the finger on the corresponding grid point to complete the grid profil-

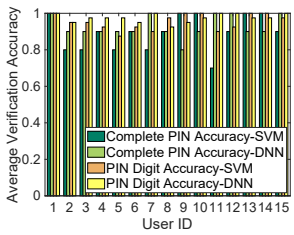
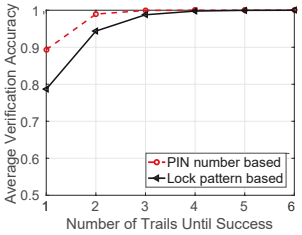
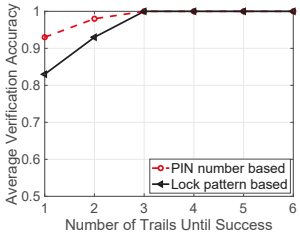


Fig. 15. Performance of PIN number-based authentication for SVM and DNN when the testing region is below sensors.



(a) Multiple trials until success based on SVM



(b) Multiple trials until success based on DNN

Fig. 16. Performance of lock pattern-based authentication when the testing region is below the vibration motor and receiver using SVM and DNN.

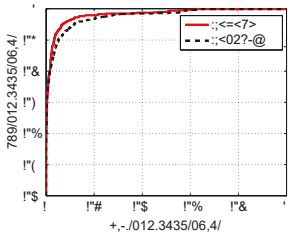


Fig. 17. Gesture based authentication of verifying legitimate users when the testing region is below the vibration motor and receiver.

ing. Similarly, the gesture profile could be constructed by simply clicking the record button then swiping the gesture through the grid points. After the profiles are constructed, the user can select the type of secret and perform real-time verification in the authentication module as shown in Figure 14(b). The app takes the vibration signals captured by the piezoelectric receiver through a $3.5mm$ headphone jack as the input. The spectral point and MFCC-based features are then extracted on the user's Android device. Based on the deployed grid layout, the selected features are fed into the SVM/DNN classifier accordingly. We implement the DNN model based on TensorFlow Lite [48].

Compared to other authentication systems based on cameras, touchscreens, or biometric readers, we explore low-cost and compact settings (i.e., piezoelectric sensors) for the potential of wide-deployment (e.g., apartments, hotel rooms, office). The estimated cost of building such an end-to-end authentication system could be maintained around tens of dollars (e.g., $\$20 \sim \$50$).

8.2 Evaluation Scenarios & Data Collection

8.2.1 Legitimate User Verification

We evaluate the performance of the system under 3 types of authentication[1]. Our data is collected across a three-month period, with 15 participants involved. Before the data collection, we allow users to input on the authenticating surface to get familiar with the system. a) For PIN number based authentication, each user is asked to sequentially press the 9 grid points for 5 seconds to create his/her grid profiles. During verification, each user presses 10 random 4-digit PIN sequences as their passcodes. b) For lock pattern based authentication, our system uses the same grid profiles. During testing, each user swipes a lock pattern 10 times to verify the authentication performance. c) For gesture based authentication, each user chooses one of the four gestures shown in Figure 10 as their preferred gestures and swipes the finger gesture 10 times. In total, we collected 450 genuine inputs (i.e., PIN sequences, lock patterns and gestures) to evaluate the system. We further collected attack inputs to evaluate the performance under attack scenarios.

8.2.2 Various Attack Scenarios

We evaluate the robustness of the system under various types of attack. Specifically, we choose one user as a legitimate user and the rest as attackers to launch the attacks.

1. The study has been approved by our institute IRB.

Blind Attack. The attacker randomly guesses the legitimate user's PIN number, lock pattern and gesture. Then the attacker uses his/her finger to press and swipe on the solid surface for 10 times. In total, we collected 420 blind attack inputs.

Credential-aware Attack. The attacker knows the legitimate user's passcode (i.e., PIN/lock pattern/gesture) but has not observed how the legitimate user presses his/her PIN numbers or swipes his/her lock patterns and gestures on the authentication surface. The attacker inputs passcode 10 times without knowing the legitimate user's detailed behavior. In total, we collected 420 inputs.

Knowledgeable Observer Attack. The attacker both knows the legitimate user's passcode and observes how the legitimate user inputs them on the authentication surface. Each attacker practices 5 times then inputs the passcode 10 times trying to pass the authentication. 420 inputs are collected.

Side-channel Attack. In addition, we perform the side-channel attack by placing additional vibration receivers on the authentication surface. In particular, two receivers are employed: one is placed adjacent to the original receiver, whereas the other is placed at the other side of the surface opposite to the original receiver.

8.3 Evaluation Metrics

Verification Accuracy/Attack Success Rate of PIN Number-based Authentication. This metric shows the percentage of correctly verified PIN numbers entered by the legitimate user or attacker respectively during the user authentication process. Specifically, it includes the complete PIN sequence verification accuracy and the PIN digit verification accuracy. The complete PIN sequence verification accuracy measures the rate of the user's input PINs being completely recognized (i.e., all numbers in the PIN sequence are correctly recognized), while the PIN digit identification accuracy shows the rate of correctly recognizing each single PIN digit.

Verification Accuracy/Attack Success Rate of Lock Pattern-based Authentication. The verification accuracy/attack success rate shows the percentage of correctly verified lock patterns input by the legitimate user or attacker respectively during the user authentication phase. Similarly, it includes the complete lock pattern verification accuracy and lock pattern segment verification accuracy.

ROC Curve of Gesture-based Authentication. The ROC curve is a plot of the true positive rate (TPR) over the false positive rate (FPR). The TPR denotes the rate of the

legitimate users passing the authentication while the FPR denotes the rate of the attackers successfully passing the system. Through varying the feature distance threshold in gesture-based authentication, we can achieve varied TPR and FPR and further obtain ROC curves to evaluate the system performance.

8.4 System Performance of Verifying Legitimate Users

PIN Number-based Verification. Figure 15 shows the identification accuracy of each PIN digit and the complete PIN sequence of 15 legitimate users based on SVM and DNN. Our PIN number based authentication achieves a high verification accuracy for both classifiers. Specifically, for the SVM-based prototype, users can obtain over 95% verification accuracy for each PIN digit. The mean verification accuracy for the complete PIN sequence reaches 90%. For the DNN-based prototype, the accuracy for both single PIN digit and complete PIN sequence improve to 97% and 92% respectively. Meanwhile, DNN shows less volatile verification accuracy among different users, with the baseline accuracy rises from 70% to 80%. Moreover, the verification accuracy of each PIN digit is higher than that of PIN sequence because recognizing the complete PIN sequence requires all the PIN numbers to be correctly identified. The results show our system is effective in verifying legitimate users.

Lock Pattern-based Verification. Figure 16(a) shows the average authentication accuracy of the lock-pattern based verification with different number of trials using SVM. Specifically, the average verification accuracy of the complete lock pattern reaches 79% with a single trial, and 95% with two trials. DNN slightly outperforms SVM as demonstrated in Figure 16(b). Particularly, for the first trial, the DNN-based verification accuracy for the segmented indices achieves over 83%. Within 3 trials, all 15 users are successfully authenticated. In addition, the accuracy of lock pattern verification is slightly lower than that of the PIN number verification, which indicates swiping a finger continuously on the surface produces more errors than pressing the finger on each individual grid point. The high verification accuracy shows SVM-based system can achieve good performance to authenticate users via lock patterns, and DNN classifier can further improve the user experience by more accurate verification with fewer attempts.

Gesture-based Verification. Figure 17 illustrates the effectiveness of legitimate user verification in gesture-based authentication with ROC curves. 15 legitimate users perform their preferred simple gestures (i.e., one of four predefined gestures as shown in Figure 10) ten times. With only one training instance (i.e., one time swiping) for each user, we observe that given a requirement of a 90% true positive rate, we can achieve as low as a 5% false positive rate on average, which indicates only around 5% of gesture trials have gained unauthorized access. We also observe that the using both DTW and EMD techniques can provide slightly better performance than that of only using EMD technique, since it considers the similarity in both time warped feature sequences and the features' distributions. The obtained high verification accuracy and the low-training efforts demonstrate that our system is capable to distinguish different users even though they perform the same simple gesture due to their distinct behavioral biometrics (i.e., finger tip size and structures).

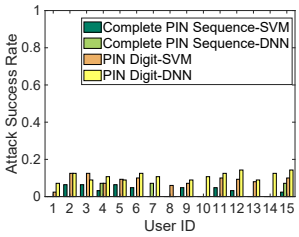


Fig. 18. Performance of PIN number authentication under knowledgeable observer attacks using SVM and DNN.

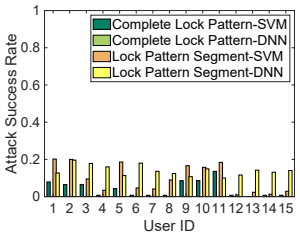


Fig. 19. Performance of lock pattern authentication under knowledgeable observer attacks using SVM and DNN.

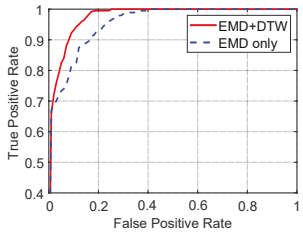
Multiple Authentication Trials and Fall-back Strategy. Figure 16 shows the average verification rate under different number of trials. We observe that both SVM and DNN-based system can achieve over 99% verification rate for both the PIN number and lock pattern inputs within three trials. For the first-time user input, our system can achieve over 89% and 79% accuracy when the user enters PIN number or lock pattern, respectively. Additionally, our system can integrate with any fall-back strategy (e.g., a physical key) to let the legitimate user bypass the system.

8.5 Attacks on Legitimate User's Credentials

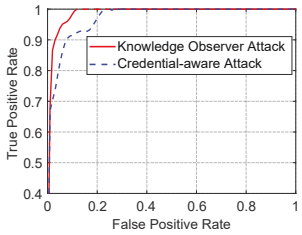
Under blind attacks, both our PIN number and lock pattern based authentications can achieve close to zero attack success rate. Similarly, for gesture-based authentication, the TPR in the obtained ROC curve is close to 100% when the FPR is close to 0%, which shows that the attackers' random gestures cannot successfully access the system.

Under credential-aware attacks, our system also achieves close to 0% attack success rate for all three types of authentications. Since the attackers do not possess the knowledge of the detailed system settings (e.g., grid size, gesture region and the authentication surface), the attackers' finger-inputs are hard to generate the similar impacts on the vibration propagation as the legitimate users do. Knowledgeable observer attack is the most extreme attack, where the attacker is capable of knowing the user's credentials and observing the legitimate user's finger inputs. Additionally, the attacker has the knowledge of the system's setting details and can perform the finger inputs on the same authentication surface. Thus in the rest of this paper, we present the performance evaluation results of our system under this more challenging knowledgeable observer attack.

PIN Number-based Authentication. Figure 18 shows the performance of our system for PIN number based authentication using SVM and DNN separately under knowledgeable observer attack, where 1 of the 15 users alternatively behaves as victim and other 14 users play as attackers. We find that our system is very effective in defending against attackers even though they have the knowledge of the legitimate user's PIN and use the same system setting (e.g., grid size and authentication surface). In particular, the attackers can only break an average of 7% single PIN digits using the SVM-based prototype and 10% using the DNN-based prototype. Notice that a complete PIN sequence comprises multiple PIN digits. Therefore it is very unlikely



(a) Performance of gesture-based authentication using wooden table with simple grid layout



(b) Performance of gesture-based authentication using acrylic panel with advanced grid layout

Fig. 20. Performance for gesture based authentication in different setups.

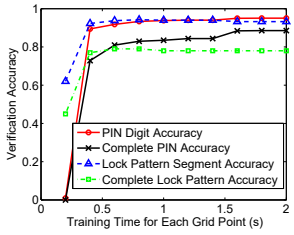


Fig. 21. Performance of both PIN number based and lock pattern based authentications with different grid point training time periods.

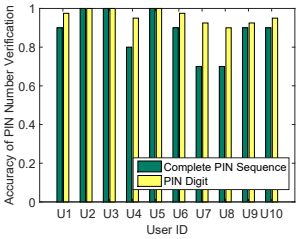


Fig. 22. Performance of PIN number based authentication in verifying legitimate user when the testing region is on a door panel.

for the knowledgeable observer to break the proposed system. Specifically, we observe the attackers can only achieve around 2% attack success rate for verifying the complete PIN sequences on the SVM-based prototype and 1% attack success rate for the DNN-based prototype. We find that although the DNN-based prototype shows a slightly higher attack success rate for single PIN digit, the complete PIN sequences authentication is less likely to compromise compared to the SVM-based prototype.

Lock Pattern-based Authentication. Similarly, we ask 15 users to alternatively play the roles of one victim and fourteen attackers. Each attacker swipes 10 lock patterns after practice based on the knowledgeable observation. Figure 19 shows the attack success rate of lock pattern-based authentication using SVM and DNN respectively. The results show that the attackers are hard to pass the system even though they imitate the legitimate user's behavior to swipe the same lock pattern on the same grid of the same authentication surface after practice. Specifically, for user 4, 6-8 and 12-15 using SVM-based prototype, all the fourteen attackers fail to attack the complete lock patterns in 10 trials. The average attack success rates of the lock pattern segment and the complete lock pattern are 5% and 11% respectively. For the DNN-based prototype, none of the attackers break into the system in our experiments. Although the attack success rate for the lock pattern segment slightly increases compared to SVM-based prototype, it is very difficult for the DNN-based system to recognize an attacker as the legitimate user, which requires all the lock pattern segments contained in a complete lock pattern to be correctly recognized. Moreover, we find the performance of the lock pattern based authentication under knowledgeable observer attack is comparably good to that of the PIN number based authentication.

Gesture-based Authentication. We first evaluate the system performance of gesture-based authentication on a wooden setup using simple grid layout to compare the performance of EMD only and EMD+DTW techniques. The experiments are performed under the knowledgeable observer attack, where attackers try to mimic the legitimate user's gesture input. Besides, we only rely on one training data for the legitimate user to test the worst case in the system. The ROC curve in Figure 20(a) shows that we can achieve 3% average false positive rate with 80% true positive rate using EMD + DTW. The EMD-only case shows 8% false positive rate and 80% true positive rate on average. The results show that EMD+DTW technique can provide better authentication performance than using EMD-only.

With the prior knowledge that EMD+DTW produces lower false positives, we next evaluate our system on the advanced grid layout using EMD+DTW technique. Both knowledgeable observer attack and credential-aware attack are evaluated. Figure 20(b) shows that under the knowledgeable observer attack, false positive rate decreases to around 1%, with the true positives remain at around 80%. Under the credential-aware attack, the system achieves a higher false positive rate around 4% with the true positives unchanged. The results indicate that even for the most challenging knowledgeable observer attack, our system is still effective in defending against attackers and can successfully authenticate legitimate users.

8.6 Side-channel Attacks

Attacks via a Vibration Receiver. One may suspect that attackers can place hidden receivers on the authentication surface to recover the vibration signals and obtain the unique features of the legitimate user. However, we observe that the received vibration signals have strong relevance to the placement of the receiving sensor because the captured vibrations comprise multiple components including the direct-path vibrations propagated through the medium surface and the multi-path reflections bounced inside the medium. Therefore, even the malicious hidden receiver is placed next to the system receiver, which increases chances to get exposed, the minor difference in the sensor's position still prevents the attack receiver from capturing the same vibrations as the system receiver. Since sensors cannot be placed at the exact same location as the system receiver, we place sensors at different locations where might be chosen to perform side-channel attack (i.e., adjacent to the original receiver and the other side of the surface opposite to the original receiver). We generate vibration signals 20 times and observe the mean and standard deviation of the Pearson Correlation coefficients [50] between the signals received by the original receiver and adversarial sensors. We find that the correlation coefficients for all adversarial sensors are very low (i.e., less than 0.2), which indicates that the vibration signals received by hidden receivers present very different patterns comparing to those received by the system receiver. The results reveal that the attack via a hidden vibration receiver is ineffective.

Attacks via a Nearby Microphone. A nearby microphone can record the acoustic sounds emitted by the vibration motor. However, a different transmission path (i.e., the air between the sensor and microphone) can largely

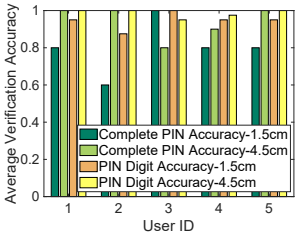


Fig. 23. Verification accuracy of PIN number based authentication with different inter-grid point distances using DNN.

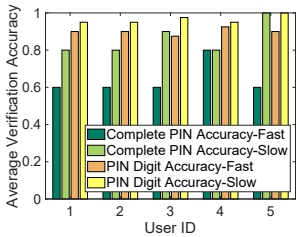


Fig. 24. Verification accuracy of PIN number based authentication with different touching speed using DNN.

change the signal patterns, making it also difficult to recover the similar vibration signals received by the vibration receiver. Additionally, a few new studies demonstrate that physical vibrations can be recovered to a certain extent by using wireless signals [51] and high-speed cameras [52]. However, these solutions can only recover relatively low-quality signals due to the limits of the hardware sensing ability in both vibration amplitude and frequency. Thus, they are mainly used for eavesdropping human speech sounds whose frequency typically falls below $1kHz$.

8.7 Impact of Training Data Size

In PIN number/lock pattern-based verification, our system achieves around 90% accuracy in identifying single PIN digit/lock-pattern segment with the grid point training time over $0.4s$ while the identification accuracy of complete PIN sequences and lock pattern achieve over 80% with the training time over $0.6s$ as shown in Figure 21. Moreover, the PIN sequence/lock pattern based authentication can achieve higher and steadier accuracy when the time is over $2s$. As for the gesture-based authentication, the result is different. Figure 17 and Figure 20(a) show that our gesture-based verification can obtain high authentication accuracy while training with a single gesture and our gesture-based authentication system could work with a very small training data size.

8.8 Impact of Grid Layout and Surface Types

We extend the virtual grid on the authentication surface from 3×3 simple layout to an advanced 4×4 layout, which could facilitate tangible applications such as the secure virtual keyboard and palm authentication. We implement our prototype for both grid layouts on wooden, acrylic and glass surfaces with the testing region resided in between the sensors to evaluate the robustness and scalability of the proposed system. We recruit 10 volunteers to first construct their grid profiles, then press at each PIN index for 10 times. The verification accuracy of SVM and DNN-based prototype both achieve over 95% on the simple grid layout for all testing materials. Particularly, the wood sheet shows the highest average accuracy of 97%, and the acrylic board and glass panel shows 96% authentication accuracy. Different surface dimensions of the same material show very limited impact on the accuracy (less than 2%). The results show that for the simple grid layout, both SVM and DNN classifier can effectively identify users and can be deployed on a broad range of surface types. For the advanced grid layout, the SVM-based prototype shows around 80% verification accuracy due to its intrinsic inefficiency for classifying more grid points. By applying the DNN-enhanced prototype on the advanced grid layout, the system achieves 96% verification accuracy on the wood sheet and the lowest of around 95% on the acrylic and glass panel. Therefore, the developed system possesses high scalability that can meet the requirements of different applications through the flexibility endowed by integrating both SVM and DNN.

8.9 Impact of Inter-Grid Point Distance

The distance between neighboring grid points could be an important factor affecting the input efficiency and verification accuracy of our system. Therefore, in addition to the $3cm$ inter-grid point distance used in the aforementioned evaluations, we further adopt $1.5cm$ and $4.5cm$ inter-grid point distances on a wood panel with a 3×3 simple grid layout to study the impact of inter-grid point distance on the user authentication performance. Particularly, we recruit 5 participants to perform DNN-based PIN authentication on the prototypes with $1.5cm$ and $4.5cm$ inter-grid point distances. For each inter-grid point distance, every participant enters a 4-digit PIN sequence 10 times. As shown in Figure 23, the average accuracy for verifying the complete PIN sequence achieves 80% and 94% for the setup with $1.5cm$ and $4.5cm$ inter-grid point distance, respectively. For verifying the PIN digits, the average verification accuracy for the setup with $1.5cm$ inter-grid point distance is around 95%. For the setup with $4.5cm$ inter-grid point distance, the average accuracy achieves close to 99%. The results show that the verification accuracy decreases when the inter-grid point distance is small (i.e., around $1.5cm$). We find that the user's fingertip is more likely to cover the neighboring grid points when touching on the setup with $1.5cm$ inter-grid point distance. Therefore, the captured vibration signals could contain the patterns from multiple grid points and producing unreliable results. The verification performance for a larger $4.5cm$ inter-grid point distance shows a comparable accuracy to the setup with $3cm$ inter-grid point distance. Given that the inter-key distance for text keys should be less than $5cm$ to achieve ideal input efficiency [53], the optimal inter-grid point distance for real-world deployment could be set as $3cm$ to $4.5cm$ for the balance between input efficiency and verification accuracy.

8.10 Impact of Finger Touching Speed

In the PIN number-based authentication, the finger pressing speed could also determine the stability of vibration signals and affect the verification performance. To investigate the impact of touching speed, we use the same setup as mentioned in Section 8.9. Specifically, 5 participants first construct their grid point index profiles at a natural touching speed (i.e., around $2s$ for each touch). Next, each participant types a 4-digit PIN code for 10 times at a fast speed and a slow speed respectively. For simplicity, we define the touching events that finish within $1s$ as the fast speed, and the touching events that allow the user to naturally press and settle the finger as slow speed. As illustrated in Figure 24, the average accuracy for verifying complete PIN sequence at the fast speed is around 64%, which is lower than the 86% accuracy at slow speed. For the PIN digit verification accuracy, the fast speed remains at around 90% high accuracy, which is only 7% lower than the performance

of slow speed. We find that pressing the grid point in a fast manner is more likely to produce the wrong grid point index and will require more trials to pass the authentication. The reason is that our system continuously samples the vibration signals using a $200ms$ sliding window, hence the captured samples should be dominated by the stable touching state, which starts after the finger fully settles on the surface and ends before the finger lifts. However, for a fast speed touching, the captured vibrations could be dominated by the intermediate touching states, where the user's touching force is continuously changing. As a result, the vibration patterns captured during a fast touch are less similar to the user's grid point index profiles and could result in more errors. The results show that our proposed system is robust to regular finger touching speeds and could keep 90% PIN digit verification accuracy even for the challenging fast touching speed. It is important to note that our experiments do not require users to control their touching force. The users are flexible to perform touching during the experiments. It is our system's unique capability to capture a user's behavioral and physiological characteristics, which helps to distinguish the user's identity.

9 Conclusion

In this paper, we propose a system that implements the idea of low-cost low-power tangible user authentication beyond touch screens to any solid surface to support smart access applications (e.g., apartment entrances, vehicle doors, or smart appliances). Utilizing low-cost physical vibration, our system performs ubiquitous user authentication via finger-input by integrating passcode, behavioral and physiological characteristics, and surface dependency together to provide enhanced security. The system is built upon a vibration-based touch sensing technique that enables touching and writing on any solid surface through analyzing unique vibration signal features (e.g., frequency response and cepstral coefficient). It is easy to deploy and flexibly provides users with three independent forms of secrets (including PIN number, lock pattern, and simple gesture) to gain security access. We perform extensive experiments with participants input their passcodes by using three forms of secrets and also study the robustness under various attacks impersonating the legitimate user or launching side-channel attacks to hack the system. Our results indicate that our system is resilient to side-channel attacks. And it can verify legitimate user with high accuracy under minimum training efforts while successfully deny the access requests from unauthorized users with a low false positive rate.

Acknowledgments

This work was partially supported by the National Science Foundation Grants CNS-1514436, CNS-1716500 and CNS-1526524. Preliminary results of this paper were presented in part at ACM CCS 2017 [16].

References

[1] "Access control market," https://www.marketsandmarkets.com/Market-Reports/access-control-market-164562182.html, 2017.
[2] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594–597, 1979.
[3] R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentication," in *USENIX Security Symposium*, 2000.
[4] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *Proceedings of the 21st Annual Computer Security Applications Conference*. IEEE, 2005.
[5] A. T. Timmons and O. D. Altan, "Grid unlock," Feb. 2 2010, uS Patent App. 12/698,321.
[6] A. De Angeli, M. Coutts, L. Coventry, G. I. Johnson, D. Cameron, and M. H. Fischer, "Vip: a visual approach to user authentication," in *Proceedings of the working conference on advanced visual interfaces (ACM AVI)*, 2002, pp. 316–323.
[7] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication," *Pattern recognition*, vol. 43, no. 3, pp. 1016–1026, 2010.
[8] A. Arakala, J. Jeffers, and K. J. Horadam, "Fuzzy extractors for minutiae-based fingerprint authentication," in *International Conference on Biometrics*. Springer, 2007, pp. 760–769.
[9] C. Mariño, M. G. Penedo, M. Penas, M. J. Carreira, and F. Gonzalez, "Personal authentication using digital retinal images," *Pattern Analysis and Applications*, vol. 9, no. 1, pp. 21–33, 2006.
[10] B. Duc, S. Fischer, and J. Bigün, "Face authentication with gabor information on deformable graphs," *IEEE Transactions on Image Processing*, vol. 8, no. 4, pp. 504–516, 1999.
[11] 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 the 18th annual international conference on Mobile computing and networking*. ACM, 2012, pp. 197–208.
[12] P. Nguyen, U. Muncuk, A. Ashok, K. R. Chowdhury, M. Gruteser, and T. Vu, "Battery-free identification token for touch sensing devices," in *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*. ACM, 2016, pp. 109–122.
[13] "How to implement fingerprint authentication in automobiles," https://www.electronicproducts.com/Sensors_and_Transducers/Sensors/How_to_implement_fingerprint_authentication_in_automobiles.aspx, 2017.
[14] "Capacitive sensor," http://www.sensorwiki.org/doku.php/sensors/capacitive, 2017.
[15] S. P. Tarzia, P. A. Dinda, R. P. Dick, and G. Memik, "Indoor localization without infrastructure using the acoustic background spectrum," in *Proceedings of the 9th international conference on Mobile systems, applications, and services (ACM MobiSys)*, 2011.
[16] J. Liu, C. Wang, Y. Chen, and N. Saxena, "Vibwrite: Towards finger-input authentication on ubiquitous surfaces via physical vibration," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 73–87.
[17] J. Chen, C. Wang, and R. Wang, "Adaptive binary tree for fast svm multiclass classification," *Neurocomputing*, vol. 72, no. 13-15, pp. 3370–3375, 2009.
[18] M. Aly, "Survey on multiclass classification methods," *Neural Netw*, vol. 19, pp. 1–9, 2005.
[19] A. Taravat, F. Del Frate, C. Cornaro, and S. Vergari, "Neural networks and support vector machine algorithms for automatic cloud classification of whole-sky ground-based images," *IEEE Geoscience and remote sensing letters*, vol. 12, no. 3, pp. 666–670, 2014.
[20] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Computer Security–ESORICS 2007*. Springer, 2007, pp. 359–374.
[21] W. Meng, W. Li, L. Jiang, and L. Meng, "On multiple password interference of touch screen patterns and text passwords," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 4818–4822.
[22] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the working conference on Advanced visual interfaces*. ACM, 2006, pp. 177–184.
[23] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 1107–1110.
[24] K. Revett, "A bioinformatics based approach to user authentication via keystroke dynamics," *International Journal of Control, Automation and Systems*, vol. 7, no. 1, pp. 7–15, 2009.
[25] N. Zheng, A. Paloski, and H. Wang, "An efficient user verification system via mouse movements," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 139–150.

[26] Y. Ren, Y. Chen, M. C. Chuah, and J. Yang, "User verification leveraging gait recognition for smartphone enabled mobile healthcare systems," *IEEE Transactions on Mobile Computing*, vol. 14, no. 9, pp. 1961–1974, 2015.

[27] T. Ohshima, T. Morita, T. Tanaka, and N. Yamamoto, "Indoor apparatus of intercom system and method for controlling indoor apparatus," June 22 2006, US Patent App. 11/472,432.

[28] J. Tian, C. Qu, W. Xu, and S. Wang, "Kinwrite: Handwriting-based authentication using kinect." in *NDSS*, 2013.

[29] M. I. Rose and L. W. Hoevel, "Access card for multiple accounts," June 23 1998, US Patent 5,770,843.

[30] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: implicit authentication based on touch screen patterns," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2012, pp. 987–996.

[31] Y. Ren, C. Wang, Y. Chen, M. C. Chuah, and J. Yang, "Critical segment based real-time e-signature for securing mobile transactions," in *Proceedings of IEEE Conference on Communications and Network Security (CNS)*, 2015, pp. 7–15.

[32] M. Sherman, G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvirta, and T. Roos, "User-generated free-form gestures for authentication: Security and memorability," in *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*. ACM, 2014, pp. 176–189.

[33] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," *Woot*, vol. 10, pp. 1–7, 2010.

[34] R. Dong, A. Schopper, T. McDowell, D. Welcome, J. Wu, W. Smutz, C. Warren, and S. Rakheja, "Vibration energy absorption (vea) in human fingers-hand-arm system," *Medical engineering & physics*, vol. 26, no. 6, pp. 483–492, 2004.

[35] K. S. R. Murty and B. Yegnanarayana, "Combining evidence from residual phase and mfcc features for speaker recognition," *IEEE Signal Processing Letters*, vol. 13, no. 1, pp. 52–55, 2006.

[36] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern classification*. John Wiley & Sons, 2012.

[37] G. A. ten Holt, M. J. Reinders, and E. Hendriks, "Multi-dimensional dynamic time warping for gesture recognition," in *Thirteenth annual conference of the Advanced School for Computing and Imaging*, vol. 300, 2007.

[38] Y. Rubner and S. U. C. S. Dept, *Perceptual metrics for image database navigation*, ser. Report STAN-CS-TR. Stanford University, 1999, no. 1621. [Online]. Available: http://books.google.com/books?id=5b1EAQAAIAAJ

[39] P. G. Kannan, S. P. Venkatagiri, M. C. Chan, A. L. Ananda, and L.-S. Peh, "Low cost crowd counting using audio tones," in *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, 2012, pp. 155–168.

[40] B. Sklar, *Digital communications*. Prentice Hall NJ, 2001, vol. 2.

[41] C.-C. Chang and C.-J. Lin, "Libsvm: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, pp. 27:1–27:27, 2011, software available at url-http://www.csie.ntu.edu.tw/ cjlin/libsvm.

[42] L. Bottou, C. Cortes, J. S. Denker, H. Drucker, I. Guyon, L. D. Jackel, Y. LeCun, U. A. Müller, E. Säckinger, P. Y. Simard *et al.*, "Comparison of classifier methods: a case study in handwritten digit recognition," in *International conference on pattern recognition*. IEEE Computer Society Press, 1994, pp. 77–77.

[43] J. H. Friedman, "Another approach to polychotomous classification," *Technical Report, Statistics Department, Stanford University*, 1996.

[44] J. C. Platt, N. Cristianini, and J. Shawe-Taylor, "Large margin dags for multiclass classification," in *Advances in neural information processing systems*, 2000, pp. 547–553.

[45] J. Weston and C. Watkins, "Multi-class support vector machines," Citeseer, Tech. Rep., 1998.

[46] F. Schwenker, "Hierarchical support vector machines for multi-class pattern recognition," in *KES'2000. Fourth International Conference on Knowledge-Based Intelligent Engineering Systems and Allied Technologies. Proceedings (Cat. No. 00TH8516)*, vol. 2. IEEE, 2000, pp. 561–565.

[47] S. Han, H. Mao, and W. J. Dally, "Deep compression: Compressing deep neural networks with pruning, trained quantization and huffman coding," *arXiv preprint arXiv:1510.00149*, 2015.

[48] P. B. e. a. Martín Abadi, Ashish Agarwal, "TensorFlow: Large-scale machine learning on heterogeneous systems," 2015, software available from tensorflow.org. [Online]. Available: https://www.tensorflow.org/

[49] S. Han, J. Pool, J. Tran, and W. Dally, "Learning both weights and connections for efficient neural network," in *Advances in neural information processing systems*, 2015, pp. 1135–1143.

[50] "Pearson product moment correlation coefficient," http://en.wikipedia.org/wiki/Pearson-product-moment-correlation-coefficient, 2017.

[51] T. Wei, S. Wang, A. Zhou, and X. Zhang, "Acoustic eavesdropping through wireless vibrometry," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 2015, pp. 130–141.

[52] A. Davis, M. Rubinstein, N. Wadhwa, G. J. Mysore, F. Durand, and W. T. Freeman, "The visual microphone: passive recovery of sound from video," *ACM Transactions on Graphics*, 2014.

[53] S. K. Card, W. K. English, and B. J. Burr, "Evaluation of mouse, rate-controlled isometric joystick, step keys, and text keys for text selection on a crt," *Ergonomics*, vol. 21, no. 8, pp. 601–613, 1978.

Xin Yang is currently a Ph.D. student at Wireless Information Network Laboratory (WINLAB), Rutgers University. His research interests include mobile sensing and computing, and machine learning. He received his B.E. degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China, and his M.S. degree from the Department of Electrical and Computer Engineering, Rutgers University.

Song Yang is currently pursuing his Ph.D. degree at Wireless Information Network Laboratory (WINLAB) and Data Analysis and Information Security (DAISY) Laboratory, Department of Electrical and Computer Engineering, Rutgers University. He received his M.S. degree from the Department of Electrical and Computer Engineering, Rutgers University, and his B.E. degree from the School of Information and Software Engineering, the University of Electronic Science and Technology of China (UESTC). His current research interests include mobile sensing and cyber security/privacy.

Jian Liu is an Assistant Professor in the Department of Electrical Engineering and Computer Science at the University of Tennessee, Knoxville. He received his Ph.D. degree in Wireless Information Network Laboratory (WINLAB) at Rutgers University. His current research interests include mobile sensing and computing, cybersecurity and privacy, intelligent systems and machine learning. He is the recipient of the Best Paper Awards from IEEE SECON 2017 and IEEE CNS 2018. He also received Best-in-session Presentation Award from IEEE INFOCOM 2017, and two Best Poster Award Runner-up from ACM MobiCom 2016 and 2018.

Chen Wang is currently an Assistant Professor at Louisiana State University. He received his Ph.D. degree at Rutgers University under the supervision of Dr. Yingying Chen in 2019. He received his BS and MS degrees from the University of Electronic Science and Technology of China, in 2009 and 2012. His research interests include cyber security and privacy, smart health care, mobile sensing and computing. He received three Best Paper Awards from IEEE Conference on Communications and Network Security (CNS 2018), ACM Conference on Information, Computer and Communications Security (ASIACCS 2016) and IEEE CNS 2014. He won the Best Poster Runner-up from ACM MobiCom 2018. His four research studies have been reported by over 150 media outlets, including IEEE Spectrum, NSF Science 360, CBS TV, BBC News, NBC, IEEE Engineering 360, Fortune, ABC News, MIT Technology Review, etc.

Yingying (Jennifer) Chen is a Professor and Peter Cherasia Endowed Faculty Scholar of Electrical and Computer Engineering at Rutgers University. She is the Associate Director of Wireless Information Network Laboratory (WINLAB). She also leads the Data Analysis and Information Security (DAISY) Lab. She is an IEEE Fellow. Her research interests include mobile sensing and computing, cyber security and privacy, Internet of Things, and smart healthcare. Her background is a combination of Computer Science, Computer Engineering and Physics. She had extensive industry experiences at Nokia previously. She has published over 200 journal articles and conference papers. She is the recipient of multiple Best Paper Awards from EAI HealthyIoT 2019, IEEE CNS 2018, IEEE SECON 2017, ACM AsiaCCS 2016, IEEE CNS 2014 and ACM MobiCom 2011. She is also the recipient of NSF CAREER Award and Google Faculty Research Award. She received NJ Inventors Hall of Fame Innovator Award and is also the recipient of IEEE Region 1 Technological Innovation in Academic Award. Her research has been reported in numerous media outlets including MIT Technology Review, CNN, Fox News Channel, Wall Street Journal, National Public Radio and IEEE Spectrum. She has been serving/served on the editorial boards of IEEE Transactions on Mobile Computing (IEEE TMC), IEEE Transactions on Wireless Communications (IEEE TWireless), IEEE/ACM Transactions on Networking (IEEE/ACM ToN) and ACM Transactions on Privacy and Security.

Nitesh Saxena is a Professor of Computer and Information Sciences at the University of Alabama at Birmingham (UAB), and the founding director of the Security and Privacy in Emerging Systems (SPIES) group/lab. He works in the broad areas of computer and network security, and applied cryptography, with a keen interest in wireless and mobile device security, and the emerging field of usable security. Saxena's current research has been externally supported by multiple grants from NSF and NIJ, and by gifts/awards/donations from the industry, including Google (2 Google Faculty Research awards), Cisco, Comcast, Intel, Nokia and Research in Motion. He has published over 110 journal, conference and workshop papers, many at toptier venues in Computer Science, including: IEEE Transactions, ISOC NDSS, ACM CCS, ACM WWW, ACM WiSec, ACM ACSAC, ACM CHI, ACM Ubicomp, IEEE Percom, IEEE ICME and IEEE S&P. On the educational/service front, Saxena currently serves as the director and principal investigator for the UAB's Scholarship for Service (SFS) program and a co-director for UAB's MS program in Computer Forensics and Security Management. He serves as an Associate Editor for flagship security journals, IEEE Transactions on Information Forensics and Security (TIFS), and Springer's International Journal of Information Security (IJIS). Saxena's work has received extensive media coverage, for example, at NBC, MSN, Fox, Discovery, ABC, Bloomberg, MIT Tech Review, ZDNet, ACM TechNews, Yahoo! Finance, Communications of ACM, Yahoo News, CNBC, Slashdot, Computer World, Science Daily and Motherboard.