WristPass: Secure Wearable Continuous Authentication via Ultrasonic Sensing

Xinyue Fang[1], Jianwei Liu[1,2], Yike Chen[1], Xian Xu[1], and Jinsong Han[1]

[1]Zhejiang University, China
[2]Hangzhou City University, China
{xinyuefang, jianweiliu, chenyike, xianxu, hanjinsong}@zju.edu.cn

***Abstract*—Smartwatches have become increasingly prevalent in people's daily lives, offering support for a wide range of privacy and security-sensitive applications, such as SMS messaging and mobile payment. Consequently, there is an imperative need for independent user authentication on smartwatches to safeguard against property loss and personal privacy breaches. However, current authentication methods rely on passwords, leaving users vulnerable to shoulder surfing attacks. Moreover, existing biometric-based authentication methods either require dedicated sensors or cannot support continuous authentication. In this paper, we propose a replay-resistant continuous authentication system on smartwatches, namely *WristPass*. It extracts acoustic impedance biometrics from ultrasonic signals. Leveraging a theoretical model based on the principle of ultrasound propagation, *WristPass* correlates spectrograms of reflected signals with impedance features of wrist skin. Utilizing a deep learning model as a feature extractor, *WristPass* mines fine-grained impedance features from the spectrograms for accurate user authentication. Additionally, to prevent *WristPass* from replay attacks, we design a device fingerprinting method to detect replayed signals. Extensive experiments show that *WristPass* can achieve 96.7% accuracy in user authentication. Furthermore, *WristPass* exhibits robustness for long-term usage.**

***Index Terms*—Wireless Sensing, User Authentication, Acoustic Impedance Biometrics**

I. Introduction

In the past decade, smart wristbands have become increasingly popular. Smartwatch, as the representative of them, enables a variety of emerging applications, such as fitness tracking and health monitoring [1]. With the development of the e-economy, the smartwatch market continuously increases. According to the report of Allied Market Research, the global smartwatch market was valued at 42.7 billion in 2022, and is projected to reach 164.7 billion by 2032 [2]. Recently, the smartwatch demonstrates a trend towards privatization. It gradually supports a wide range of privacy and security-critical applications, such as SMS messaging and mobile payment [3]. To ensure security and protect ongoing sessions, the smartwatch necessitates one-time user verification and continuous authentication functions to enforce access control.

Traditional authentications of wearable devices rely on "what users know", i.e., password [4], [5]. But such knowledge-based methods not only demand users to remember certain digital sequences, but also are vulnerable to shoulder-surfing attacks and smudge attacks [3], [6]. In order to avoid this dilemma, "something users are" is utilized to offer more convenient and secure authentication. For example, Hutchins et al. [7] introduce a rhythm-based password which is a set of recorded beats when the user taps the device. Sehrt et al. [8] extract bone conduction features from white noise sound to achieve user identification. Chen et al. [6] use the motor to generate vibration signals for bony feature acquisition. Yang et al. [9] extract arm physical characteristics from responses generated by the motor to identify users. Lee et al. [3] also design a challenge-response scheme to extract body structure features for user authentication. However, these methods either require dedicated hardware (e.g., laryngophone) that not possessed in smartwatches [8] or cannot support continuous authentication [3], [6], [7], [9]. Therefore, there is an urgent demand for a low-cost and secure continuous authentication method on smartwatch-like wristbands.

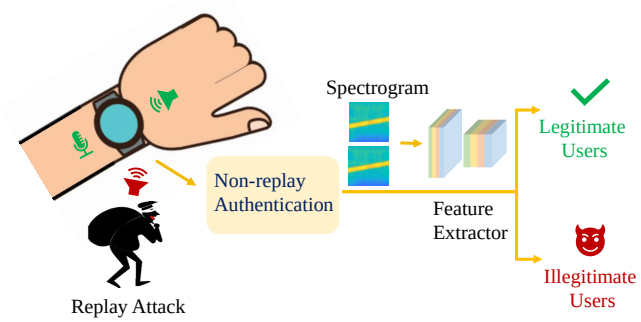


Fig. 1. Illustration of *WristPass*.

In this paper, we propose a novel continuous authentication system on the smartwatch named *WristPass*. It uses the smartwatch's in-built electronic components (i.e., speaker and microphone) to emit and capture ultrasounds to probe the wrist skin biometrics for authentication. As shown in Fig. 1, when an authentication attempt is initiated, the speaker of the smartwatch emits a delicate ultrasonic signal. Then, *WristPass* receives the ultrasound reflected from the user's wrist and detects replay attacks by judging whether the signals originate from the smartwatch's built-in speaker. For a non-replay authentication request, *WristPass* extracts skin features, namely acoustic impedance biometrics, from ultrasonic signals to accomplish user authentication. Compared with previous

Jinsong Han is the corresponding author.

works, *WristPass* can be deployed on commercial smartwatches without introducing extra hardware. Meanwhile, as ultrasound is imperceptible to humans and can be transmitted automatically without user cooperation, it has outstanding usability and user-friendliness. Besides, *WristPass* is highly secure due to the anti-replay mechanism we have designed.

To realize *WristPass* in practice, we address the following questions: (1) **How to extract effective and representative acoustic impedance features from acoustic signals to achieve accurate user authentication?** Unlike visual data such as images and videos, interpreting ultrasonic signals is not straightforward. Identifying the segment of the signal that encapsulates impedance biometrics poses a challenge. To figure out the embodiment of the impedance characteristics in the ultrasound reflection, we build a theoretical correlation between them based on the ultrasound propagation principle. Upon this theoretical model, we conduct frequency-domain analysis on the ultrasonic signals to get spectrograms, which makes the impedance features more prominent. Then, we develop a deep learning model to extract fine-grained impedance features from spectrograms to achieve accurate authentication. (2) **How to prevent *WristPass* from replay attacks?** The open nature of the acoustic channel exposes the authentication system susceptible to potential replay attacks. Attackers can eavesdrop during the legal authentication process and replay the recorded ultrasonic signals to the smartwatch, attempting to deceive *WristPass*. To enhance the security of *WristPass*, we shift our focus to the physical characteristics of the speaker. We noticed that the speaker possesses unique hardware fingerprints. Hence, we first extract hardware fingerprints of the speaker from the ultrasonic signals captured by the smartwatch. Then, we utilize a one-class classifier to discern whether the signals originate from the smartwatch's built-in speaker or illegitimate replay devices, thereby providing anti-replay functionality.

We build a prototype of *WristPass* on a commercial off-the-shelf (COTS) smartwatch and perform extensive experiments. We evaluate *WristPass* with 18 volunteers under different conditions. The experiment results show that *WristPass* can achieve an authentication success rate of 96.7%. Meanwhile, *WristPass* can defend against various attacks. Moreover, the robustness study demonstrates that the performance of *WristPass* will not degrade over time. In summary, our contributions are as follows:

- We propose a replay-resistant continuous authentication system on smartwatches, namely *WristPass*. It achieves non-intrusive and user-friendly user identification by capturing skin impedance biometrics from ultrasonic reflections without introducing any hardware overhead.
- We establish a theoretical correlation between the ultrasonic signals and skin acoustic impedance biometrics based on the ultrasound propagation principle. The proposed authentication scheme is potential to be integrated into other devices with audio pickup outfits, such as smart AR glasses.
- We prototype *WristPass* with COTS devices and perform extensive experiments. The experiment results indicate that *WristPass* can achieve accurate and robust authentication, while defending against various attacks.

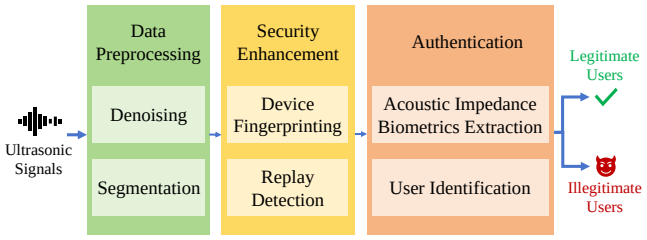


Fig. 2. Workflow of *WristPass*.

II. Threat Model

Analyzing the security of an authentication system is paramount. In an adversarial environment against smartwatch authentication, the attacker's goal is to steal private information, such as health data and messages, or perform unauthorized operations like online payments. In the threat model, we assume that the attacker has gained physical access to user's smartwatch. We mainly consider four types of most threatening and common attacks on smart wristband authentication.

Zero-effort attack. For this attack, we assume that the attacker is unfamiliar with *WristPass*. Rather than following the authentication process to present a biometric feature, the attacker endeavors to break the authentication system with zero effort.

Mimic attack. In this attack, the attacker first observes the user's behavior (e.g., hand gesture) during the verification process and replicates the wearing position as well as strap tightness. Then, s/he endeavors to bypass *WristPass* by imitating the user's authentication habit.

Impersonation attack. For this attack, we presume that the attacker is aware of the appearance characteristics (e.g., shape) of the user's wrist. S/he invites a person whose wrist resembles that of the user to initiate authentication, aiming to trick *WristPass*.

Replay attack. Due to the openness of the physical world, wireless signal-based authentications usually suffer from replay attacks. In this attack, we assume a sophisticated attacker who has basement knowledge about *WristPass*. S/he uses a qualified microphone to record ultrasound during the authentication sessions. Then, the recorded signals are replayed to the smartwatch by an external speaker, trying to be accepted as a legal user.

III. System Overview

To establish a secure continuous authentication system on smart wristbands, *WristPass* extracts the acoustic impedance of the wearer's wrist skin from the received ultrasound signals to differentiate persons. As shown in Fig. 2, *WristPass* is primarily composed of three modules: data preprocessing, security enhancement, and user authentication. When an individual initiates an authentication request with the smartwatch, *WristPass* emits an ultrasound as the stimulus signal, specifically a chirp signal ranging from 17kHz to 22kHz. Such a frequency band falls within the range barely detectable by the human

ear, thereby imperceptible to users. The duration of the chirp signal is set to 5 seconds, as prior research demonstrate that a duration exceeding 5 seconds would not significantly enhance the acoustic sensing performance [8], [10]. Then, the emitted ultrasound is reflected by the wrist skin and received by the smartwatch. Afterward, the data preprocessing module will perform signal denoising and segmentation to get a clean signal. Subsequently, in the security enhancement module, our defense mechanism is activated to ascertain the source of the received ultrasonic signals. If they originate from an unauthorized device (e.g., replayed by a cellphone), the authentication request will be rejected. Otherwise, they will be fed into the user authentication module. In this module, *WristPass* extracts wrist skin biometrics (i.e., impedance features) from the clean signals and employs a deep learning model to achieve user identification. Particularly, if the user wants to perform one-time verification, the aforementioned operations only need to be performed once. If a continuous authentication is necessary, *WristPass* will repeat these operations until the security-critical session concludes.

Data preprocessing. This module plays an essential role of providing clean ultrasound samples. The main processes include removing the noise from ultrasonic signals through filtering and segmenting the signals to obtain each complete chirp signal. We will elaborate on this module in Sec. IV.

Security enhancement. With the processed ultrasonic signals, *WristPass* extracts the device fingerprints to determine whether the authentication request is initiated by a replay attacker or not. If the signals are detected from illegitimate devices, *WristPass* would deny the access; otherwise, *WristPass* proceeds with the user authentication mechanism in the third module. The details of this process will be introduced in Sec. VII.

User authentication. In this module, *WristPass* initially derives the signal spectrogram from the ultrasound, which can reflect the user's acoustic impedance. Then, *WristPass* extracts deep acoustic impedance features from the spectrogram using a well-designed deep learning model, and performs user classification. If all the probabilities output by the learning model fall below a pre-set acceptance threshold, *WristPass* identifies the wearer as an illegitimate user and consequently denies the access. Otherwise, the authentication is deemed to be initiated by a legitimate user associated with the largest probability. The user authentication approach will be detailed in Sec. V and Sec. VI.

IV. Data Preprocessing

Raw ultrasonic signals reflected by the wrist skin contain much environment and hardware noise that is irrelevant to the acoustic impedance. Therefore, in the data preprocessing module, we utilize a denoising method to obtain clean ultrasonic measurements. In addition, to obtain each chirp signal for subsequent feature extraction, we locate each chirp profile and perform signal segmentation.

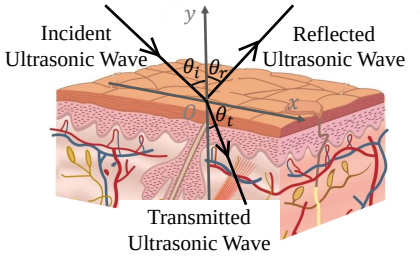


Fig. 3. Ultrasonic signal propagation path.

A. Signal Denoising

Besides the acoustic impedance features, the microphone of the smartwatch also picks up environmental and hardware noise that would degrade the authentication performance. To solve this problem, we utilize a bandpass Butterworth filter [11] to remove such noise, thereby getting stable amplitude-frequency characteristics that embody the impedance biometrics. The passband frequency range of the filter is set to 17-22kHz. Moreover, we apply a Hamming window [12] to smooth the reflected signals and reduce the frequency leakage caused by signal truncation.

B. Signal Segmentation

Next, we adopt a segmentation method to locate and intercept the chirp signals from denoised microphone data. Time stamp-based methods cannot deal with unintended signal interruptions caused by hardware instability. So we use a phase-locked loop [13], a tool capable of locating signals with a certain frequency. Specifically, we detect the frequency points of 17kHz and 22kHz of the signals. Then, these cutting points are used to segment each chirp signal.

V. Extracting Acoustic Impedance Biometrics from Ultrasound Reflection

To extract effective and representative acoustic impedance features from ultrasonic signals, we first construct an ultrasound propagation model to figure out the correlation between wrist acoustic impedance and ultrasonic signals. Based on this model, we qualify the acoustic impedance biometrics by frequency-domain analysis.

A. Acoustic Impedance Biometrics in Ultrasound Reflection

Acoustic impedance biometrics of the wrist skin is the key enabler of *WristPass*. To obtain accurate impedance features, we build a theoretical model based on the principle of ultrasound propagation to analyze the impedance information in ultrasound reflection.

As shown in Fig. 3, we consider a two-dimensional signal propagation path. In the x-y plane, the ultrasound wave emitted from the built-in speaker of the smartwatch enters the wrist skin through the air. Let's denote the incident angle, the reflection angle, and the transmission angle as θ_i, θ_r, and θ_t, respectively. According to the principle of sound wave propagation [14], the sound pressure P_i generated by the incident wave at the air-skin boundary can be expressed as:

$$P_i = P_{i0}\exp(i(wt - \frac{w}{c_1}xcos\theta_i - \frac{w}{c_1}ysin\theta_i)), \quad (1)$$

where P_{i0} is the sound pressure amplitude of the incident wave, w is the angular frequency, and c_1 is the propagation speed of the sound wave in the air. Similarly, the sound pressure P_r and P_t, generated by the reflected wave and transmitted wave at the boundary can be respectively expressed:

$$P_r = P_{r0}\exp(i(wt + \frac{w}{c_1}xcos\theta_r - \frac{w}{c_1}ysin\theta_r)), \quad (2)$$

$$P_t = P_{t0}\exp(i(wt - \frac{w}{c_2}xcos\theta_t - \frac{w}{c_2}ysin\theta_t)), \quad (3)$$

where P_{r0} and P_{t0} are the sound pressure amplitudes of the reflected wave and the transmitted wave, respectively. c_2 is the propagation speed of sound waves in the wrist skin. Further, we can get the particles' normal vibration velocities perpendicular to the boundary as follows:

$$v_{ix} = \frac{P_i}{\rho_1 c_1}cos\theta_i, \quad (4)$$

$$v_{rx} = -\frac{P_r}{\rho_1 c_1}cos\theta_r, \quad (5)$$

$$v_{tx} = \frac{P_t}{\rho_2 c_2}cos\theta_t, \quad (6)$$

where ρ_1 and ρ_2 are the density of the air and the wrist skin, respectively. Note that the acoustic impedance [14] is defined as $Z = \rho c$, so the acoustic impedance along the normal line can be calculated as:

$$Z_n = Z/cos\theta = \rho c/cos\theta, \quad (7)$$

At a boundary between two different media, the sound waves on both sides of the interface must meet the following two Boundary Conditions [14]: (a) the sound pressure remains continuous, (b) the particle's normal vibration velocity perpendicular to the boundary remains continuous, that is:

$$(P_i + P_r)|_{x=0} = P_t|_{x=0}, \quad (8)$$

$$(v_{ix} + v_{rx})|_{x=0} = v_{tx}|_{x=0}. \quad (9)$$

Meanwhile, known from Snell's Law, the propagation direction of the incident ultrasonic wave, reflected ultrasonic wave and transmitted ultrasonic wave must adhere to:

$$\frac{sin\theta_i}{c_1} = \frac{sin\theta_r}{c_1} = \frac{sin\theta_t}{c_2}. \quad (10)$$

Taking Eq. 1 through Eq. 7 and Eq. 10 into the boundary conditions Eq. 8 and Eq. 9, we can obtain the reflection coefficient r_P of sound pressure as follows:

$$r_P = \frac{P_{r0}}{P_{i0}} = \frac{\rho_2 c_2 cos\theta_i - \rho_1 c_1 cos\theta_t}{\rho_2 c_2 cos\theta_i + \rho_1 c_1 cos\theta_t} = \frac{Z_{n2} - Z_{n1}}{Z_{n2} + Z_{n1}}, \quad (11)$$

where Z_{n1} and Z_{n2} are the acoustic impedance along the normal line of the air and the wrist skin, respectively. Consequently, with the definition of sound intensity $I = P_0^2/2Z_n$, we can calculate the reflection coefficient r_I of sound intensity as follows:

$$\begin{aligned} r_I &= \frac{I_{r0}}{I_{i0}} = \frac{P_{r0}^2/2Z_{n1}}{P_{i0}^2/2Z_{n1}} \\ &= (\frac{\rho_2 c_2 cos\theta_i - \rho_1 c_1 cos\theta_t}{\rho_2 c_2 cos\theta_i + \rho_1 c_1 cos\theta_t})^2 = (\frac{Z_{n2} - Z_{n1}}{Z_{n2} + Z_{n1}})^2. \end{aligned} \quad (12)$$

It can be deduced from Eq. 12 that, with the same incident angle, the intensity of the reflected ultrasonic wave is determined by the acoustic impedance of the skin. In other words, the acoustic impedance information of skin can be embodied by the intensity of the reflected ultrasonic waves. Further, since different people possess distinct and unique acoustic impedance of wrist skin, there exists the potential to achieve user authentication by probing the acoustic impedance through ultrasonic sensing with a smartwatch.

B. Signal Spectrogram Derivation

According to the above theoretical analysis, the intensity of the reflected ultrasound can reveal the acoustic impedance biometrics. Meanwhile, we noticed that the Short-Time Fourier Transform (STFT) [15] can make the intensity of the reflected ultrasound more prominent. Thus, we apply the STFT technique to transfer the acoustic signals into the spectrograms.

Specifically, based on a window function $h(\tau)$ with length T, the signal is divided into several short-time windows. The Fourier Transform is applied to each window to get the corresponding spectrum information. By moving the window on the timeline, the spectral characteristics of signals at different time can be acquired. The calculation method is as follows:

$$STFT(t, f) = \sum_{\tau=t}^{t+T-1} s(\tau)h(\tau - T)\exp(-j2\pi f\tau), \quad (13)$$

where t and f are the time and the frequency index, respectively. To get the intensity of signals, we compute the modular value of the STFT result as follows:

$$spectrum(t, f) = |STFT(t, f)^2|. \quad (14)$$

Now we convert the reflected signals to a two-dimensional matrix with the intensity information. To further extract the skin acoustic impedance, we will feed this intensity matrix into a deep learning model. For ease of training, we convert the intensity matrix to a grey-scale spectrogram. Each pixel at the spectrogram position (t, f) represents the intensity of the signal at that point. However, due to signal reflection attenuation, most values in the original matrix are close to zero. In this case, directly mapping the matrix to the spectrogram will result in information loss. To address this issue, we use a square root mapping method. Specifically, we calculate the square root of all values in the matrix and then map the resulting values to integers ranging from 0 to 255. After the above processing, we will obtain a two-dimensional signal spectrogram with sufficient and prominent impedance information for further authentication.

VI. User Authentication

So far, we have reconstructed spectrograms from reflected ultrasonic signals, which contain sufficient acoustic impedance biometrics. Next, we map the impedance features into user identities for authentication. We noticed that convolutional neural networks (CNN) have shown excellent feature extraction abilities [16]. Thereby we develop a CNN-based feature

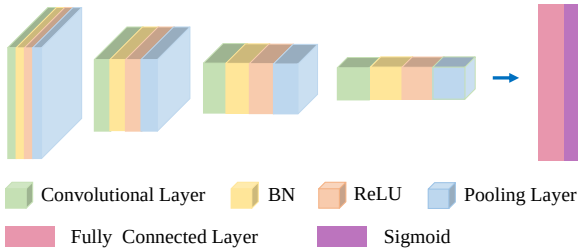


Fig. 4. The architecture of our biometric extractor.

extractor to mine fine-grained impedance features from spectrograms. In this section, we first introduce the architecture of our CNN model, and then detail the training strategy.

A. Architecture of Feature Extractor

We develop a CNN-based feature extractor with four convolutional layers and one fully connected layer to extract deep impedance features and identify users. The inputs of the extractor are the spectrograms, while the outputs are probabilities indicating the likelihood that the impedance biometrics correspond to each legitimate user. The identity associated with the highest probability is regarded as the final result.

The detailed structure of the feature extractor is shown in Fig. 4. Each convolutional layer is followed by a batch normalization (BN) function [17] and a rectified linear unit (ReLU) [18]. The convolutional kernel size and the slide stride are empirically set to 3×3 and 1×1, respectively. BN is used to prevent data distribution from offset and ReLU is used to decrease the inter-neuronal dependence. They work jointly to improve the effectiveness and robustness of the feature extractor. Meanwhile, after each convolutional layer, a max pooling layer is arranged to reduce the size for further feature extraction. The pooling kernel is set to 2×2 empirically.

After undergoing the two-dimensional convolutional operation, the output is flattened into a feature vector and fed into a fully connected layer with a Sigmoid function [19]. This layer maps the feature vector into different classes (i.e., different user IDs), so that we can train the feature extractor by loss calculation and back propagation [20]. The Sigmoid function normalizes the outputs to get the probability for each class.

B. Training Strategy

To ensure our feature extractor ability of mining the impedance information, we adopt a supervised learning manner to update its parameters. Specifically, we employ cross-entropy [21] as the loss function, which can be computed as:

$$CrossEntropy = -\sum_{x}(p(x)\log q(x)), \tag{15}$$

where the probability distribution $p(x)$ is the expected output, while the probability distribution $q(x)$ is the real output. Besides, we utilize Adam [22] as the optimizer, as it possesses adaptive learning rates, allowing it to find individual learning rates for each parameter.

In the registration phase, each user needs to provide several acoustic signal samples as training data. In the authentication process, the unseen spectrograms with impedance biometrics will be fed into the well-trained feature extractor, which will output the probabilities that the input belongs to each legitimate user. If all probabilities are smaller than the threshold, the individual is regarded as an illegal invader. Otherwise, the authentication request is approved and the individual is considered to be a legitimate user belonging to the identity with the highest probability.

VII. Security Enhancement

This section first analyzes the security of *WristPass*, and then, details the defense to protect *WristPass* from attacks.

A. Security Analysis

Zero-effort attack: Since *WristPass* necessitates wrist biometrics to initiate the authentication session, the attacker who is unfamiliar with the principle cannot pass the verification. So *WristPass* is capable of defending against zero-effort attacks.
Mimic attack: Even if the attacker imitates the user's behaviour, the wrist acoustic impedance is still dissimilar to the legitimate user, resulting in the output probabilities less than the acceptance threshold. Hence, *WristPass* can defend against mimic attacks.
Impersonation attack: Due to the uniqueness of the wrist acoustic impedance, even wrists with similar shape or size in appearance still have different wrist acoustic impedance, which can be identified by *WristPass*. Therefore, the attack will fail and *WristPass* is able to defend against impersonation attacks.
Replay attack: Because of the open nature of acoustic channels, eavesdropping is almost impossible to guard against in practice. The attacker can use a hidden microphone to record ultrasound that contains user's biometrics, and then infiltrates into *WristPass* by replaying the recordings. So, it is necessary to find a method for defending against replay attacks.

According to the aforementioned analysis, *WristPass* demonstrates inherent resistance against zero-effort, mimic, and impersonation attacks. However, it is not naturally resilient to replay attacks. Therefore, in the subsequent sections, we devise an anti-replay method to mitigate such attacks.

B. Anti-replay Design

To prevent *WristPass* from replay attacks, our insight is to determine whether the received signals originate from the smartwatch itself. If they come from external devices other than the smartwatch's built-in speaker, the authentication attempt is very likely to be initiated by a replay attacker. To this end, we propose a device fingerprinting approach to ascertain the source of the received signals. The approach involves extracting device fingerprints from ultrasonic signals and then utilizing a one-class classifier to figure out the signals' origin.
Device fingerprinting. Due to manufacturing imperfections, speakers on different devices possess distinct characteristics [23]. Further, the acoustic signals generated by different speakers have distinguishable fingerprints. Therefore, we can extract hardware features from ultrasound to judge if it was emitted by a malicious speaker. Moreover, previous works show that frequency responses of speakers can serve as device

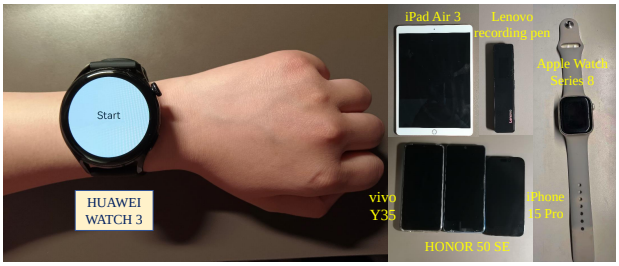


Fig. 5. Experiment setup.

fingerprints [24], [25]. Inspired from that, we calculate the statistical characteristics of the signal spectrograms reconstructed from ultrasound, i.e., mean μ and variance σ^2, as the fingerprints of the corresponding devices. They can be calculated as follows:

$$\mu = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} g(i,j), \tag{16}$$

$$\sigma^2 = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (g(i,j) - \mu)^2, \tag{17}$$

where $M \times N$ is the size of the spectrogram. $g(i,j)$ is the greyscale value of the point on row i and column j. Finally, we construct a fingerprint vector with the two types of statistical scalars.

Replay detection. To ascertain whether the ultrasound originates from the smartwatch's speaker, we train a one-class classifier with the legitimate data. It is widely known that One-Class Support Vector Machine (SVM) is significantly effective in unsupervised learning with only one class data [26]. Therefore, we train the One-Class SVM model using data collected from the smartwatch. Subsequently, we utilize this well-trained model to eliminate signals emitted by external speakers.

VIII. Evaluation

This section first describes the implementation of *WristPass*, and then details its performance under real-world environments.

Experiment setup. As shown in Fig. 5, we build a proof-of-concept prototype of *WristPass* to evaluate its authentication performance. This prototype is implemented on a commercial off-the-shelf (COTS) smartwatch, i.e., HUAWEI WATCH 3. To enable ultrasound transmitting and receiving simultaneously, we develop a Harmony App based on DevEco Studio 3.0. This app utilizes the *AudioRenderer package* to make the smartwatch emit the ultrasonic chirp signals with its built-in speaker and record the reflected ultrasound via a built-in microphone. The sampling rate of the acoustic signal is set to 48kHz. Additionally, to evaluate the effectiveness of our device fingerprint-based anti-replay method, we use six common COTS sound pick-up devices as malicious recorders, including three smartphones (iPhone 15 Pro, vivo Y35, HONOR 50 SE), one digital recording pen (Lenovo), one smartwatch (Apple Watch Series 8), and one tablet (iPad Air 3). All experiments are conducted by adhering to the approval of our university's Institutional Review Board (IRB).

Data collection. We invite 18 volunteers (eleven females and seven males) to participate in our experiments, with heights ranging from 151cm to 179cm and ages ranging from 23 to 72. Among them, 14 volunteers participate in the experiment as legitimate users and 4 volunteers as illegitimate users. We set an acceptance threshold (empirically set to 0.93) to determine whether legitimate or not. Before data collection, participants are allowed to familiarize themselves with the smartwatch and adjust the wristband according to their preference. Afterwards, each participant is asked to collect at least 60 signal samples for evaluation.

Metrics. We define four metrics to quantify the performance of *WristPass*: Authentication Success Rate (ASR), False Accept Rate (FAR), False Reject Rate (FRR), and Defense Success Rate (DSR). ASR describes the probability that *WristPass* correctly identifies a legitimate user. It can be calculated by:

$$ASR = 100\% \times \frac{N_{user}^{corr}}{N_{user}}, \tag{18}$$

where N_{user}^{corr} and N_{user} are the number of successfully accepted legitimate authentication attempts and the number of all legitimate authentication attempts, respectively. DSR is the probability that an illegitimate user is successfully detected. It can be calculated as:

$$DSR = 100\% \times \frac{N_{il}^{corr}}{N_{il}}, \tag{19}$$

where N_{il}^{corr} is the number of successfully detected illegitimate authentication attempts and N_{il} is the number of all illegitimate authentication attempts. FRR indicates the probability that *WristPass* mistakenly authenticates a legitimate user as an illegitimate one. It can be formulated as:

$$FRR = 100\% \times \frac{N_{user}^{wr}}{N_{user}}, \tag{20}$$

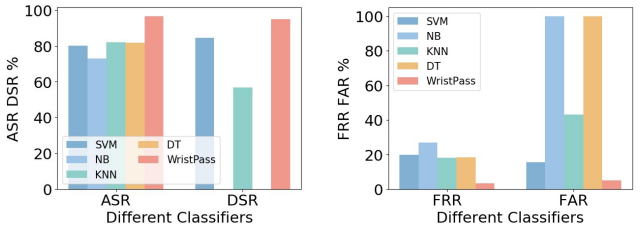
where N_{user}^{wr} is the number of wrongly rejected legitimate authentication attempts. FAR represents the probability that *WristPass* falsely accepts an illegitimate user as a legitimate one. It can be expressed as:

$$FAR = 100\% \times \frac{N_{il}^{wr}}{N_{il}}, \tag{21}$$

where N_{il}^{wr} and N_{il} are the number of wrongly accepted illegitimate authentication attempts and the number of all illegitimate authentication attempts, respectively. The higher the ASR and DSR, as well as the lower the FAR and FRR, the better the authentication capability and security of *WristPass*.

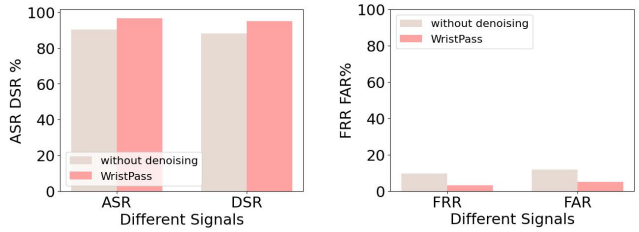
A. Overall Performance

We first evaluate the performance of our feature extractor by comparing it with four commonly-used classifiers, including Support Vector Machine (SVM), Naive Bayes classifier (NB), K-Nearest Neighbours (KNN), and Decision Tree (DT). For the dataset, we make a [80%, 20%] random split for training and testing. Each classifier runs ten times and we take the average of these metrics as the final results. The ASR, DSR, FRR, and FAR of these classifiers are shown in Fig. 6. It can be observed that NB has the worst performance. The overall



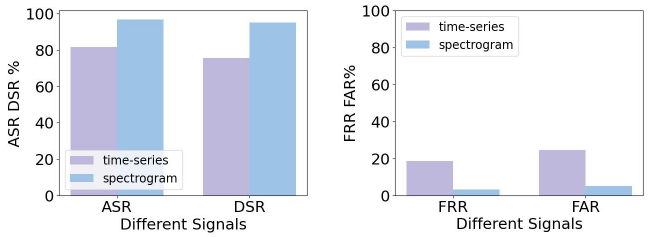
(a) ASR, DSR of classifiers. (b) FRR, FAR of classifiers.

Fig. 6. Overall performance of classifiers.



(a) ASR, DSR of different signals. (b) FRR, FAR of different signals.

Fig. 7. Overall performance of without denoising signals and *WristPass*.



(a) ASR, DSR of different signals. (b) FRR, FAR of different signals.

Fig. 8. Overall performance of time-series signals and spectrograms.

ASR and DSR of our feature extractor are 96.7% and 95% respectively, which outperforms other classifiers. Meanwhile, our feature extractor also achieves the lowest FRR and FAR of 3.3% and 5%, respectively. These results demonstrate that our feature extractor is able to mine deep and fine-grained impedance biometrics to achieve accurate user authentication, while other traditional classifiers do not have such ability.

Next, to prove the effectiveness of our denoising method, we compare the performance of *WristPass* with that of signals without data denoising. As shown in Fig. 7, the ASRs for *WristPass* and signals without denoising are 96.7% and 90.3%, respectively. Meanwhile, the DSRs of *WristPass* and signals without denoising are 95% and 88.2%, respectively. These results indicate that *WristPass* can effectively remove the noise in the raw signals to realize high-performance authentication.

Lastly, to show the superiority of our spectrograms, we compare the performance with that achieved with time-series ultrasound signals. As shown in Fig. 8, the ASRs for spectrograms and time-series signals are 96.7% and 81.5%, respectively. Meanwhile, the DSRs of spectrograms and time-series signals are 95.0% and 75.4%, respectively. The comparison results indicate that our signal spectrograms are effective in making impedance biometrics more prominent.

B. Security Study

This part evaluates the security of *WristPass* against the four attacks introduced in the threat model.

Zero-effort attack. In this attack, an attacker attempts to gain recognition from *WristPass* by wearing the smartwatch directly. To assess the defense ability of *WristPass* against the attack, we treat three volunteers as attackers to initiate malicious authentication requests. The result is shown in Table I, the mean DSR for attackers is 99.54%, which indicates *WristPass* is able to defend against zero-effort attacks effectively.

TABLE I
DEFENSE ABILITY OF *WristPass*.

Attack	DSR	FAR
Zero-effort attack	99.54	0.46
Mimic attack	98.89	1.11
Impersonation attack	98.33	1.67
Replay attack	99.79	0.21

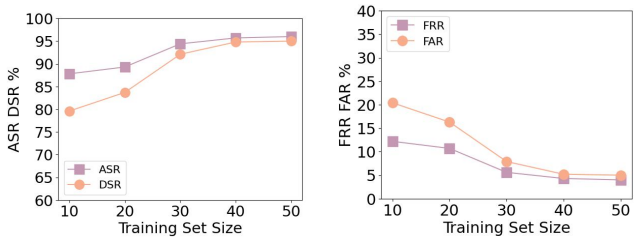
Mimic attack. In this attack, the attacker tries to trick *WristPass* by mimicking the behaviour of a legitimate user. In the defense experiment, we invite three volunteers to mimic the way (wearing manners and hand gestures) when the legitimate users initiate the authentication sessions. As shown in Table I, the mean DSR is 98.89%. Therefore, *WristPass* is capable of defending against mimic attacks.

Impersonation attack. In this attack, the attacker is able to find an illegitimate user whose wrist is similar to a legitimate one. The attacker tries to bypass *WristPass* by making the illegitimate user wear the smartwatch to initiate authentication. In the defense experiment, we selected two pairs of volunteers with similar wrists. For each pair, we treat one volunteer as an illegitimate user, and the other as a legitimate one. The experiment result (Table I) shows that the DSR for impersonation attacker is 98.33%. Therefore, *WristPass* can also defend against impersonation attacks.

Replay attack. In this attack, the attacker first eavesdrops on the ultrasonic signals during legitimate authentication, and then replays the recordings to deceive *WristPass*. To simulate replay attacks, we use other devices with microphones to record the reflected signals from the legitimate user's wrist. Then, we replay the recorded audio to the smartwatch to evaluate the defense ability of *WristPass*. As shown in Table I, the DSRs of different recording devices are 99.79%. Thus, our anti-replay method is effective in detecting replay trials.

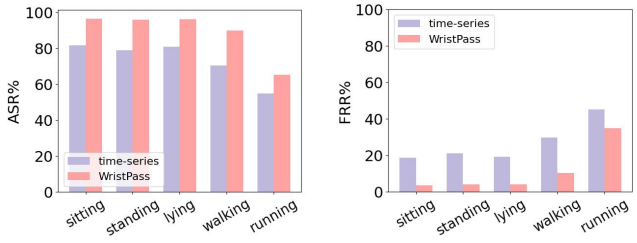
C. Effect of Training Set Size

As *WristPass* adopts supervised learning to achieve user authentication, the size of the training set size, i.e., the number of training samples (chirp sounds) provided by each user, would affect the authentication performance. In this experiment, we investigate such effect by varying the number of each user's training samples from 10 to 50 in step of 10. The resulting ASR, DSR, FRR, and FAR are illustrated in Fig. 9. It can be found that the ASRs and DSRs increase as the training set size grows, while the FRRs and FARs decrease. When the training set size increases to 40, the ASR



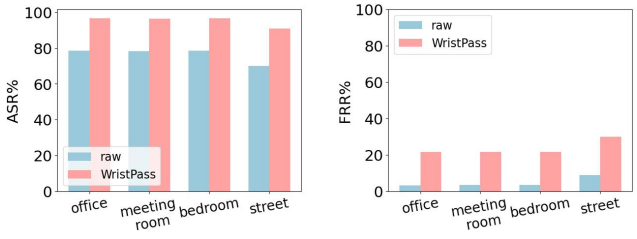
(a) Effect of the training set size on ASR and DSR. (b) Effect of the training set size on FRR and FAR.

Fig. 9. Effect of training set size.



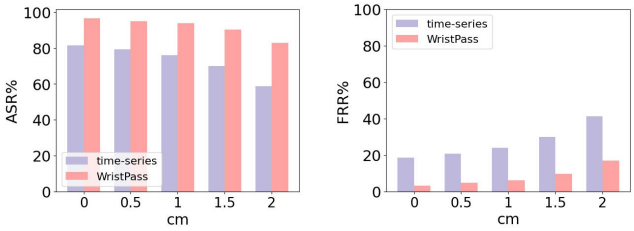
(a) ASR of different signals. (b) FRR of different signals.

Fig. 10. Impact of body posture and motion.



(a) ASR of different signals. (b) FRR of different signals.

Fig. 11. Impact of environmental noise.



(a) ASR of different signals. (b) FRR of different signals.

Fig. 12. Impact of smartwatch wearing manner.

and DSR are gradually becoming saturated. The performance under 50 training samples is only slightly better than that under 40 training samples. Therefore, collecting 50 data for model training is sufficient for providing a good authentication service. Since collecting 50 chirp sounds only consumes 250 seconds, *WristPass* is very user-friendly.

D. Robustness Analysis

In this part, we focus on four factors that may impact the performance of *WristPass*, including user's posture and motion, environment noise, smartwatch wearing manner, and time.

Impact of body posture and motion. During the usage of the smartwatch, people may engage in other activities concurrently with various postures or body movements. Thus, we consider five common user postures and motions, including sitting, standing, lying, walking, and running. Fig. 10 illustrates that *WristPass* is robust against various postures and body movements except for running. So we advise users not to register while running.

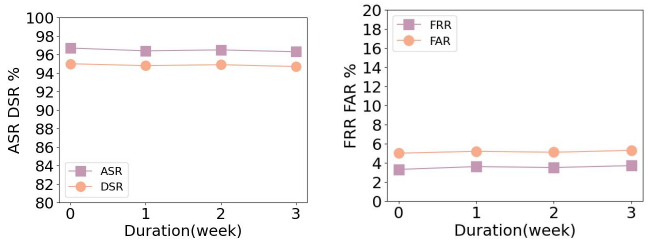
Impact of environmental noise. People often wear smartwatches in various scenarios with diverse environmental noise. To assess *WristPass*'s robustness against noise interference, we conduct experiments in four typical scenarios: an office, a meeting room, a bedroom, and a street side. As shown in Fig. 11, *WristPass* maintains high ASRs in various scenarios. Although the ASR drops slightly at the street side, it still remains above 91%, significantly higher than the ASRs of the raw signals. This suggests that our data denoising method can effectively eliminate noise and improve the quality of biometrics. More importantly, *WristPass* is robust against environmental interference.

Impact of smartwatch wearing manner. In practice, people may wear the smartwatch on different positions of the wrist. Therefore. we evaluate the performance when the smartwatch position shifts on the wrist. We measure the reflected signals from 0 to 2cm (in step of 0.5cm) away from the baseline where the user usually wears the smartwatch habitually. The resulting ASRs and DSRs are shown in Fig. 12. It can be observed that when the distance between the wearing position and the baseline is less than 1.5cm, the ASRs are above 90%. When the distance keeps increasing, the ASR would decrease obviously. Considering that people tend to wear their watches in their customary positions, the distance changes of wearing position is usually within 1.5cm, where *WristPass* still demonstrates high ASR. Hence, the user's wearing habits can help *WristPass* maintain good authentication performance.

Long-term observation. We conduct a long-term study for three weeks to verify the stability of the used acoustic impedance biometrics. Four participants (two legitimate users and two illegitimate users) take part in the experiments. They are tested three times over a three-week period, with a week between each two. As shown in Fig. 13, the ASRs of *WristPass* are always higher than 96%, while the DSRs of *WristPass* maintain above 96%. This means that the performance of *WristPass* will not degrade significantly over time.

E. Overhead

In this part, we evaluate the storage overhead of *WristPass*. It mainly comes from three aspects: the Harmony APP, the authentication signal, and the feature extractor. Firstly, the Harmony APP only takes up 158KB. Besides, one authentication signal sample consumes about 0.98MB. As for the feature extractor, it occupies about 236MB. Thus, the total storage overhead of *WristPass* is 237MB approximately, which is far less than the smartwatch's memory capacity of 10GB. Therefore, the storage overhead of *WristPass* is acceptable. To further reduce the storage consumption, users can adopt knowledge distillation technique [27], or perform authentication on a cloud server.



(a) ASR and DSR of different time. (b) FRR and FAR of different time.
Fig. 13. Long-term observation.

TABLE II
COMPARISON WITH EXISTING METHODS.

System	User-imperceptible	without Dedicated Hardware	Continuous Authentication	Replay-resistant
Beat-PIN [7]	×	✓	×	✓
VA [3]	×	✓	×	/
WristConduct [8]	×	×	✓	×
WristPass	✓	✓	✓	✓

F. Comparison with Existing Methods

We compare *WristPass* with three state-of-the-art wearable authentication methods: Beat-PIN [7], VA [3], and WristConduct [8], in terms of user-friendliness, hardware overhead, continuous authentication ability, and replay resilience. As depicted in Table II, Beat-PIN requires user interaction to obtain user's tapping rhythm. VA needs to motivate the motor to generate vibrations. WristConduct emits audible white noise. These methods would cause discomfort to users, but *WristPass* only emits user-imperceptible ultrasound, thus greatly enhancing the user-friendliness. Besides, although WristConduct offers continuous authentication, it carries the risk of replay attacks and requires dedicated hardware, which is unavailable on COTS smartwatches. Beat-PIN and VA are replay-resistant and can be implemented on COTS smartwatches, yet they cannot support continuous authentication. Because Beat-PIN requires user interaction, while the vibrations of VA may cause discomfort to users. Different from the three works, *WristPass* is not only replay-resistant, but also supports continuous authentication. In summary, compared with existing methods, *WristPass* stands out as it is the only system that enables secure, continuous, and user-friendly authentication on COTS smartwatch without any dedicated hardware.

IX. RELATED WORK

This work is mainly related to two kinds of techniques: ultrasonic sensing and smartwatch-based authentication.

A. Ultrasonic sensing

Ultrasonic signals are widely utilized across various applications due to their inaudibility, accessibility, and cost-effectiveness [28]–[30]. COTS mobile and wearable devices can transmit and receive ultrasound without causing disturbance to surrounding individuals, thus offering a promising platform for ultrasonic sensing [12], [31]–[34]. For example, ultrasonic signals can be used for recognizing finger/hand gestures [35]. VSkin [36] utilizes ultrasound to capture finger tapping and movements. RobuCIR [37] proposes a contact-free gesture recognition system based on ultrasonic sensing. Besides, ultrasonic sensing enables devices to support health monitoring. Ubi-Asthma [38] implements an asthma detection system on the smartwatch using ultrasonic signals to obtain health-related breathing signals. UltraMotion [1] employs the paired smartwatch and smartphone for real-time arm motion tracking. Different from previous works, we leverage ultrasound to capture user's skin acoustic impedance biometrics to achieve continuous authentication.

B. Authentication on Smartwatch

Over the past decade, smartwatches have demonstrated a trend towards privatization [39]. To ensure security, smartwatches need a reliable user authentication system [40]. Traditional methods like passwords and patterns are vulnerable towards thermal attacks or smudge attacks [3], [6]. Beat-PIN [7], [41] takes a set of recorded beats as a user's password when the user taps the device. However, tapping rhythm based method needs interaction with users, either cannot provide continuous authentication. VibID [9] extracts arm physical features from vibration responses for user authentication. Lee et al. [3] also design a challenge-response scheme to obtain body physical structure features. However, these vibration-based methods would cause discomfort to users. WristConduct [8] emits audible white noise to extract bone conduction features. However, it is vulnerable to replay attacks and requires dedicated hardware. Different from prior approaches, *WristPass* achieves replay-resistant continuous authentication by collecting acoustic impedance features, which is imperceptible to users and does not require any interactions.

X. CONCLUSION

In this paper, we propose a replay-resistant continuous authentication system on smartwatches, namely *WristPass*. It extracts acoustic impedance biometrics from ultrasound signals reflected off the wrist skin to identify users. To do so, we initially build a theoretical model to figure out the correlation between the impedance features and the ultrasound reflection. Based on this model, we perform frequency-domain analysis on the signal to get spectrograms. Then, we employ a deep learning model to mine fine-grained impedance features from the spectrograms and achieve accurate user authentication. To protect *WristPass* from replay attacks, we design a device fingerprinting method to detect replayed signals. Extensive experiments show that *WristPass* can achieve an authentication success rate of 96.7%. Meanwhile, *WristPass* is secure and robust for long-term use.

ACKNOWLEDGEMENT

This paper is supported by the National Natural Science Foundation of China under grant U21A20462 and 62372400, National Key R&D Program of China under grant No. 2023YFC3805602, "Pioneer" and "Leading Goose" R&D Program of Zhejiang under grant No. 2023C01033.

REFERENCES

[1] X. Niu, K. Zou, D. Shen, S. Drew, S. Wu, G. Guo, and R. Chen, "Ultramotion: High-precision ultrasonic arm tracking for real-world exercises," *IEEE Transactions Mobile Computing (TMC)*, vol. 23, no. 2, pp. 1846–1862, 2024.

[2] A. M. Research, "Smartwatch market research, 2032," https://www.alliedmarketresearch.com/smartwatch-market#:~:text=The%20global%20smartwatch%20market%20was%20valued%20at%20%2442.7,multifaceted%20device%20seamlessly%20using%20technology%20into%20our%20routines., 2022.

[3] S. Lee, W. Choi, and D. H. Lee, "Usable user authentication on a smartwatch using vibration," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2021.

[4] T. Nguyen and N. D. Memon, "Smartwatches locking methods: A comparative study," in *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[5] Y. Zhao, Z. Qiu, Y. Yang, W. Li, and M. Fan, "An empirical study of touch-based authentication methods on smartwatches," in *Proceedings of the ACM International Symposium on Wearable Computers (ISWC)*, 2017.

[6] W. Chen, L. Chen, Y. Huang, X. Zhang, L. Wang, R. Ruby, and K. Wu, "Taprint: Secure text input for commodity smart wristbands," in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2019.

[7] B. Hutchins, A. Reddy, W. Jin, M. Zhou, M. Li, and L. Yang, "*Beat-PIN*: A user authentication mechanism for wearable devices through secret beats," in *Proceedings of the ACM on Asia Conference on Computer and Communications Security (AsiaCCS)*, 2018.

[8] J. Sehrt, F. Y. Lu, L. Husske, A. Roesler, and V. Schwind, "Wristconduct: Biometric user authentication using bone conduction at the wrist," in *Proceedings of the Mensch und Computer (MuC)*, 2022.

[9] L. Yang, W. Wang, and Q. Zhang, "Vibid: User identification through bio-vibrometry," in *Proceedings of the ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2016.

[10] S. Schneegass, Y. Oualil, and A. Bulling, "Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, 2016.

[11] A. V. Oppenheim, *Discrete-time signal processing*. Pearson Education India, 1999.

[12] R. Wang, L. Huang, and C. Wang, "Low-effort VR headset user authentication using head-reverberated sounds with replay resistance," in *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, 2023.

[13] G. Hsieh and J. C. Hung, "Phase-locked loop techniques. A survey," *IEEE Trans. Ind. Electron.*, vol. 43, no. 6, pp. 609–615, 1996.

[14] H. G. Tattersall, "The ultrasonic pulse-echo technique as applied to adhesion testing," *Journal of Physics D: Applied Physics*, vol. 6, no. 7, p. 819, 1973.

[15] L. Cohen, "Time-frequency distributions-a review," *Proc. IEEE*, vol. 77, no. 7, pp. 941–981, 1989.

[16] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, 2017.

[17] C. Garbin, X. Zhu, and O. Marques, "Dropout vs. batch normalization: an empirical study of their impact to deep learning," *Multim. Tools Appl.*, vol. 79, no. 19-20, pp. 12 777–12 815, 2020.

[18] R. Arora, A. Basu, P. Mianjy, and A. Mukherjee, "Understanding deep neural networks with rectified linear units," in *Proceedings of the International Conference on Learning Representations (ICLR)*, 2018.

[19] G. Mourgias-Alexandris, G. Dabos, N. Passalis, A. Tefas, A. Totovic, and N. Pleros, "All-optical recurrent neural network with sigmoid activation function," in *Proceedings of the IEEE Optical Fiber Communications Conference and Exhibition (OFC)*, 2020.

[20] A. Mukherjee, D. K. Jain, P. Goswami, Q. Xin, L. Yang, and J. J. P. C. Rodrigues, "Back propagation neural network based cluster head identification in MIMO sensor networks for intelligent transportation systems," *IEEE Access*, vol. 8, pp. 28 524–28 532, 2020.

[21] L. Li, M. Doroslovacki, and M. H. Loew, "Approximating the gradient of cross-entropy loss function," *IEEE Access*, vol. 8, pp. 111 626–111 635, 2020.

[22] X. Jiang, B. Hu, S. C. Satapathy, S. Wang, and Y. Zhang, "Fingerspelling identification for chinese sign language via alexnet-based transfer learning and adam optimizer," *Sci. Program.*, vol. 2020, pp. 3 291 426:1–3 291 426:13, 2020.

[23] A. Das, N. Borisov, and M. Caesar, "Do you hear what I hear?: Fingerprinting smart devices through embedded acoustic components," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2014.

[24] Z. Zhou, W. Diao, X. Liu, and K. Zhang, "Acoustic fingerprinting revisited: Generate stable device ID stealthily with inaudible sound," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2014.

[25] Z. Ba, S. Piao, and K. Ren, "Defending against speaker fingerprinting based device tracking for smartphones," in *Proceedings of the IEEE Symposium on Privacy-Aware Computing, PAC*, 2017.

[26] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Comput.*, vol. 13, no. 7, pp. 1443–1471, 2001.

[27] G. E. Hinton, O. Vinyals, and J. Dean, "Distilling the knowledge in a neural network," *CoRR*, vol. abs/1503.02531, 2015.

[28] J. Tan, C. Nguyen, and X. Wang, "Silenttalk: Lip reading through ultrasonic sensing on mobile phones," in *Proceedings of the IEEE Conference on Computer Communications, (INFOCOM)*, 2017.

[29] L. Lu, J. Yu, Y. Chen, H. Liu, Y. Zhu, Y. Liu, and M. Li, "Lippass: Lip reading-based user authentication on smartphones leveraging acoustic signals," in *Proceedings of the IEEE Conference on Computer Communications, (INFOCOM)*, 2018.

[30] J. Tan, X. Wang, C. Nguyen, and Y. Shi, "Silentkey: A new authentication framework through ultrasonic-based lip reading," *Proceedings of the ACM Interactive, Mobile, Wearable and Ubiquitous Technol (IMWUT)*, vol. 2, no. 1, pp. 36:1–36:18, 2018.

[31] Y. Zhang, W. Huang, C. Yang, W. Wang, Y. Chen, C. You, D. Huang, G. Xue, and J. Yu, "Endophasia: Utilizing acoustic-based imaging for issuing contact-free silent speech commands," *Proceedings of the ACM Interactive, Mobile, Wearable and Ubiquitous Technol (IMWUT)*, vol. 4, no. 1, pp. 37:1–37:26, 2020.

[32] Y. Gao, W. Wang, V. V. Phoha, W. Sun, and Z. Jin, "Earecho: Using ear canal echo for wearable authentication," *Proceedings of the ACM Interactive, Mobile, Wearable and Ubiquitous Technol (IMWUT)*, vol. 3, no. 3, pp. 81:1–81:24, 2019.

[33] L. Huang and C. Wang, "Pcr-auth: Solving authentication puzzle challenge with encoded palm contact response," in *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, 2022.

[34] L. Lu, J. Yu, Y. Chen, and Y. Wang, "Vocallock: Sensing vocal tract for passphrase-independent user authentication leveraging acoustic signals on smartphones," *Proceedings of the ACM Interactive, Mobile, Wearable and Ubiquitous Technol (IMWUT)*, vol. 4, no. 2, pp. 51:1–51:24, 2020.

[35] B. V. Dam, Y. Murillo, M. Li, and S. Pollin, "In-air ultrasonic 3d-touchscreen with gesture recognition using existing hardware for smart devices," in *Proceedings of the 2016 IEEE International Workshop on Signal Processing Systems (SiPS)*, 2016.

[36] K. Sun, T. Zhao, W. Wang, and L. Xie, "Vskin: Sensing touch gestures on surfaces of mobile devices using acoustic signals," in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2018.

[37] Y. Wang, J. Shen, and Y. Zheng, "Push the limit of acoustic gesture recognition," *IEEE Transactions Mobile Computing (TMC)*, vol. 21, no. 5, pp. 1798–1811, 2022.

[38] Y. Wu, J. Zhang, Y. Chen, J. Wang, W. Shi, and Q. Zhang, "Ubi-asthma: Toward ubiquitous asthma detection using the smartwatch," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11 576–11 587, 2023.

[39] Y. Zeng, A. Pande, J. Zhu, and P. Mohapatra, "Wearia: Wearable device implicit authentication based on activity information," in *Proceedings of the IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, (WoWMoM)*, 2017.

[40] A. Lewis, Y. Li, and M. Xie, "Real time motion-based authentication for smartwatch," in *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, 2016.

[41] H. Zhang, X. Xiao, S. Ni, C. Dou, W. Zhou, and S. Xia, "Smartwatch user authentication by sensing tapping rhythms and using one-class DBSCAN," *Sensors*, vol. 21, no. 7, p. 2456, 2021.