HandKey: Knocking-Triggered Robust Vibration Signature for Keyless Unlocking

Hangcheng Cao, *Student Member, IEEE*, Daibo Liu, *Member, IEEE*, Hongbo Jiang, *Senior Member, IEEE*, Chao Cai, Tianyue Zheng, *Graduate Student Member, IEEE*, John C. S. Lui, *Fellow, IEEE*, and Jun Luo, *Senior Member, IEEE*

Abstract—Door lock is regarded as a critical line of defending the privacy and security of personal areas. However, for inner doors in environments like factories, existing locking mechanisms can be poor in user-friendliness and high in cost. For instance, mechanical locks require carrying keys that inevitably compromise user experiences, while smart locks always require non-trivial sensors. Therefore, inner doors urgently require a lightweight unlocking scheme that can properly balance user-friendliness, cost, and security. To this end, we propose HandKey as a keyless unlocking scheme to supplement existing lock systems. HandKey relies on two principles: the simplicity of hand knocking doors and the uniqueness of vibration triggered by the knocking force. In other words, a door and a hand knocking it jointly form a unique physical system that generates hand-dependent and user-specific vibration signatures uniquely representing a user identity. In designing HandKey, we first analyze the vibration mechanism behind it and the impacts of gestures and door materials on vibration signatures. Then we innovatively construct a signal processing and deep learning-based pipeline to extract signatures robust to variable knocking behaviors for representing user identity. Finally, we implement a HandKey prototype and use extensive evaluation to demonstrate its security and effectiveness.

Index Terms—Authentication, behavior-independent signature, keyless unlocking, vibration signature

1 Introduction

Door locksalways play a key role in preventing illegitimate invasion and hence protecting personal security. However, for environments accommodating multiple users (e.g., companies or institutes), inner doors are only applied to restrict personnel activity areas. Therefore, their dominating requirements for locks are *low cost*, *user-friendliness*, as well as an adequate *security level (in particular, robustness to theft and counterfeit)*. Unfortunately, current unlocking mechanisms often cannot fully meet these requirements. To illustrate the mismatches between functionalities and requirements, we consider three main categories of unlocking schemes: i) mechanical key or electronic card [1], [2], ii) keyless access via passwords or drawing patterns [3], [4], and iii) biometrics-based identity verification [5], [6].

Category i) requires users to carry physical keys/cards at all times. As losing and forgetting them inevitably happen in human daily life, such mechanisms sometimes cause terrible user experience [7]. In practice, relying on permission managers to recover from this loss is both cumbersome and lacking of timeliness. Most importantly, an illegitimate person can steal the magnetic stripe or utilize the near-field communication technology [8] to slinkingly replicate entrance accessing permission, thus gaining free entrance to sensitive areas like personal offices. Category ii) aims to bring better user experiences and security, but the current performance is far from satisfactory; it demands users to remember tedious numbers and then manually input them when unlocking. Since each user often owns not just one but a lot of accounts (e.g., online banks and instant messaging applications) entailing distinct passwords, remembering them becomes a heavy burden. Moreover, password/patterns do raise security risk as they can be stolen by peeping [3] and side-channel [9] attacks.

Thanks to its keyless nature (thus the resulting security and convenience), category iii) has been widely adopted on smart locks, yet they necessitate multiple non-trivial sensors to identify user biometrics reliably, resulting in a high cost and hence not suitable for inner-door locks. For instance, FaceID [10] demands a structured light system to capture facial 3D features with flood illuminators, dot projectors, and an infrared camera, greatly increasing hardware costs. Qualcomm Fingerprint Sensor [11] leverages non-trivial

- *Hangcheng Cao, Daibo Liu, and Hongbo Jiang are with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan 410082, China. E-mail: {hangchengcao, dbliu}@hnu.edu.cn, hongbojiang2004@gmail.com.*
- *Chao Cai is with the College of Life Science and Technology, Huazhong University of Science and Technology, Wuhan, Hubei 430074 USA. E-mail: caichao08@gmail.com.*
- *Tianyue Zheng and Jun Luo are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798. E-mail: tianyue002@e.ntu.edu.sg, junluo@ntu.edu.sg.*
- *John C. S. Lui is with the Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong. E-mail: cslui@cse.cuhk.edu.hk.*

Manuscript received 11 April 2022; revised 24 July 2022; accepted 17 October 2022. Date of publication 25 October 2022; date of current version 5 December 2023.
This work was supported in part by the National Natural Science Foundation of China under Grants U20A20181, 61732017, 61902122 and 61902060, China Scholarship Council (CSC), and in part by the National Social Science Foundation of China under Grant 19ZDA103.
(Corresponding author: Hongbo Jiang.)
Digital Object Identifier no. 10.1109/TMC.2022.3216868

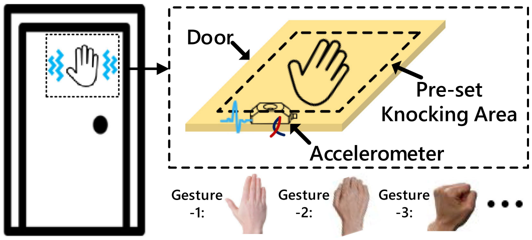


Fig. 1. The usage illustration of HandKey: a predefined knocking area and three typical knocking gestures.

ultrasonic readers to construct accurate fingerprint images by scanning the pores of a user's fingers. In addition, recent proposals [12], [13] leverage vibration signals emitted by motors in wearable devices to authenticate users: they both argue that identical vibration waves, after propagating through arms and fingers, become signatures unique to individual users. However, requiring user-held devices has compromised the keyless promise of this category.

Given that existing schemes largely fail to meet the main requirements for inner-door locks, namely, low-cost, user-friendliness, and robustness to theft and counterfeit, it is imperative to look for alternatives. To this end, we plan to exploit two properties inherent to hand knocking doors, to fully meet the aforementioned unlocking requirements. On one hand, knocking on doors by hand is easy to operate for users, as it has been used for thousands of years as a gesture to ask a door to be opened. On the other hand, thanks to the intrinsic differences among human users in bone structure, muscle distribution, and shape of hands [14], physical contact between hand and door jointly forms a unique system. Triggered by the knocking force, this system generates hand-dependent vibration signals unique to individual users. These two properties have motivated us to ask the following question: *can we employ simple knocking operations and unique hand-dependent vibration signals to realize an adequate unlocking approach for inner doors?*

In response to this question, we specifically leverage the aforementioned two properties to construct *HandKey* as a keyless unlocking scheme in this paper. Basically, HandKey employs user-specific vibration signatures created by hand knocking as "keys," and it verifies signatures after sensing them via an accelerometer. As illustrated in Fig. 1, a user knocks on a *pre-set knocking area*[1] to unlock a door. HandKey adopts an accelerometer to record the induced vibration signatures and then verifies the feature similarity between newly captured and registered signatures, so as to determine whether to unlock or not. The adequacy and effectiveness of HandKey manifest in four aspects:

- HandKey leverages a common accelerometer to complete data collection, ensuring a low hardware cost.
- Users need only to execute hand knocking during authentication, imposing minimal user involvement and thus being very user-friendly.
- The combination of a hand and door forms a unique structure, physically guaranteeing the uniqueness of vibration signatures for authentication purpose.
- The signature generation strongly relies on the structure of user hands, making it impossible for attackers to replicate signatures and hence ensuring the security of HandKey.

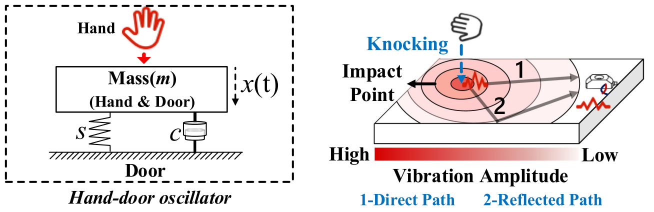
However, implementing HandKey faces several technical challenges. First of all, though deeming the hand-door as an oscillator excited by the knocking force is theoretically sound, the intrinsic properties of this oscillator are unknown without prior knowledge of the mutual interactions within the oscillator. Second, the knowledge on extracting what effective features from the vibration signals to characterize user identity is also missing. Third, subtle changes in knocking behavior can lead to varying signatures even from the same hand, so achieving behavior-robustness is crucial but challenging. To tackle these challenges, we first analyze the working principles of the hand-door oscillator and reveal decisive factors such as mass and spring constant crucial to vibration generation. We explore the signature variations caused by different knocking gestures and door materials in a feasibility study, establishing a foundation for the development of HandKey. Second, we specifically design a learning-driven signal processing module to transform original vibration signals into user identity features; it involves Discrete Wavelet Transform (DWT) [15] based noise removal and Variational Auto-Encoder (VAE) [16] feature extraction. Finally, we apply a typical LeNet [17] network to construct Triplet model [18] for obtaining behavior-independent signatures robust to user behaviors; these signatures are taken to drive the authentication process that compares a new signature with multiple stored templates associated with an identity and determines its authenticity via voting.

In summary, our main contributions in designing HandKey are summarized as follows:

- We propose a lightweight keyless unlocking method HandKey for inner doors; it delivers adequate security, smooth user experience, and low cost.
- We analyze the vibration mechanism and key parameters of the hand-door oscillator, thereby revealing the reason for signature uniqueness across users.
- We design a series of strategies for obtaining linear time-frequency features via PCA and non-linear features via VAE, aiming to effectively characterize a user identity.
- We leverage a LeNet-based network to build a Triplet model, in order to extract behavior-independent vibration signatures robust to variations in knocking behavior.
- We implement a HandKey prototype and conduct comprehensive experiments to validate its effectiveness; The promising results demonstrate that our method can achieve an accuracy of 97.71%.

The remainder of this paper is organized as follows. Section 2 introduces vibration mechanism and investigates the feasibility of using hand-dependent vibration signals for keyless door unlocking. Potential attacks and system overview are presented in Section 3. We elaborate the technical details in Section 4, and report the implementation and performance

[1] Distance changes between knocking positions and the accelerometer sensor, can directly lead to similarity reduction of vibration signatures generated by the same user. Therefore, we preset a knocking area on a door to ensure that positions of multiple hand knocks are close to each other as much as possible.



(a) The mass-spring-damper model of hand-door oscillator.

(b) Vibration attenuation during the propagation phase.

Fig. 2. The illustration of vibration generation and propagation.

evaluation of HandKey respectively in Sections 5 and 6. After discussing limitations and related works in Sections 7 and 8, we finally conclude this paper in Section 9.

2 Background and Feasibility Analysis

In this section, we first introduce a simple yet effective model to characterize vibration generation and propagation. Then we perform feasibility studies to corroborate the theoretical uniqueness of vibration signatures, justifying using them for authenticating users. Finally, we demonstrate the behavior impacts on vibration signatures, aiming to concretely motivate our latter design.

2.1 Vibration Mechanism of Hand Knocking Door

When a hand knocks on a door, the *force-bearing area* (i.e., the contact area between them) is deformed and thus generates vibration waves. Vibration generation and propagation depend on structure properties such as spring constant and damper coefficient of both hand and door, which jointly form an oscillator [19]. Therefore, knocking on the same door by the hand of a certain user should produce user-specific vibration signatures. More importantly, as the hand structure parameters such as bone and shape are important determining factors of this oscillator, it is highly possible that changes in them may significantly alter the vibration signature. Therefore, we construct a simple model to reveal this potential impact (hence the *uniqueness* of vibration signature for individual users) in the following.

As a forced spring system [20], the process of vibration generation in the *hand-door oscillator* involves two stages: compression and stretch. In the first stage, the force of hand waving is exerted on doors, causing the force-bearing area and hand to squeeze against each other and hence transforming kinetic energy into elastic potential energy. This stage ends with the force-bearing area deforms to its greatest extent when the exerted force offsets the resistance of the door material. In the second stage, the force-bearing area begins to gradually restore its original state, releasing energy and generating vibrations. To describe this process, we adopt the well-known mass-spring-damper model [21]. As shown in Fig. 2a, the hand-door oscillator can be characterized using its mass m, spring constant s, and damper coefficient c. In our case, these parameters are determined by the bone, muscle, and shape users' hands, making the structure of an oscillator uniquely determined by a user [14]. According to Hooke's law [22] and Newton's second law [23], we formulate the relation between the knocking force $f_{t=0}$ and the vertical displacement of door surface $x(t)$ (i.e., the *vibration signature*) as follows:

$$f_{t=0} = ma(t) + cv(t) + sx(t), \tag{1}$$

where $a(t)$ and $v(t)$ are respectively the acceleration and speed of the door. Leveraging the physical relation among acceleration, speed, and displacement [24] allows us to further simplify Eqn. (1) as

$$f_{t=0} = m\frac{d^2x(t)}{dt^2} + c\frac{dx(t)}{dt} + sx(t). \tag{2}$$

According to Eqn. (2), the vibration signature $x(t)$ is uniquely determined by parameters m, s, and c given the knocking force $f_{t=0}$. Moreover, as changes in $f_{t=0}$ only affect vibration amplitude, the shape of vibration envelope (morphology) can be regarded as a unique signature.

Vibration signal $x(t)$ is generated in the force-bearing area and then propagates outward through the hand-door oscillator, which is eventually sensed by an accelerometer fixed on the door. The propagation process consists of two distinct parts. On one hand, the signal waveform propagates along a line (a.k.a. *direct path*) towards the accelerometer. On the other hand, vibration waves reaching the medium boundary can be refected towards the accelerometer and hence form *reflected paths*. Though there could be multiple refected paths caused by various medium boundaries, we only show one refected path as an example in Fig. 2b for the sake of brevity. During this process, vibration amplitude continuously attenuates, which is characterized by the following vibration attenuation model [25]

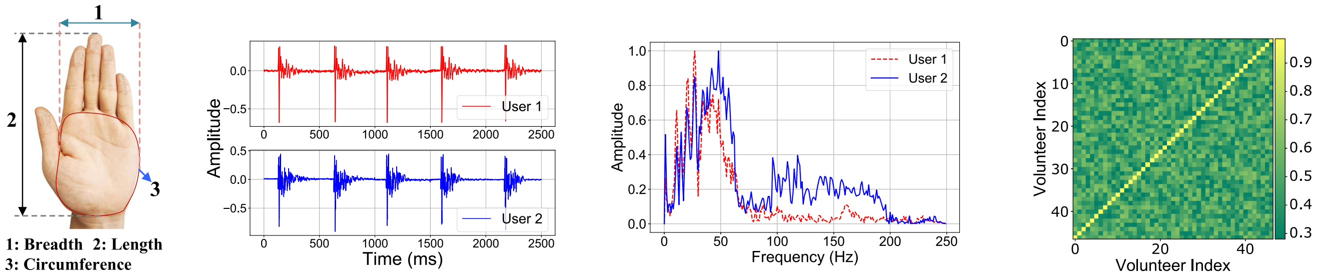
$$y(t) = x(t)e^{-\mu r}, \tag{3}$$

where μ is the attenuation coefficient of medium structure, and r is the propagation distance between the impact point and accelerometer. Different door materials may lead to distinct values of the coefficient μ, which in turn affects the attenuation of $x(t)$ during propagating.

2.2 Feasibility Study on Vibration for Authentication

In this section, we conduct a feasibility study to corroborate the theoretical analysis presented in the previous section. As illustrated in Fig. 1, we deploy a BU-27135 accelerometer with a sampling rate of 10 kHz in the bottom position of preset knocking area, for sensing vibration in real-time. Unless otherwise specified, all users use their right hands with Gesture − 1 (Fig. 1) to knock on a wooden door, and they keep their hands on the door for about two seconds, for largely preserving the oscillator structure during the vibration propagation.

The *uniqueness of vibration signatures* to represent corresponding user identities is the foundation of our design. To verify its uniqueness, we first let two users with identical hand shapes knock on a door five times utilizing the same gesture and position. Hand shape is measured by three critical parameters, i.e., length, breadth, and circumference shown in Fig. 3a, according to a study from NASA [26]. The signals sensed by the accelerometer are shown in Figs. 3b and 3c. One may clearly discern the differences between two time domain waveforms, and the spectral densities of them also present distinct distributions: one concentrates below 80 Hz while another up to around 200 Hz. Therefore, even with identical hand shapes, differences in internal structures



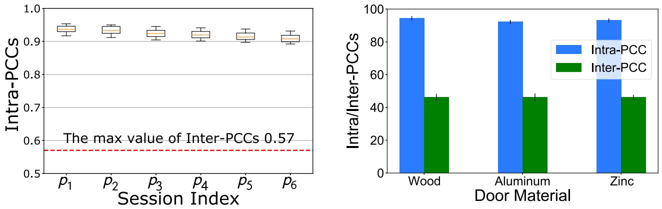
(a) Hand shape. (b) Time domain signatures. (c) Frequency domain signatures. (d) Vibration signal similarity.

Fig. 3. An illustration of hand-shape parameters (a). Vibration signatures generated by two human hands while each knocking the door five times (b) and their frequency domain versions (c). Similarities of vibration signatures among 47 users (d).

such as muscle tissue and bone, still ensure the uniqueness of vibration signatures. We further calculate Pearson Correlation Coefficient (PCC) [27] of two arbitrary signatures from the same user (referred to as Intra-PCC) and across distinct users (Inter-PCC). PCC is an accurate and effective method to measure sample similarity. Fig. 3d presents signature similarities of 47 users; the minimum Intra-PCC is 0.91 much higher than the maximum Inter-PCC value at 0.57. These results confirm that vibration signatures across users can be correctly classified and hence have potential to effectively represent user identities.

The *long-time stability of vibration signatures* is another necessary condition for our design to be practical. To confirm this stability, we ask users to knock on doors at six regularly spaced time periods $p_1, p_2, \ldots, p_6$ during the last three months. They knock ten times during each period and intervals between adjacent periods are about 15 days. Subsequently, to verify the stability of vibration signatures, we calculate PCCs between signatures (of the same user) collected during p_1 those from other periods. As shown in Fig. 4a, with a three-month time span between p_1 and p_6, the average value of Intra-PCCs drops by only 0.05 and still maintains a large difference from Inter-PCCs. This indicates that vibration signature, as biometrics, is sufficiently stable during a long-time period.

The *variations in knocking door material* may also affect the vibration signatures, as door is part of the oscillator. To quantify the impact of door materials, we let users knock on different types of doors, i.e., wood, aluminum, and zinc alloy, while each type includes five distinct thicknesses. Subsequently, we report the average Intra/Inter-PCCs in Fig. 4b, which indicates a sufficiently wide gap between Intra- and Inter-PCCs for each material (consisting of one type with five thicknesses). Therefore, we may safely deem the door material as having insignificant impact on the vibration signature, hence it can be neglected in our latter design.



(a) Temporal stability of PCCs. (b) Impacts of door materials.

Fig. 4. Variations in vibration signature similarity as (a) the time interval increases from half a month to three months and (b) under three distinct door materials.

In addition to the uniqueness confirmed earlier, another important property of the vibration signature is its *non-replicability*. In other words, no one can fake the hand of a legitimate user, because many features of a hand (e.g., its bond structure and muscle) that determine the vibration signatures are intrinsic and hence cannot be replicated even with sophisticated anatomy. This is in sharp contrast to other biometrics such as fingerprint and iris: they stay on the surface of human bodies and thus may often be replicated.

2.3 Interference From Knocking Behavior

Except for the inherent structure of hands and doors, the effects of knocking behavior imposing on final output vibration signatures should be attached with great importance. The most obvious is that adjusting knocking gestures can directly change the whole oscillator structure. To study its effects, we let users knock on a door using three common gestures (i.e., Gesture – 1/2/3 in Fig. 1), while each of them offers the total of thirty vibration signatures. The average Intra-PCC and Inter-PCC of them in each gesture as displayed in Fig. 5. For HandKey, a sufficiently large difference between Intra-PCC and Inter-PCC indicates that signatures are unique across users while consistent for the same user. It is clear that Gesture – 1 performs the best in this sense, while the other two gestures perform slightly worse but still offer sufficient discriminability.

By reviewing vibration mechanism, the reasons for performance differences among gestures become clear: the parameters such as spring and damping coefficients of an oscillator's sub-components can impose more impacts on output vibration signals, when their contact areas become larger [28]. Gestures having larger force-bearing areas with door allow the hand structure traits to be more involved in the oscillator, thereby ensuring the signature uniqueness/discriminability. Therefore, we recommend users to choose

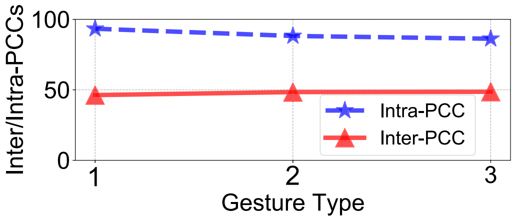
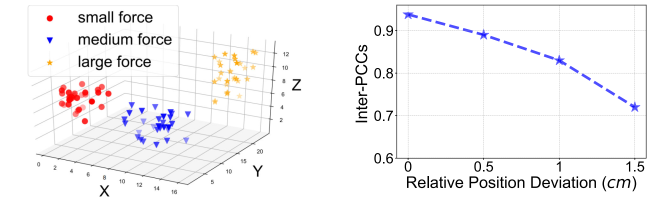


Fig. 5. The signature similarity under three common knocking gestures.



(a) Signature clustering by t-SNE. (b) Impact of knocking position.

Fig. 6. Signature similarity decreasing caused by user behavior changes: (a) knocking strength and (b) position.

gestures with large force-bearing areas for enhancing signature uniqueness.

Moreover, we have learnt from Eqn. (2) and (3) that knocking force $f_{t=0}$ and distance r, though not affecting the signature morphology, may still cause inconsistency between registered and newly sensed signatures of the same user; they potentially result in a higher false positive or negative rate. To explore the effects brought by $f_{t=0}$, we first ask one user to knock with three distinct forces (i.e., small, medium, and large). t-SNE [29] is then leveraged for clustering similar samples in an adjacent three-dimensional space, thereby visually analyzing the similarity of these signatures. As illustrated in Fig. 6a, the strength of $f_{t=0}$ slightly changes the distribution support of the resulting signatures, thereby reducing Intra-PCCs and causing a higher ratio of rejecting legitimate users. Moreover, to study the impact of distance deviation on vibration signatures, we let users knock on four positions, while the first one is away from others with 0.5 cm, 1 cm, and 1.5 cm respectively. Fig. 6b displays signature similarity decreasing to 0.72 as position deviation increases to 1.5 cm; these results also indicate a potentially higher false positive rate. To maintain the performance vibration signature under the above two factors, we plan to leverage suitable deep learning model to distill *behavior-independent signature* robust to these factors, and we also consider setting a knocking area on the door to limit force-bearing range and hence confining the position deviation within a tolerable range.

3 Potential Attacks and System Overview

In this section, we first introduce potential attacks threatening unlocking security and then present the detailed workflow of HandKey.

3.1 Attack Models

We assume that Alice is an attacker who tries to spoof HandKey, for illegitimately entering Bob's private space. Considering the existing approaches and actual scenarios for compromising identity verification system, Alice enacts the following attacks:

- *Zero-effort Attack*. Alice does not master any information (e.g., knocking gesture, force, and position) about how Bob unlocks a door by HandKey. Without prior knowledge, Alice attempts to unlock the door by aimless knocking. This type of attack is easy to operate and hence ordinary attackers can perform it.
- *Imitation Attack*. We assume that Alice has a chummy relationship with Bob, thus he/she can stand around Bob and observe how to use HandKey. Moreover, Alice records the complete unlocking process through a latent camera and then practices to imitate Bob's knocking behaviors. Finally, Alice relying on this useful information tries to trick HandKey. Imitation attack is regarded as an effective way to deceive unlocking schemes that leveraging behavior traits, so being widely discussed in existing authentication works [30], [31], [32].
- *Side-channel Attack*. Alice tries to place an accelerometer in inconspicuous positions to record vibration signatures when a legitimate user knocking on the door. He/she then releases captured vibration waves through adjustable motors to spoof HandKey. This approach sounds promising yet is short of implementability. We detailedly explain the reasons for its invalidation in Section 6.10.

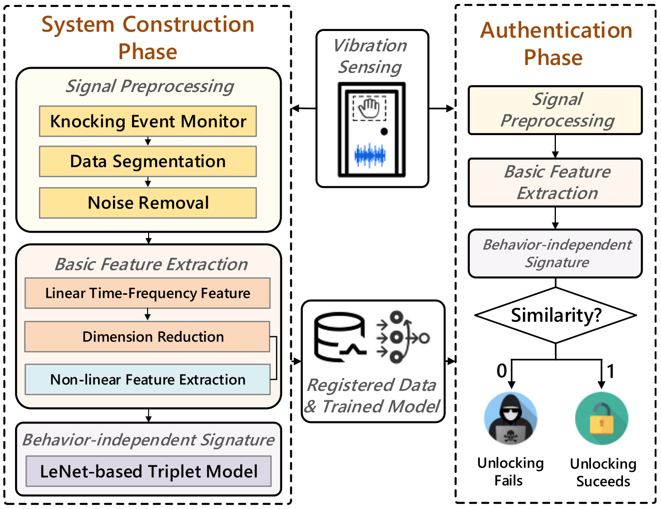
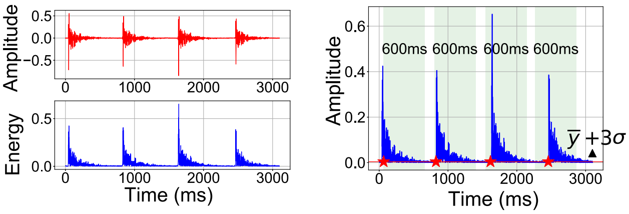


Fig. 7. The workflow of HandKey, including four major modules: vibration sensing, signal preprocessing, basic feature extraction, and behavior-independent signature.

3.2 HandKey Overview

On the basis of running state, HandKey's workflow (illustrated in Fig. 7) can be divided into two major phases: system construction and authentication. In fact, both phases involve almost the same data processing flow, except that the latter phase executes a comparison between newly captured user signatures with the registered ones obtained during the former phase. Therefore, we focus on discussing the construction phase, but leave design details to Section 4.

In *Vibration Sensing*, users knock on the pre-set knocking area with habitual gestures and forces, for registering identity signatures. HandKey then detects knocking event and segments vibration data corresponding to user signature from original signals, in *Knocking Event Monitor* and *Data Segmentation* respectively. Considering user experience, HandKey allows users to knock with relatively small forces. In this case, sensed vibration amplitude and signal-to-noise ratio of signature are both low. Therefore, we design a Discrete Wavelet Transform (DWT) [15] based method in *Noise Removal*, to filter inherent noise caused by electronic components. Subsequently, we extract Mel-Frequency Cepstral Coefficients (MFCCs) [33] based linear fine-grained features in *Linear Time-frequency Feature* while relying on Principal Component



(a) Sensed vibration signals. (b) Starting points recognition.

Fig. 8. Knocking event (a) and vibration signal segmentation (b).

Analysis (PCA) in *Dimension Reduction* to compress the feature dimension. Afterward, Variational AutoEncoder (VAE) [16] based *Feature Extractor* obtains latent non-linear characteristics derived from hand structure. To sum up, linear and non-linear features respectively and complementarily represent the basic and latent hand structure attributes from vibration signals. Finally, as these original features may not well handle the interference caused by behavior changes, we designed a LeNet-based Triplet model to extract behavior-independent signatures and hence ensure the robustness of HandKey.

4 HandKey Design

In this section, we detailedly introduce the technical modules of HandKey, mainly involving knocking event detection, noise data removal, basic feature extraction, and obtaining behavior-independent signature.

4.1 Signal Preprocessing

4.1.1 Knocking Detection and Data Segmentation

Detecting and segmenting vibration signal of each knocking event is the premise of further identity signature extraction. We observe that there is bursting energy fluctuation (i.e., absolute amplitude differences between adjacent samples) brought by hand knocking door as shown in Fig. 8a. Therefore, we leverage a fluctuation threshold-based sliding window to detect knocking event occurrence relying on [34]. The sensed vibration data from idle/non-knocking period is denoted as $y_{\text{idle}}(t)$. The mean $\bar{y}$ and standard deviation σ of its energy fluctuation sequence can be calculated as follows:

$$\bar{y} = \frac{1}{T}\sum_{t=0}^{T-1}|y_{\text{idle}}(t+1) - y_{\text{idle}}(t)|, \tag{4}$$

$$\sigma = \sqrt{\frac{1}{T}\sum_{t=0}^{T-1}(|y_{\text{idle}}(t+1) - y_{\text{idle}}(t)| - \bar{y})^2}, \tag{5}$$

where T is the number of samples. Relying on the analysis of energy fluctuation distribution, we discover appearance time t_{a} of knocking event accompanying by two markers: the first sample's value in sliding window is larger than $\bar{y}+3\sigma$; the averaging amplitude of all samples is greater than $5.8\bar{y}$. In HandKey, we set window size as 600 ms that typically larger than time duration of signatures and its sliding step is 20 ms. Fig. 8b presents the result of data segmentation, and starting times t_{a} of knocking events are marked with red stars.

4.1.2 Noise Removal

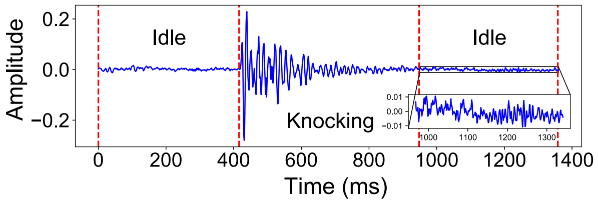


Fig. 9. Sensed vibration data in knocking and idle periods.

Data captured by an accelerometer always consists of vibration signature and intrinsic noise introduced by internal electromagnetic components. In Fig. 9, it's visible that an accelerometer continuously bulks out non-zero amplitude samples (noise) even during an idle period. In this section, we employ the multi-resolution characteristic of DWT to remove noise in frequency bands. It can analyze signals in multiple frequency scales and effectively remove noise components while retaining needed ones [35], [36]. DWT divides sensed vibration data (i.e., $y(t)$) into two parts, approximate coefficients (i.e., w_j) corresponding to low-frequency bands and detail coefficients (i.e., u_j) corresponding to high-frequency bands

$$w_j = 2^{-j/2}\int y(t)\varphi(2^{-j}t - 2\,k)dt, \tag{6}$$

$$u_j = 2^{-j/2}\int y(t)\psi(2^{-j}t - 2\,k)dt, \tag{7}$$

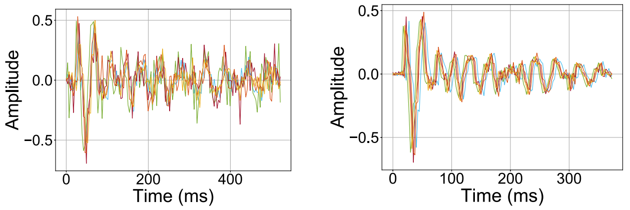
where $\varphi(\cdot)$ and $\psi(\cdot)$ are scaling and wavelet functions respectively. j is a scaling parameter and k is movement step. Especially, the low-frequency band can be divided multiple times, for obtaining approximate coefficients at varied scales. In HandKey, we represent original vibration data using seven frequency scales with considering actual denoising performance. The physical contact of hand and door makes them enjoy large coefficients in resonance frequency scales/bands [37] while background noise owns small ones. To filter out noise and preserve important vibration features, we select a dynamic threshold on the basis of [38] and then coefficients lower than it will be set up to zero on each scale. Finally, denoised data $\overline{y(t)}$ on jth scale is reconstructed through rescaled discrete orthogonal functions (i.e., $h(\cdot)$ and $g(\cdot)$) and corresponding coefficients

$$\overline{y_j(t)} = \sum_k h(n-2\,k)\overline{w_{j+1}} + \sum_k g(n-2\,k)\overline{u_{j+1}}, \tag{8}$$

where $\overline{w_{j+1}}$ and $\overline{u_{j+1}}$ are corrected approximate coefficients and detail coefficients on $(j+1)$th scale respectively. In Fig. 10, we present five vibration signal segments and their denoising versions from the same user. Clearly, denoising module makes these waveforms more consistent, confirming the effectiveness of the proposed DWT-based method.

4.2 Basic Feature Extraction

In this section, we first extract linear features in time-frequency domain relying on vibration mechanism of the hand-door oscillator. Specially, we employ a PCA approach to reduce the dimension of the MFCC-based linear features. We further design a VAE encoder to explore non-linear features derived from hand structure. In short, linear features outline the basic characteristics of vibration signal and the learning-based non-linear part further explores latent hand structure attributes; they apparent complement each other.



(a) Five vibration segments. (b) Denoised identity signatures.

Fig. 10. Original signals (a) and noise removal version (b).

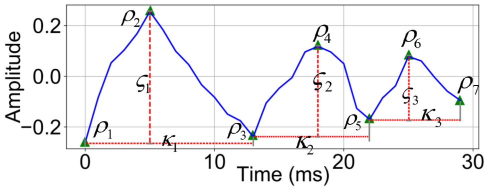


Fig. 11. Extracting time-domain features in three peaks.

4.2.1 Linear Time-Frequency Features

For each hand-door oscillator, there are four main structure parameters affecting vibration signatures: mass m, spring constant s, damper coefficient c and attenuation coefficient μ. These parameters jointly determine duration time $\boldsymbol{\kappa}$, amplitude range $\boldsymbol{\varsigma}$ and attenuation degree $\boldsymbol{\tau}$ of a oscillator's reciprocating motion. For instance, if they have larger values, the duration time $\boldsymbol{\kappa}$ of vibration become short. To explicitly describe the extraction process of the three features, we present part of vibration signature in Fig. 11 as an example. HandKey first detects extreme points (e.g., ρ_1 and ρ_2) marked with green triangles, which are boundary points of peaks. There are three peaks in this case, i.e., $\rho_1\overset{\frown}{\rho_2}\rho_3$, $\rho_3\overset{\frown}{\rho_4}\rho_5$, and $\rho_5\overset{\frown}{\rho_6}\rho_7$. Then we leverage maximum horizontal and vertical range distances of peaks to represent $\kappa = \{\kappa_1, \kappa_2, \kappa_3\}$ and $\varsigma = \{\varsigma_1, \varsigma_2, \varsigma_3\}$ respectively. Vibration attenuation degree ξ is defined as $\{\frac{\varsigma_2}{\varsigma_1}, \frac{\varsigma_3}{\varsigma_1}\}$. Subsequently, nearest-neighbor interpolation [39] is employed to align feature vectors to a fixed length (i.e., the maximum number of peaks in registered signatures). Moreover, we calculate mean, variance, skewness, kurtosis, and form factor [40] to present the global characteristic of each signature.

Learned from Section 2.2, the frequency-domain energy distribution of vibration signature across users are unique. Therefore, we leverage MFCCs to further represent spectrum differences among signatures. It's widely utilized to extract subtle spectrum pattern variations of time series data. Unlike applying MFCC to the speech recognition field, we needn't transform vibration signal into mel spectrum scale in HandKey. In our case, time frame of each knocking event is 100 ms and frame-shifting step is set as 25 ms. Furthermore, we calculate the delta and delta-delta of MFCCs to sense the dynamic characteristics of vibration signals. Finally, we obtain a feature vector with 1215 elements. Nevertheless, directly utilizing MFCC-based features of such a huge dimension to construct the following behavior-independent signature extraction model undoubtedly results in limited computing resource's curse. Fortunately, we discover that spectrum powers of partial frequency bands are repeatedly counted by multiple triangular filters, thus leading to information redundancy within initial MFCCs.

To compress MFCC-based features and completing dimension reduction, we resort to PCA [41] filtering out superfluous information. Its essence is to leverage a set of orthogonal components in a low-dimensional space for representing high-dimensional features while avoids losing critical characteristics. PCA is always employed to dimension reduction, benefiting from its low computation cost and without complex parameter setting. We use matrix $A_{g_1\times g_3}$ to save g_3 (i.e., 1215) dimension features extracted from g_1 vibration signatures, then apply Singular Value Decomposition (SVD) [42] to decompose it into three submatrices: row matrix $U_{g_1\times g_2}$, diagonal matrix $Q_{g_2\times g_2}$, and column matrix $\mathrm{V}^T_{g_2\times g_3}$

$$A_{g_1\times g_3} = U_{g_1\times g_2} \times Q_{g_2\times g_2} \times \mathrm{V}^T_{g_2\times g_3}. \tag{9}$$

The singular values in $Q_{g_2\times g_2}$ is denoted as $\{r_1, r_2, \ldots, r_G\}$. We then select the columns of $\mathrm{V}^T_{g_2\times g_3}$ corresponding to top-$\overline{G}$ singular values in $Q_{g_2\times g_2}$, and obtain the principal component $\overline{A_{g_1\times\overline{G}}}$ from original features

$$\overline{A_{g_1\times\overline{G}}} = A_{g_1\times g_2} \times \mathrm{V}_{\mathrm{g}_2\times\overline{\mathrm{G}}} \tag{10}$$

In our system, we set $\overline{G}$ for compressing the original feature into $\overline{G}$ dimensions. The value of $\overline{G}$ is selected with satisfying the following demand

$$\arg\min\left\{\overline{G}\,\middle|\,\sum_{i=1}^{\overline{G}} w_i \Big/ \sum_{i=1}^{G} r_i\ >\ \vartheta\right\} \tag{11}$$

The ϑ is set as an empirical value 0.92, which is determined to balance the trade-off between unlocking accuracy and time-consuming, referring to system performance evaluation Section 6.6. Moreover, we find that singular value distributions of MFCC-based features and orderings of their principal components are distinguishable. The view is consistent with the above analysis, that is, the resonance frequency distribution of each hand-door oscillator is unique.

4.2.2 Non-Linear Feature Extraction

Learning-based models holding a huge superiority in mining latent non-linear characteristics of samples, are regarded as effective tools for feature extraction [43]. In particular, VAE only requires a small size dataset for completing feature extractor training and hence being widely acclaimed; it can effectively capture numerical distributions of key parameters determining sample generation. In HandKey, we apply VAE to extract latent structure parameters (e.g., mass and spring constant) of the hand-door oscillator from vibration signatures. The VAE model consists of three sub-modules presented in Fig. 12. Each vibration signature $y(t) = [y_1(t), y_2(t), \cdots y_l(t)]$ feeding into VAE and then the specific numerical distribution of each latent parameter is ascertained through an encoder.

Subsequently, a compressed latent parameter vector of structure $z = [z_1, z_2, \cdots z_\ell]$ is obtained; a decoder reconstructs input signature relying on z thereby outputting $\hat{y}(t) = [\hat{y}_1(t), \hat{y}_2(t), \cdots \hat{y}_l(t)]$. Essentially, the process of encoding and decoding on vibration signatures prompts VAE's latent parameter layers to possess the power that representing

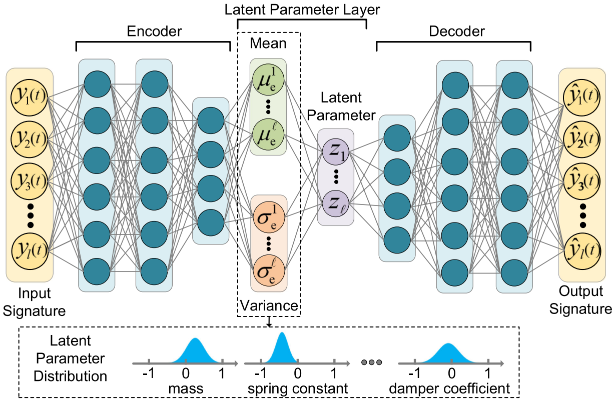


Fig. 12. The VAE model containing three sub-modules: encoder, latent parameter layer, and decoder.

the nonlinear characteristics of each hand-door oscillator structure. To empower our VAE, two goals require to be followed during model training phase: (1) minimizing the reconstruction loss between $y(t)$ and $\hat{y}(t)$ to ensure latent parameters correctly representing vibration signature; (2) promoting the underlying distribution $q_\theta(z|y(t))$ of latent parameters to move closer the normal one, hence preventing from model over-fitting and parameter space irregularity. Referring to [44], the two goals can be formulated as following loss function

$$\mathcal{L}(\bar{q}_\theta, q_\phi; y(t)) = \mathcal{D}_{\mathbf{KL}}(q_\phi(z|y(t))||\bar{q}_\theta(z)) + \|y(t) - \hat{y}(t)\|_2, \tag{12}$$

where $\mathcal{D}_{\mathbf{KL}}$ is Kullback-Leibler divergence measuring the difference between two probability distributions. $\bar{q}_\theta(z)$ is the prior standard normal distribution $\mathcal{N}(0;1)$ and $||\cdot||_2$ is the L2 norm to present reconstruction loss of input and output signatures. In HandKey, the number of neurons contained in VAE's three modules is (64, 64, 32), (24, 12), and (32, 64, 64) respectively. Its detailed inputting data collection, and parameter settings (e.g., weight decay ratio and optimizer) in the training process are consistent with the following behavior-independent signature extraction module.

4.3 Behavior-Independent Signature

Knocking behaviors of the same user between registration and identity authentication phases are not identical, inducing signature similarity decrease and hence the success ratio of authentication. To make unlocking scheme practical, the final signature extracted by HandKey should both effectively distinguish users and resist interference from user behavior changes. In this section, we construct Triplet model [18] as the behavior-independent signature extraction tool employing LeNet [17] network which is a typical learning-based approach to extracting condensed features of input images. The essence of Triplet model is to restore similar parts of features from the same user and simultaneously amplify differences across users. To be specific, this model makes Intra-PCCs much larger than Inter-PCCs even if knocking behavior changes, hence ensuring unlocking accuracy. As shown in Fig. 13, the Triplet consists of three sub-modules sharing identical weights. $\{\nu^{\text{neg}}, \nu^{\text{anc}}, \nu^{\text{pos}}\}$ is a 3-tuple including three feature vectors as the basic inputting unit. Therein, ν^{anc} and ν^{pos} from the same legitimate (positive) user; the former acts as the newly sensed authentication signature feature and the latter is the registered feature template to represent user identity; while ν^{neg} is a randomly selected one from other (negative) person. To reduce the loss of feature vectors ν^{anc} and ν^{pos} while make ν^{neg} far away from them, we leverage the following function [45] controlling weight update in each iteration

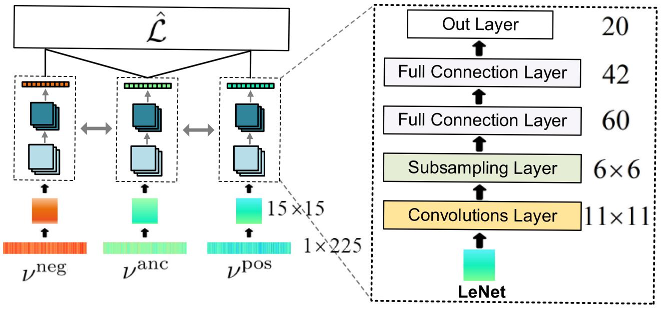


Fig. 13. The structure of HandKey's LeNet-based Triplet model.

$$\hat{\text{L}} = \max(||\nu^{\text{anc}} - \nu^{\text{pos}}||_2 - ||\nu^{\text{anc}} - \nu^{\text{neg}}||_2 + \alpha, 0), \tag{13}$$

where α is a margin threshold that is enforced between positive and negative pairs.

For filtering out behavior interference, the training process of Triplet model is elaborately designed. We let arbitrary twenty users knock on random fifteen positions of the pre-set knocking area, with three force ranges (i.e., small, medium, and large). Each user offers ten vibration signatures in one position-force combination, with a total of 450 (i.e., $15 \times 3 \times 10$). HandKey then extracts 214-element feature vector from each original signature, that is, 89 elements from time domain, 113 ones of compressed MFCCs, and the remaining part generated by our VAE-based extractor. In the following, successive "0" is filled at the end of feature vectors, for shaping them into 15×15 matrices inputting LeNet models. Especially, the pairing scheme of input vector tuples is critical to guide the Triplet model extracting behavior-independent signatures. In HandKey, there are two types of input pair: ν^{neg} and ν^{pos} have similar knocking behaviors while ν^{anc} is not; ν^{neg} and ν^{anc} have similar knocking behaviors while ν^{pos} is not. In this scheme, the model can learn to ignore behavioral differences in vibration samples from the same user and just focuses on hand-dependent features. When iterating, the amount of data in each batch is 32. The weight decay ratio is set to 0.01 and the number of parameters updated in each iteration is randomly selected 50%. Moreover, each parameter's optimization strategy is set as Adam optimizer [46] and the maximum number of training iteration is 10^6 until the loss stabilizes.

4.4 Identity Authentication

In the registration phase, a user u knocks on a door to generate vibration signature ν_u^{pos} as his/her identity template. HandKey then reuses the feature vectors from other users who participated in training Triplet model as the negative templates ν_u^{neg}. Both templates are then stored in our database. Upon authenticating user u, HandKey obtains a newly sensed signature ν_u^{anc}, thereby constructing a 3-tuple (i.e., $\{\nu_u^{\text{neg}}, \nu_u^{\text{anc}}, \nu_u^{\text{pos}}\}$) by combining it with the saved identity template and a negative one. Subsequently, this feature 3-

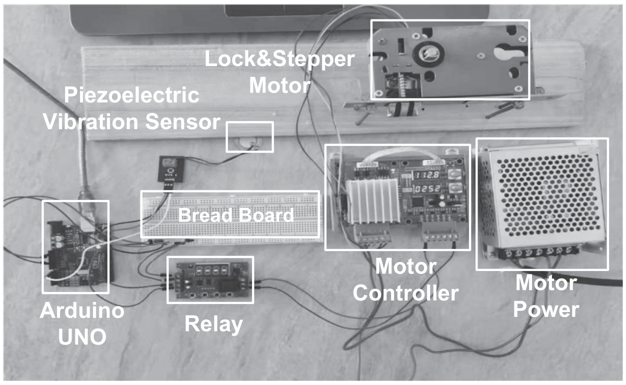


Fig. 14. The experiment setup of HandKey.

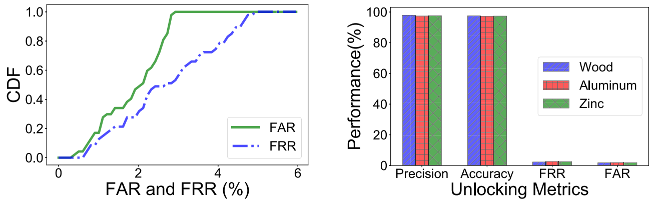
tuple is fed into the trained Triplet model for verifying user identity. HandKey could repeat the above process for forming multiple 3-tuples by traversing all ν_u^{neg} and apply a standard voting mechanism on all classification results to judge ν_u^{anc}'s authenticity. However, we only randomly choose 32 3-tuples in a batch in order to strike a balance between computational cost and authentication security. Finally, if more than a half tuples' $\|\nu_u^{\mathrm{anc}} - \nu_u^{\mathrm{pos}}\|$ less than $\|\nu_u^{\mathrm{anc}} - \nu_u^{\mathrm{neg}}\|$, the newly sensed signature is more similar to the registered identity template and hence the user is accepted, otherwise rejected.

5 Implementation

The devices used in the following experiments have shown in Fig. 14. Users knock on the door and piezoelectric/BU-27135 sensors sense vibration data in real-time. We leverage BU-27135 for vibration collection in the feasibility study and verifying experiment due to its high sensitivity with a sampling frequency of up to 10 kHz. In the following, a Shenzhou notebook with an Intel i5-8400 CPU, GeForce GTX1060 6 G GPU, and 16 G RAM, is denoted as a processing unit to receive vibration signature by the serial interface. The JetBrains PyCharm 2019 software is applied to analyze and process the sensed data. In HandKey, signal preprocessing and signature extraction modules are both completed in the notebook. Arduino UNO receives an authentication result (i.e, locking/unlocking) and then controls the motor controller to implement it. We recruit 47 users (18 females and 29 males) denoted as $U_1, U_2, \ldots U_{47}$ aged from 21 to 43 for evaluating our system. HandKey is built on three types of doors (i.e., wood, aluminum, zinc) and three gestures (i.e., $\mathsf{Gesture}-1$, $\mathsf{Gesture}-2$, and $\mathsf{Gesture}-3$), respectively. In default, users knock the pre-set knocking area thirty times on each door with habitual forces, by the right hand using $\mathsf{Gesture}-1$. Moreover, the dataset verifying the impacts of specific parameters and unlocking security under potential attacks is customized.

6 Performance Evaluation

In this section, we evaluate HandKey's performance under practical scenarios. Before diving into experiment details, we first discuss basic metrics for evaluation. As identity verification is a binary classification problem, there are four basic cases related to authentication result, namely true positive (TP), true negative (TN), false positive (FP), and false negative (FN). To comprehensively measure the performance of HandKey, we use False Accept Rate (FAR), False Reject Rate (FRR), Precision, and Accuracy as evaluation metrics. Basically $\mathrm{FAR} = \frac{\mathrm{FP}}{\mathrm{FP+TN}}$ measures the ratio of an authentication system incorrectly accepting illegitimate users. $\mathrm{FRR} = \frac{\mathrm{FN}}{\mathrm{FN+TP}}$ shows the ratio of incorrectly rejecting legitimate user. Moreover, $\mathrm{Precision} = \frac{\mathrm{TP}}{\mathrm{TP+FP}}$ measures the overall system performance, while $\mathrm{Accuracy} = \frac{\mathrm{TP+TN}}{\mathrm{TP+TN+FP+FN}}$ is the ratio of samples being correctly classified. A secure and effective unlocking system should have low values of FAR and FRR, and high values of Precision and Accuracy.



(a) CDF of incorrect verification. (b) Performance in three doors.

Fig. 15. Results in (a) show low incorrect unlocking rates among all users. (b) Presents stable unlocking performance when implementing HandKey on three different doors.

6.1 Overall Performance

We select one user (e.g., U_1) as the legitimate user who has registered personal identity information in HandKey, and other users (e.g., $U_2, \ldots U_{47}$) play the role of illegitimate ones. Following the cross-validation principle, every user is treated as the legitimate user in turn and we finally obtain a total of 47 authentication results from all users. In the following, we input sensed vibration signatures into the trained model and count the correct verification ratio of these positive and negative samples. The cumulative distribution function of all users' FARs and FRRs are shown in Fig. 15a. Averaging values of the two metrics are 1.87% and 2.72% respectively. From the result, we conclude that HandKey incorrectly verifies the identity of users at a low ratio. Moreover, the unlocking performances of three types of doors are verified. In Fig. 15b, we see that there are negligible differences in Precision (97.71%) and Accuracy (97.37%) when knocking on three doors respectively, and their averaging values are 97.54%. The result indicates that door materials almost don't affect unlocking performance that is consistent with our analysis in the feasibility study. Therefore, signature differences among users are mainly caused by hand structure; regardless of door materials, a hand can still ensure the structure uniqueness of the hand-door oscillator.

6.2 Impact of Knocking Trial Times

Existing unlocking systems acquiescently allow users to continuously authenticate/input identity information five times until unlocking. If identity verification still fails for the fifth time, systems will be locked over a while. Therefore, the ratio of users successfully passing authentication within five times reflects unlocking effectiveness. In this section, we present changes in HandKey performance within the maximum number of knocking trials from one to five. As illustrated in Fig. 16, four metrics are continuously optimized as the number of trials increases. Especially, at the fifth trial, FRR is

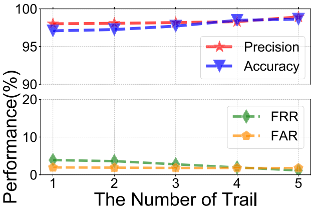


Fig. 16. Unlocking performance with trials from one to five.

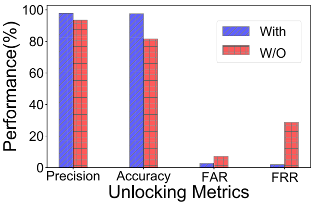


Fig. 17. Unlocking performance with/without using behavior-independent signatures.

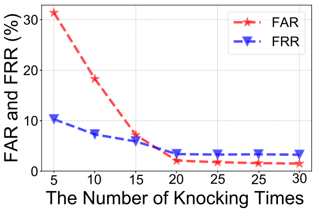


Fig. 18. The impact of registration data size on FAR and FRR.

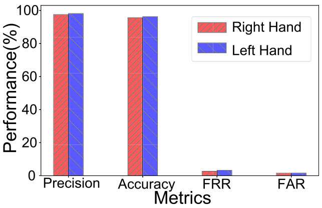


Fig. 19. Unlocking performance when knocking with right/left hand.

decreased to 1.15% meaning that HandKey unlocks the door when the legitimate user knocks with high accuracy.

6.3 Impact of Behavior-Independent Signature

During user registration and identity authentication phases, knocking behaviors may be various, hence causing similarity decreasing of vibration signatures from the same user. To relieve the interference of knocking position and force variation, HandKey extracts behavior-independent signatures by the LeNet-based Triplet model as described in Section 4.3. We evaluate HandKey performance changes caused by suspending this model and directly judge user identity using initial linear and non-linear features. As shown in Fig. 17, the value of FRR when feeding behavior-independent signatures into the trained model is 1.87% which is much less than 29.05% without applying the Triplet model. In this case, legitimate users are misidentified at a high rate. Moreover, the FAR increases to 7.14% when behavioral interference isn't properly processed, which means the signature uniqueness among individuals is compromised. The result verifies that behavior-independent signatures extracted in HandKey are effective, that can enhance unlocking convenience and ensure signature distinctiveness among users.

6.4 Impact of Registration Data Size

HandKey has trained VAE-based feature extractor and Triplet model relying on a pre-collected dataset. For adapting the model to a specific person, newly registered users should input their vibration signatures for adding personal identity information to the trained extractor and Triplet model. If an unlocking system requires collecting a large amount of registered data to extract identity information, it undoubtedly compromises user experiences. Therefore, the desired system should construct a model for security authentication by as few registered signatures as possible. In this section, we employ different sizes of registration data to evaluate HandKey's performance. Users knock on the door from 5 to 35 times respectively for model construction. As shown in Fig. 18, when the number of knocking times reaches 20, HandKey shows excellent performance with 2.16% FAR and 3.41% FRR. This result indicates that users can complete the data registration by inputting just a few vibration signatures that spending within one minute.

6.5 Impact of Knocking Hand

Due to differences in personal habits, some users may choose to knock utilizing right hands while the others leverage left ones. Relative positions between two hands and the pre-set knocking area are distinct, thus sensed vibration signatures of them are different. In this section, we explore unlocking performances by employing two hands to register information respectively. Ten random users participate in this experiment and they knock fifty times with each hand using habitual forces on the wood door. 50% data is used for training our model and the other tests unlocking performance. As shown in Fig. 19, HandKey's performances of knocking by two hands are both satisfactory. To be specific, their averaging values of Precision and Accuracy are respectively greater than 98% and 96%. It shows that two hands can generate unique signatures for representing user identity.

6.6 Impact of Dimension Reduction Threshold

To remove redundant information of original MFCC-based features, we leverage the PCA-based approach to complete dimension reduction in Section 4.2.1. A small threshold ϑ means that only fewer features are retained, and the probability of losing important information representing user identity is increased. Therefore, choosing a proper ϑ is critical to HandKey's unlocking performance. In the following, we explore the change tendencies of FRR and FAR when adjusting ϑ from 0.1 to 1. The averaging values of them as illustrated in Fig. 20. We see that the smallest FAR is obtained when ϑ is set as 0.92, and the corresponding FRR is below 2.75%. In this case, HandKey can ensure legitimate users successfully access and effectively resist potential attacks, thus the default value of ϑ is 0.92.

6.7 Impact of Wearing Accessory

Some users are accustomed to wearing watches, smart bracelets, gloves, and other wearable devices. These accessories may indirectly affect the overall structure of the hand-door

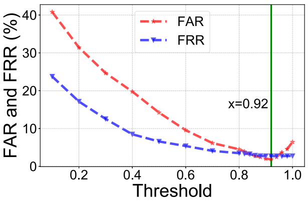


Fig. 20. Adjusting dimension reduction threshold to evaluate unlocking performance.

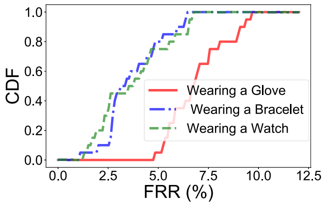


Fig. 21. Comparing FRRs when users wearing different accessories.

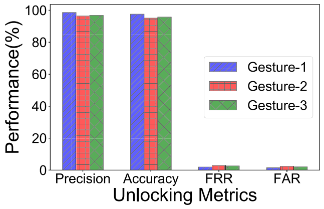


Fig. 22. Unlocking using three common gestures.

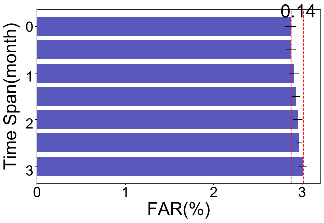


Fig. 23. FRRs under distinct time spans.

oscillator. To verify the impact of wearing them, we collect vibration signatures when users wear a TISSOT watch with 60 g, a Huawei bracelet with 30 g, and a glove with general thickness respectively. Subsequently, all signatures are fed into the trained model constructed by non-wearing accessory registration data. As shown in Fig. 21, wearing a glove on hand owns a few larger FRR (6.83%) compared with a bracelet/watch on the wrist. We summarize the reasons for FRR increasing as follows: gloves cover an entire hand and hence slightly change the oscillator structure. As the above analysis, the vibration signature generation and propagation strongly depend on oscillator structure, thus changing this structure doubtlessly affects the signature and hence performance in FRR; otherwise, it would allow attacks to easily fake a legitimate user. In HandKey, by designing the behavior-independent signature extraction module, the FRR caused by wearing gloves is 6.83% which is satisfactory and reasonable.

6.8 Impact of Knocking Gestures

HandKey supports users to choose personal favorite gestures instead of just the fixed one to represent identity information and unlocking inner doors. In this section, we evaluate HandKey's unlocking performance using three common gestures. The results are illustrated in Fig. 22 presenting that $\mathsf{Gesture}-1$ presents a better unlocking accuracy compared with the other two gestures. In general, they all offer satisfactory performance with Precision larger than 97%. We summarize the reason for performance differences caused by gestures as follows: a large contact area between a hand and the pre-set knocking area enables the hand structure to have more effects on vibration generation and propagation. Therefore, we recommend that users choose accustomed gestures for data registration while increasing the contact area as much as possible.

6.9 The Stability of Vibration Signature

Vibration signature stability across a long-term span is one critical indicator for measuring unlocking performance. If one user's signatures significantly change over time, it inevitably causes a high probability of failure authentication and hence compromising user experience. For verifying signature stability, we record the unlocking performance of users after completing the initial registration, as the time interval increases from half a month to three months. In the following, the averaging authentication performance of each period is presented in Fig. 23. The result indicates that even if the time span between registration and authentication phases is up to three months, HandKey still keeps a satisfactory performance of recognizing legitimate users with a small FRR increasing of 0.14%. Thus, we conclude that the vibration signature is stable enough to ensure the unlocking performance of HandKey.

6.10 Unlocking Security Under Attacks

In this section, we evaluate the unlocking security of HandKey under three potential attacks that are zero-effort, imitation, and side-channel. In the first type, all users are divided into two parts, thirty of them as legitimate users registering personal information in HandKey, and other ones are attackers. We ask each attacker to output fifty vibration signatures from random knocking forces and positions. Sensed signatures then are compared with the registered ones to obtain feature similarities and hence judge identity. The averaging ratio (i.e., FAR of 1.53%) of misjudging these illegitimate is presented in Fig. 24. To implement the imitation attack, we select eight users to combine four legality-attack pairs. Two users belonging to the same pair have the most similar hand shapes among 47 users. One person in the pair acts as a registered user, and the other is denoted as an attacker who observes and practices to imitate legitimate users' knocking behaviors. We obtain fifty vibration signatures from each attacker, and the averaging FAR is 2.04%. The experiment results present that imitation attack doesn't cause obvious changes in the misclassification rate (i.e., FAR) of negative samples, with an increase only of 0.17% compared to the baseline 1.87%.

The side-channel attack with a complex design seems to have powerful destructive capabilities but lacks practicality. The reasons behind this view are as follows: First, the vast majority of doors are flat and unobstructed. If attackers deploy malicious sensors within human visible ranges (e.g.,

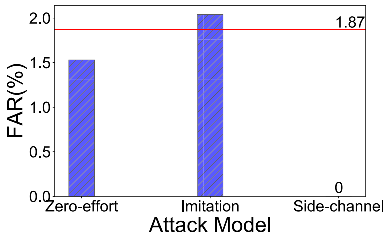


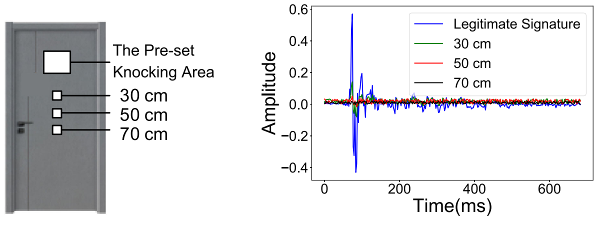
Fig. 24. FARs under potential attacks.

around the pre-set knocking area), they can be easily detected by users. Second, assuming a sensor placing in the lower half of doors that are far away from the knocking position, sensed signals are severely distorted and become invalid. We place an accelerometer at 30 cm, 50 cm, and 70 cm away from the preset knocking area to collect vibration signals and then observe their differences with the legitimate user signature. As illustrated in Fig. 25b, at a distance greater than 30 cm, sensed signal energy is low and its waveform greatly differs from the legitimate signature. The result indicates that malicious attackers cannot steal signatures matching the identity of legitimate users, and thus are unable to carry out further attacks. We ask ten users to knock on doors fifty times and collect vibration signals at the above-mentioned positions in real-time. The trained model then verifies their identity and none of the recorded vibration signals can spoof HandKey i.e., $\mathrm{FAR} = 0$.

6.11 Time Latency and Hardware Cost

In HandKey, vibration signal first is sensed by the accelerometer, then transmitted to the computer completing further data processing. Without considering data communication, we focus on the time taken for performing authentication action. For HandKey, models such as the PCA-based dimension reduction, VAE-based feature extractor, and LeNet-based Triplet network are trained offline. Therefore, the main time-consuming parts are noise removal and original feature extraction. We input twenty vibration signatures of each user into our model and record the running time of two data processing parts. The time costs of them are $0.64 \pm 0.29\ s$ and $0.81 \pm 0.24\ s$ respectively. Generally, HandKey can achieve a satisfactory running speed for unlocking.

The total hardware cost of HandKey prototype is 72.9 dollars and its sub-module costs termwise lie in Table 1. We also count the selling prices of the top-50 popular smart locks on the Amazon website [47]; their average price is up to 157 dollars more than the twice of HandKey. Relying on these statistics, the fact is displayed that the cost of HandKey is indeed low. Moreover, smart lock manufacturers leveraging HandKey as the prototype can massively produce these modules to further compress costs. Thus, the estimated cost for HandKey could be significantly reduced.



(a) The position of malicious sensor.

(b) Sensed vibration signals.

Fig. 25. Implementing the side-channel attack. (a) Illustrates the three positions placing an accelerometer. (b) shows sensed vibration signals in four data collection positions when the user knocks on the door.

TABLE 1
The Detailed Cost of Each Module of HandKey Prototype

Module Name	Arduino ATmega328	Elprico Relay	Abovehill Motor&Power	Sensor	Fittings	Total Cost
Unit Price($)	22.8	8.1	18.4	17.2	6.4	72.9

7 Limitation and Future Work

In this section, we review the keyless unlocking system HandKey, mainly including the limitations that need to be further solved and outlook for system performance improvement in the future work.

The size of HandKey's prototype needs to further dwindle. Current data sensing/processing modules of HandKey are scattered, hence owning a large size. We should integrate all modules into a small unit that is convenient for installation and usage. Nevertheless, it is a technical problem rather than related to academic research. For manufacturers, producing a market-oriented smart lock utilizing unique vibration signatures is easy to achieve. In the next version, we will try to compress current prototype size to facilitate rapid deployment.

We consider combining HandKey with existing "keys" (e.g., fingerprint and face) in a conjunctive manner to further facilitate (hand-)disabled users. In this manner, HandKey allows users to flexibly select appropriate unlocking ways on account of actual demands. Nevertheless, we must prudently handle the tradeoff between convenience and security under such a setting, since there are intrinsic drawbacks in combined keys as stated in Section 1. Therefore, for unlocking the inner door, whether enabling the conjunctive mechanism needs careful consideration.

Moreover, we explore utilizing vibration signatures constructs an authentication approach applying to hand-holding mobile devices like smartphones. In this case, the hand and a smartphone can be regarded as an oscillator. When a finger touches the screen, the oscillator can generate hand-specific vibration signals triggered by touching forces; meanwhile, a built-in accelerometer on smartphones senses it in real-time. During the interaction of finger and device, the user identity can be continuously tracked, thereby ensuring system security in the entire service session.

8 Related Work

In this section, we revisit previous efforts on user authentication and unlocking systems. Moreover, we present the difference of HandKey compared with them.

8.1 Unlocking Using Physical Key and Magnetic Card

Traditional physical keys are made of metals or magnetic cards [1], [2]. The key is regarded as an identity token, and its holder can unlock a specific lock and enter private spaces. However, physical keys exist inherent shortcomings: first, due to strict correspondence between key and lock, the user who possesses permissions to enter multiple personal areas, needs to carry a bunch of keys. Without a doubt, this is a terrible experience for most users. Second, forgetting and losing keys inevitably happen in daily life [7]. In this case, locks must be quickly replaced, hence leading to usage cost and security risk increasing [48]. Third, metal keys are prone to rust and plastic cards may be accidentally degaussed [49]. When jagged parts of a key are deformed, users lose permission to unlock doors. All the above three issues inevitably compromise user experience and personal security.

8.2 Unlocking Door in a Keyless Way

To enhance convenience of unlocking ways, smart locks [50] are emerging and given high hope. It allows unlocking a door by verifying pre-stored identity information without carrying any physical keys. Earlier appeared keyless schemes require users to enter Personal Identification Numbers (PINs) [51] and graphical patterns [52] for identity verification. However, the password-based approaches can be easily peeked by someone close [3] and vulnerable to side-channel attack [9]. Followed by that, biometrics are leveraged to represent user identity and unlocking permission, including, among others, fingerprint [53], face [54], and voice [55], teeth [56]. But constructing door entry systems relying on these traits also faces major obstacles in deployment, due to the high cost of non-trivial sensors. For instance, FaceID [10] captures facial 3D features using customized flood illuminators and dot projectors; Qualcomm Fingerprint Sensor [11] leverages extraordinary ultrasonic readers to scan the pores of users' fingers. Moreover, their flaws are continuously discovered by researchers. To be specific, exquisitely designed masks can deceive most face recognition systems [57] and voice authentication always incorrectly rejects unlocking of legitimate users under ambient noise interference.

8.3 Vibration-Based Authentication and Unlocking

Some advanced works are devoted to exploring unique vibration patterns generated by users to authenticate identity. For example, [12], [13], [31] show the feasibility of distinguishing users employing vibration features of arms and fingers stimulated by a motor, while HandPass [58] just applicable for mobile scenarios. Therein, [12] and [13] require users either to wear a wristband or to hold a smartphone for capturing vibration patterns, thus they are mobile-customized and not suitable for implementing keyless unlocking. Users leveraging VibWrite [31] paint specific graphic patterns on a vibrating panel with fingers for verifying identity, which increases user intervention. Moreover, they require motors to impose active high-frequency vibration that may weaken user-friendliness. Taprint [32] regards hands as virtual number keyboards and supports text inputting by tapping finger knuckles. It argues that captured sensed vibration features can distinguish users and tapping positions, thereby achieving secure inputting. Nevertheless, it needs users to actively calibrate the system to relieve the interference of variable tapping behaviors. Some emerging authentication approaches leverage vibration patterns relying on knocking behaviors (e.g., Thumprint [59], AwareLESS [60], and KeyClick [61]) to distinguish users. But behavior-based traits can be easily controlled and changed by subjective factors, thereby leading to identity feature changes and failed authentication.

Different from the above methods, HandKey captures unique vibration signatures when a hand knocks on doors in a natural (passive) way, which offers users excellent experiences. We adequately explore the effects of dominating factors such as knocking gesture and door material on vibration signatures, making HandKey more practical. In the following, we extract behavior-independent signatures leveraging a LeNet-based Triplet model, hence presenting the essential hand structural property even if knocking behaviors change.

9 Conclusion

In this article, we have proposed a keyless unlocking system HandKey that employs the unique vibration signature generated by the hand-door oscillator. HandKey offers a low-cost, user-friendliness, and secure unlocking scheme implemented on inner doors. It leverages only a common accelerometer to complete vibration signal reception. To effectively represent the unique signature and solve the interference brought by variable knocking behavior, we have elaborately designed corresponding strategies. For instance, we first extracted linear features by analyzing the vibration mechanism in time and frequency domains; we employed a VAE-based model to capture hidden nonlinear features. Subsequently, we leveraged the LeNet-based Triplet model to resolve the effects of knocking behavior variation, thereby obtaining behavior-independent signatures. Finally, we have evaluated the authentication performance by conducting extensive experiments; the promising results have proved a 1.87% FAR and a 97.71% Accuracy. Benefiting from the lightweight mode, HandKey could achieve large-scale deployment to provide users with effective unlocking services on inner doors.

References

[1] G. Asil T and K. Yucel K, "Mechanical/electronic lock and key therefor," U.S. Patent US6374653B1, Apr. 23, 2002.

[2] G. Asil T, "Access control system with mechanical keys which store data," U.S. Patent US5245329, Sep. 14, 1993.

[3] G. Ye et al., "Cracking android pattern lock in five attempts," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2017, pp. 1–15.

[4] D. Li, X.-P. Zhang, M. Hu, G. Zhai, and X. Yang, "Physical password breaking via thermal sequence analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 5, pp. 1142–1154, May 2019.

[5] R. Cappelli, M. Ferrara, and D. Maltoni, "On the operational quality of fingerprint scanners," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 2, pp. 192–202, Jun. 2008.

[6] Y. Chen, J. Sun, X. Jin, T. Li, R. Zhang, and Y. Zhang, "Your face your heart: Secure mobile face authentication with photoplethysmograms," *IEEE Conf. Comput. Commun.*, 2017, pp. 1–9.

[7] Vivint, "6 things to do if you lose your keys," 2020. [Online]. Available: https://www.vivint.com/resources/article/keyless-entry-to-avoid-the-stress-of-losing-your-keys

[8] C. Vedat, O. Busra, and O. Kerem, "A survey on near field communication (NFC) technology," *Wireless Pers. Commun.*, vol. 71, no. 3, pp. 2259–2294, 2013.

[9] M. Zhou et al., "PatternListener: Cracking android pattern lock using acoustic signals," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 1775–1787.

[10] Apple, “About face ID advanced technology,” 2018. [Online]. Available: https://support.apple.com/en-sg/HT208108

[11] Qualcomm, “Fingerprint Sensors,” 2018. [Online]. Available: https://www.qualcomm.com/products/government/fingerprint-sensors

[12] L. Yang, W. Wang, and Q. Zhang, “VibID: User identification through bio-vibrometry,” *Proc. 15th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw.*, 2016, pp. 11:1–11:12.

[13] X. Xu et al., “TouchPass: Towards behavior-irrelevant on-touch user authentication on smartphones leveraging vibrations,” *Proc. 26th Annu. Int. Conf. Mobile Comput. Netw.*, 2020, pp. 24:1–24:13.

[14] M. MaryW and M. Robert F, “Evolution of the human hand: Approaches to acquiring, analysing and interpreting the anatomical evidence,” *J. Anatomy*, vol. 197, no. 1, pp. 121–140, 2000.

[15] M. ShensaJ, “The discrete wavelet transform: Wedding the a trous and mallat algorithms,” *IEEE Trans. Signal Process.*, vol. 40, no. 10, pp. 2464–2482, Oct. 2002.

[16] Y. Pu et al., “Variational autoencoder for deep learning of images, labels and captions,” in *Proc. Int. Conf. Neural Inf. Process. Syst.*, 2016, pp. 2352–2360.

[17] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.

[18] H. Elad and A. Nir, “Deep metric learning using triplet network,” in *Proc. Int. Workshop Similarity-Based Pattern Recognit.*, 2015, pp. 84–92.

[19] S. RSJL, S. JL, and S. NG, “Non-linear modelling of an electro-rheological vibration damper,” *J. Electrostatics*, vol. 20, no. 2, pp. 167–184, 1987.

[20] S. Yao, X. Zhou, and G. Hu, “Experimental study on negative effective mass in a 1D mass–spring system,” *New J. Phys.*, vol. 10, no. 4, 2008, Art. no. 043020.

[21] U. of Washington, Mass-spring-damper systems the theory, in 2020. [Online]. Available: https://faculty.washington.edu/seattle/physics227/reading/reading-3b.pdf

[22] P. Bruc, “Newton’s interpretation of newton’s second law,” *Arch. Hist. Exact Ences*, vol. 60, no. 2, pp. 157–207, 2006.

[23] S. Yao, X. Zhou, and G. Hu, “De potentia restitutiva, or of spring explaining the power of springing bodies,” in *Sixth Cutler Lecture*, London, U.K.: John Martyn, 1678, pp. 331–356.

[24] Wikipedia, Acceleration, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Acceleration

[25] L. George, “Semiactive control for vibration attenuation,” *J. Intell. Mater. Syst. Struct.*, vol. 5, no. 6, pp. 841–846, 1994.

[26] National Aeronautics and Space Administration, USA, Anthropometry and biomechanics, 2020. [Online]. Available: https://msis.jsc.nasa.gov/sections/section03.htm

[27] B. Jacob, J. Chen, Y. Huang, and C. Israel, “Pearson correlation coefficient,” in *Noise Reduction in Speech Processing*, Berlin, Germany: Springer, 2009, pp. 1–4.

[28] G. Graham ML, “Inverse problems in vibration,” *Appl. Mech. Rev.*, vol. 39, no. 7, pp. 1013–1016, 1986.

[29] V. der Maaten and L. G. Hinton, “Visualizing data using t-SNE,” *J. Mach. Learn. Res.*, vol. 9, no. 2605, pp. 2579–2605, 2008.

[30] A. Singh Rathore et al., “Sonicprint: A generally adoptable and secure fingerprint biometrics in smart devices,” in *Proc. 18th Int. Conf. Mobile Syst., Appl. Serv.*, 2020, pp. 121–134.

[31] J. Liu, C. Wang, Y. Chen, and N. Saxena, “VibWrite: Towards finger-input authentication on ubiquitous surfaces via physical vibration,” *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 73–87.

[32] W. Chen et al., “Taprint: Secure text input for commodity smart wristbands,” *Proc. 25th Annu. Int. Conf. Mobile Comput. Netw.*, 2019, pp. 17:1–17:16.

[33] V. Rivarol, D. O’Shaughnessy, and F. Azarshid, “Generalized mel frequency cepstral coefficients for large-vocabulary speaker-independent continuous-speech recognition,” *IEEE Trans. Speech Audio Process.*, vol. 7, no. 5, pp. 525–532, Sep. 1999.

[34] C. Cai, H. Pu, P. Wang, Z. Chen, and J. Luo, “We hear your PACE: Passive acoustic localization of multiple walking persons,” *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 5, no. 2, pp. 55:1–55:24, 2021.

[35] X. Zhou, C. Zhou, and I. J. Kemp, “An improved methodology for application of wavelet transform to partial discharge measurement denoising,” *IEEE Trans. Dielectr. Electr. Insul*, vol. 12, no. 3, pp. 586–594, Jun. 2005.

[36] Z. Huo, Y. Zhang, P. Francq, L. Shu, and J. Huang, “Incipient fault diagnosis of roller bearing using optimized wavelet transform based multi-speed vibration signatures,” *IEEE Access*, vol. 5, pp. 19442–19456, 2017.

[37] D. W. Chee, “A theory of resonance,” *PMLA/Publications Modern Lang. Assoc. Amer.*, vol. 112, no. 5, pp. 1060–1071, 1997.

[38] F. Xiao and Y. Zhang, “A comparative study on thresholding methods in wavelet-based image denoising,” *Procedia Eng.*, vol. 15, pp. 3998–4003, 2011.

[39] J. Nan and W. Luo, “Quantum image scaling using nearest neighbor interpolation,” *Quantum Inf. Process.*, vol. 14, no. 5, pp. 1559–1571, 2015.

[40] Z. Li et al., “E-eye: Hidden electronics recognition through mmWave nonlinear effects,” *Proc. 16th ACM Conf. Embedded Netw. Sensor Syst.*, 2018, pp. 68–81.

[41] W. S. EsbensenKim and G. Paul, “Principal component analysis,” *Chemometrics Intell. Lab. Syst.*, vol. 2, no. 1/3, pp. 37–52, 1987.

[42] W. JohnM, S. Catherine, and B. ChristopherS, “Singular value decomposition of wintertime sea surface temperature and 500-mb height anomalies,” *J. Climate*, vol. 5, no. 6, pp. 561–576, 1992.

[43] S. Pouyanfar et al., “A survey on deep learning: Algorithms, techniques, and applications,” *ACM Comput. Surv.*, vol. 51, no. 5, pp. 92:1–92:36, 2019.

[44] P. DiederikKingma and M. Welling, “Auto-encoding variational bayes,” in *Proc. Int. Conf. Learn. Representations*, 2014.

[45] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A unified embedding for face recognition and clustering,” in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2015, pp. 815–823.

[46] Z. Zhang, “Improved adam optimizer for deep neural networks,” *IEEE/ACM 26th Int. Symp. Qual. Serv.*, 2018, pp. 1–2.

[47] Amazon, Smart lock, in 2022. [Online]. Available: https://www.amazon.com/

[48] B. D. Security, Should you change your locks after losing house keys?, in 2021. [Online]. Available: https://www.butlerdurrellsecurity.com/should-you-change-your-locks-after-losing-house-keys/

[49] L. G. LTD, “How to clean rust off of keys?” in 2020. [Online]. Available: https://www.hunker.com/13420729/how-to-clean-rust-off-of-keys

[50] Wikipedia, Smart lock, in 2020. [Online]. Available: https://en.wikipedia.org/wiki/Smart_lock

[51] J. Yan, A. Blackwell, R. Anderson, and A. Grant, “Password memorability and security: Empirical results,” *IEEE Secur. Privacy*, vol. 2, no. 5, pp. 25–31, Sep./Oct. 2004.

[52] P. Andriotis and T. Tryfona, “Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method,” in *Proc. Int. Conf. Hum. Aspects Inf. Secur., Privacy, Trust*, 2014, pp. 115–126.

[53] D. Zhang, F. Liu, Q. Zhao, G. Lu, and N. Luo, “Selecting a reference high resolution for fingerprint recognition using minutiae and pores,” *IEEE Trans. Instrum. Meas.*, vol. 60, no. 3, pp. 863–871, Mar. 2011.

[54] P. Perera and V. M. Patel, “Face-based multiple user active authentication on mobile devices,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 5, pp. 1240–1250, May 2019.

[55] W. Huang, W. Tang, K. Zhang, H. Zhu, and Y. Zhang, “Thwarting unauthorized voice eavesdropping via touch sensing in mobile systems,” in *Proc. IEEE Conf. Comput. Commun.*, 2022, pp. 31–40.

[56] H. Jiang, H. Cao, D. Liu and, J. Xiong, and Z. Cao, “SmileAuth: Using dental edge biometrics for user authentication on smartphones,” *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 4, no. 3, pp. 84:1–84:24, 2020.

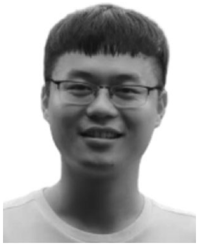
[57] N. Erdogmus and S. Marcel, “Spoofing face recognition with 3D masks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 7, pp. 1084–1097, Jul. 2014.

[58] H. Cao, H. Jiang, D. Liu, and J. Xiong, “Evidence in hand: Passive vibration response-based continuous user authentication,” in *Proc. IEEE 41st Int. Conf. Distrib. Comput. Syst.*, 2021, pp. 1020–1030.

[59] S. Das, G. Laput, C. Harrison, and J. I. Hong, “Thumprint: Socially-inclusive local group authentication through shared secret knocks,” *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2017, pp. 3764–3774.

[60] H. Manabe and M. Fukumoto, “AwareLESS authentication: Insensible input based authentication,” *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2007, pp. 2561–2566.

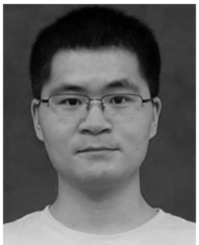
[61] H.-Y. Chen, J. Park, S. Dai, and H. Z. Tan, “Design and evaluation of identifiable KeyClick signals for mobile devices,” *IEEE Trans. Haptics*, vol. 4, no. 4, pp. 229–241, Fourth Quarter 2011.



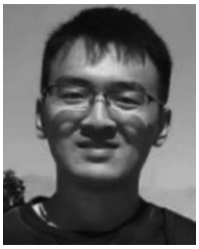
Hangcheng Cao (Student Member, IEEE) is currently working toward the PhD degree with the College of Computer Science and Electronic Engineer, Hunan University, China. From 2021 to 2022, he works as a joint PhD student with the School of Computer Science and Engineering at Nanyang Technological University (NTU), Singapore. He has published papers in ACM Ubicomp/IMWUT 2020, IEEE ICDCS 2021, etc. His research interests lie in the area of IoT security, particularly user authentication on smart devices, side channel attacks, and data anomaly detection.

Daibo Liu (Member, IEEE) received the PhD degree in computer science and engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2018. He was a visiting researcher with the School of Software, Tsinghua University from 2014-2016, and Department of Electrical and Computer Engineering, University of Wisconsin–Madison from 2016-2017. He is currently an assistant professor with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China. His research interests cover the broad areas of low power wireless networks, mobile and pervasive computing, and system security. He is a member of the ACM.

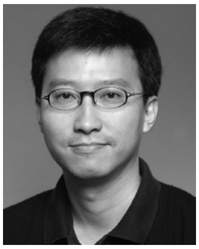
Hongbo Jiang (Senior Member, IEEE) received the PhD degree from Case Western Reserve University, in 2008. He is currently a full professor with the College of Computer Science and Electronic Engineering, Hunan University. He was a professor with the Huazhong University of Science and Technology. He has been serving on the editorial board of *IEEE/ACM Transactions on Networking*, *IEEE Transactions on Mobile Computing*, *ACM Transactions on Sensor Networks*, *IEEE Transactions on Network Science and Engineering*, *IEEE Transactions on Intelligent Transportation Systems*, *IEEE Internet of Things Journal*, etc. He was also invited to serve on the TPC of IEEE INFOCOM, ACM WWW, ACM/IEEE MobiHoc, IEEE ICDCS, IEEE ICNP, etc. He is an elected fellow of IET (The Institution of Engineering and Technology), fellow of BCS (The British Computer Society), senior member of ACM, and full member of IFIP TC6 WG6.2. Now his research focuses on computer networking, especially, wireless networks, data science in Internet of Things, and mobile computing.



Chao Cai received the PhD degree from the School of Electronic Information and Engineering, Huazhong University of Science and Technology, Wuhan, China. He is an associate professor with the College of Life Science and Technology, Huazhong University of Science and Technology. He has worded as a postdoc with the School of Computer Science and Engineering, Nanyang Technology University, Singapore. He has published papers in *IEEE Comunication Survey and Tutorial*, *IEEE Transactions on Mobile Computing*, *IEEE Transactions on Network and Service Management*, *IEEE Internet of Things Journal*, IEEE INFOCOM, ACM MobiCom, ACM Ubicomp, ACM Sensys, etc. His current research interests include mobile computing, acoustic sensing, wireless sensing, embedded system, digital signal processing, and deep learning



Tianyue Zheng (Graduate Student Member, IEEE) received the BEng degree in telecommunication engineering from the Harbin Institute of Technology, China, and the MEng degree in computer engineering from the University of Toronto, Canada. He is currently working toward the PhD degree in computer science with Nanyang Technological University, Singapore. He has published papers in *IEEE Transactions on Mobile Computing*, *IEEE Communications Magazine*, IEEE INFOCOM, ACM MobiCom, ACM Ubicomp/IMWUT, ACM Sensys, etc. His research interests include RF sensing and deep learning.



John C. S. Lui (Fellow, IEEE) received the PhD degree in computer science from the University of California, Los Angeles, CA, USA, in 1992. He is currently the Choh-Ming Li professor with the Department of Computer Science and Engineering, The Chinese University of Hong Kong (CUHK), Hong Kong. He was the chairman of the department from 2005 to 2011. His current research interests are in communication networks, network/system security (e.g., cloud security, mobile security, etc.), network economics, network sciences (e.g., online social networks, information spreading, etc.), cloud computing, large-scale distributed systems, and performance evaluation theory. He is an elected member of the IFIP WG 7.3, a fellow of the Association for Computing Machinery (ACM), a senior research fellow of the Croucher Foundation, and was the chair of the ACM SIGMETRICS. He has been serving in the Editorial Board of the *IEEE/ACM Transactions on Networking*, *IEEE Transactions on Computers*, *IEEE Transactions on Parallel and Distributed Systems*, *Performance Evaluation*, and the *International Journal of Network Security*. He received various departmental teaching awards and the CUHK Vice-Chancellors Exemplary Teaching Award. He is also a co-recipient of the Best Paper Award in the IFIP WG 7.3 Performance 2005, IEEE/IFIP NOMS 2006, and SIMPLEX 2013.

Jun Luo (Senior Member, IEEE) received the BS and MS degrees in electrical engineering from Tsinghua University, China, and the PhD degree in Computer science from EPFL (Swiss Federal Institute of Technology in Lausanne), Lausanne, Switzerland. From 2006 to 2008, he has worked as a postdoctoral research fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada. In 2008, he joined the faculty of the School Of Computer Science and Engineering, Nanyang Technological University in Singapore, where he is currently an associate professor. His research interests include mobile and pervasive computing, wireless networking, machine learning and computer vision, as well as applied operations research.