Active Acoustic Sensing Based Authentication System Using a Door Handle

Tomoki Konishi
IPLAB
University of Tsukuba
Tsukuba, Japan
konishi@iplab.cs.tsukuba.ac.jp

Myungguen Choi
IPLAB
University of Tsukuba
Tsukuba, Japan
choi@iplab.cs.tsukuba.ac.jp

Buntarou Shizuki
IPLAB
University of Tsukuba
Tsukuba, Japan
shizuki@cs.tsukuba.ac.jp

Abstract

This paper presents a system that authenticates users solely based on the action of grasping a door handle. The system authenticates users by utilizing the differences in frequency characteristics between a hand and a door handle when grasped. The frequency characteristics of a hand vary from person to person depending on anatomical differences such as skeletal structure and muscle composition. This system is beneficial because it is not vulnerable to shoulder surfing and allows authentication solely by grasping the door handle. Data were collected from 25 users, and the system achieved an F1 score of 93.0% in the 25-class classification. In the One-vs-Rest classification using unknown users as test data, the average equal error rate was 4.76%.

CCS Concepts

• **Security and privacy → Biometrics**.

Keywords

Smart lock, Biometrics, Security, User identification, Machine learning

ACM Reference Format:

Tomoki Konishi, Myungguen Choi, and Buntarou Shizuki. 2024. Active Acoustic Sensing Based Authentication System Using a Door Handle. In *International Conference on Mobile and Ubiquitous Multimedia (MUM '24), December 01–04, 2024, Stockholm, Sweden.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3701571.3701587

1 Introduction

Smart locks are becoming increasingly popular because they do not require a physical key. Current smart locks use authentication technologies based on knowledge (PIN and password) [1, 35], possession (smartphones and card keys) [13, 14, 32], or biometrics (fingerprint [39, 43], voiceprint [7, 15, 21], iris [45], and faceprint [48]). However, these technologies faced numerous issues, as follows. Knowledge-based authentication technologies are susceptible to attacks [1, 54], such as dictionary attacks and shoulder surfing, and they become inconvenient for users if the number of passcode digits is too large [2, 11]. Meanwhile, possession-based authentication technologies carry the risk of unauthorized use if the smartphone or card key is lost, biometric-based authentication technologies are vulnerable to presentation attacks using photos, voice recordings, and fingerprint films.

To address these issues, several authentication methods using a door handle have been proposed [12, 41]. SmartHandle [12] focuses on the individual differences in hand movements when opening a door and performs authentication based on the natural action of lowering the door handle. Sekiguchi *et al.* [41] asked users to design their preferred door handle-lowering gestures, which were then used for authentication. These studies perform authentication based on the act of lowering a door handle, realizing methods that avoid the risk of loss and are robust against presentation attacks. While SmartHandle [12] poses a risk of shoulder surfing, Sekiguchi *et al.* [41] conducted experiments to assess resistance to shoulder surfing. However, users are required to perform a particular gesture to unlock the door, which also raises concerns about the memorability of the gestures.

To avoid shoulder surfing and eliminate the need for additional actions to unlock the door, we developed a system that authenticates users solely based on how they grasp the door handle. This system does not require any particular actions to unlock the door, and thus, there is no risk of shoulder surfing. The system uses active acoustic sensing [37] in the inaudible frequency range to authenticate users by detecting differences in frequency characteristics when they grasp the door handle. Active acoustic sensing is a technique that involves transmitting acoustic signals to a target object and analyzing its vibration response to recognize changes in the shape, material, and boundary conditions of the object [37]. In this study, the acoustic signals obtained through active acoustic sensing vary depending on the hand itself and the door handle's boundary condition, i.e., how users grasp it, making imitation by third parties difficult. Therefore, we hypothesize that active acoustic sensing applied to the door handle could authenticate a user's grasp.

The contributions of this study are as follows. 1) We implement an authentication system using active acoustic sensing, which verifies users based on how they grasp the door handle. 2) We demonstrate that our system can classify 25 participants with an F1 score of 93.0% based on how they grasp the door handle. 3) Finally, we demonstrate that this system can reject imposters with an average equal error rate (EER) of 4.76%.

2 Related Work

In this study, we aim to authenticate users based on how they grasp the door handle using active acoustic sensing. In this section, we

MUM '24, December 01–04, 2024, Stockholm, Sweden

ACM ISBN 979-8-4007-1283-8/24/12
https://doi.org/10.1145/3701571.3701587

provide an overview of related work on active acoustic sensing and authentication systems using door handles.

2.1 Active Acoustic Sensing

Active acoustic sensing is a technique that involves transmitting acoustic signals to a target object and analyzing its vibration response to recognize changes in the shape, state, material, and boundary conditions of the object [37]. Researchers developed systems utilizing active acoustic sensing for various purposes, including gesture recognition [3, 16, 22, 26, 33, 36, 44, 51, 53, 55], force estimation [34, 38], internal structure identification of 3D printed objects [24, 25], and silent speech recognition [56]. These studies use active acoustic sensing for object recognition and user activity recognition, while in this study, we use active acoustic sensing for user authentication.

The acoustic signals obtained through active acoustic sensing vary depending on the object's shape, state, and material, making imitation by third parties difficult; hence, it is widely used in user authentication research. Authentication systems using active acoustic sensing have often been studied in the context of wearable devices, particularly earphones [4, 5, 9, 10, 17, 31, 49, 52].

Research has also been conducted on devices other than earphones. Watanabe *et al.* [50] used a microphone and speaker attached to a device imitating a smartwatch to identify users, resulting in 91.2% accuracy among nine participants. Liu *et al.* [29] used a microphone attached to the throat to capture the resonance of voices transmitted through the body and identified users, resulting in 91.4% accuracy among 29 participants. Isobe *et al.* [18, 19] attached a microphone and speaker to the nose pads of smart glasses to identify wearers with 9% EER among 12 participants. SkullID [42] attached a speaker to the right mastoid process and a microphone at various skull locations to authenticate smart glass users with 2.35% EER among 25 participants. Iwakiri *et al.* [20] used a microphone and speaker connected to a device imitating a smart ring to identify users, resulting in an EER of of 2.7% among seven participants. Finally, LipPass [30] used a smartphone's microphone and speaker to identify users based on differences in lip movements while speaking, resulting in 90.2% accuracy with 48 participants.

We implement a system that applies active acoustic sensing to door handles to authenticate users based on differences in the frequency characteristics of a hand and a door handle.

2.2 Authentication System using Door Handle

Several authentication systems use door handles, some of which also use such actions as turning the door handle, opening and closing the door, and images of the hand grasping the door handle [6, 8, 12, 40, 41, 47]. SmartHandle [12] uses an inertial measurement unit (IMU), gyroscope, and magnetometer to capture hand movements during door opening to authenticate users. SenseHandle [40] authenticates users based on door opening and closing actions using an IMU, swept frequency capacitive sensing, and active acoustic sensing. Vegas *et al.* [47] identifies users based on door opening actions using an IMU and gyroscope. Tietz *et al.* [46] identifies users based on touch interactions using pressure sensors. Futami *et al.* [8] identify users using an angular velocity sensor on the door handle based on room entry and exit actions. Kusanagi *et al.* [6] authenticates users using images of the metacarpophalangeal joints obtained from a camera mounted above the door handle. Sekiguchi *et al.* [41] authenticates users by recognizing their designed method of turning the door handle using capacitive sensors, pressure sensors, and an IMU attached to the door handle.

We authenticate users solely based on the action of grasping the door handle. To achieve this, we utilize the frequency characteristics of a hand and a door handle when the user grasps the door handle, which differ between users. This method does not require actions, such as opening the door or turning the door handle, during authentication, and it does not involve any particular gestures, thereby eliminating the risk of shoulder surfing.

3 Principle of Authentication

Our system uses active acoustic sensing [37] for authentication, as shown in Figure 1. Specifically, the system uses the frequency characteristics of a hand and a door handle for authentication when a user grasps the door handle. To observe these frequency characteristics, we attach a pair of piezoelectric elements to the door handle. One is used to transmit ultrasonic chirp sine signals through the door handle to the hand, and the other is used as a microphone to record acoustic signals from the door handle.

Note that the frequency characteristics of a hand vary from person to person depending on anatomical differences, such as skeletal structure and muscle composition. For example, a hand has 27 bones, and its shape and size differ from person to person, making their replication virtually impossible. In addition, due to the anatomical differences, how to grasp a door handle differs from person to person, meaning that the boundary condition differs. These differences make the frequency characteristics of the hand and door handle unique, allowing them to be used for authentication.

4 Implementation

In this study, we implemented the system shown in Figures 1 and 2 to test the principle described in Section 3. The system transmits a chirp signal from a speaker attached to the door handle, and it obtains the frequency characteristics by using the Fast Fourier Transform (FFT) on the acoustic signal received by a microphone. The obtained frequency characteristics are then input into a machine learning model to estimate the user. This section details the implementation of the system.

4.1 Hardware

The door handle used in this study is a lever-handle type (Figure 2a). A piezoelectric element (THRIVE, K2512BP1, $25 \times 12 \times 0.23$ mm) was used as the microphone and speaker. To avoid interfering with the grasping action, the microphone and speaker were fixed with vinyl tape on the side surfaces at both ends of the door handle. The piezoelectric elements were connected through a two-core shielded cable (Mogami, Superflexible Shielded 2-core AWG36) to a line plug (Pro Audition, AS-106) and then connected to a computer (OS: Windows 11, CPU: Intel Core i7-1065G7 1.50 GHz, RAM: 32 GB) via an audio interface (Steinberg, UR24C).

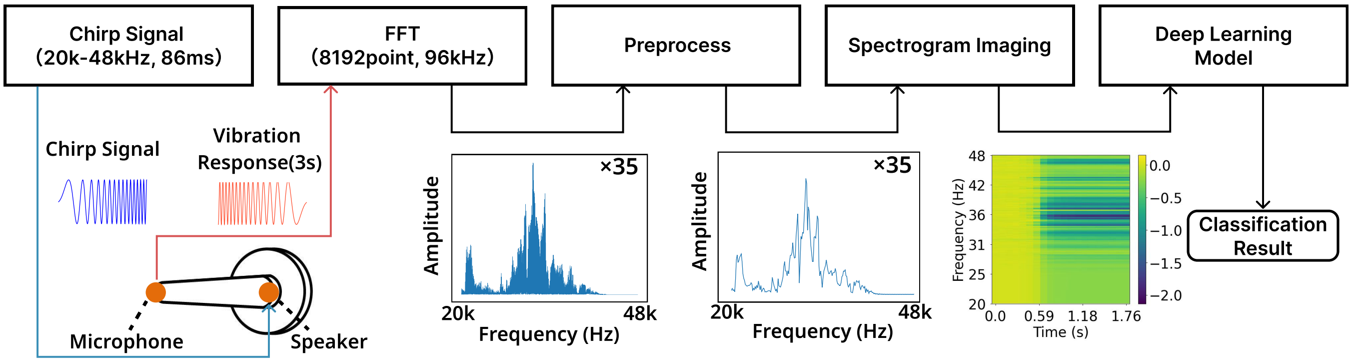

Figure 1: System overview.

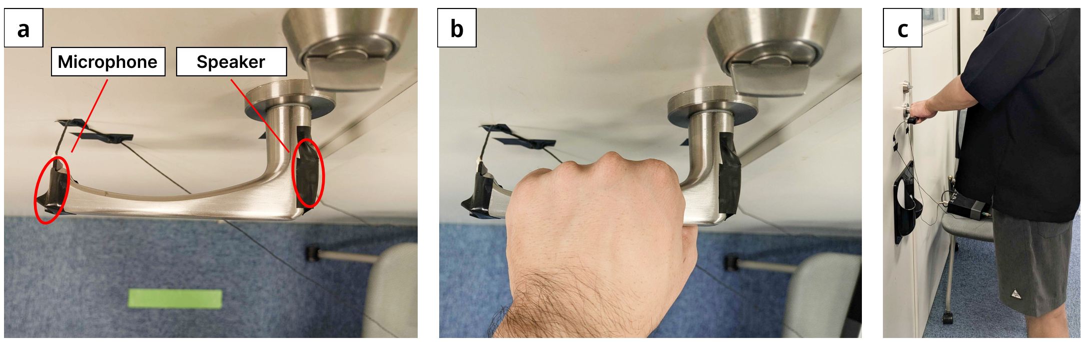

Figure 2: Setup in the experiment. (a) The door handle. (b) The act of grasping the door handle. (c) The side view.

4.2 Software

The software, similar to prior research on active acoustic sensing [26, 37], consists of four components: the chirp signal generation part, the FFT part, the preprocessing and feature extraction part, and the machine learning part.

4.2.1 Chirp signal. In the chirp signal generation part, a sinusoidal linear chirp signal whose frequency ranges between 20 kHz and 48 kHz is generated. The chirp signal increases monotonically for approximately 43 ms. The sampling rate used for signal playback was 96 kHz.

4.2.2 FFT. FFT is performed to convert the acoustic signals obtained from the microphone into frequency data. The FFT is conducted on the acoustic signals sampled at 96 kHz, with 8,192 points (i.e., two cycles of the chirp signal) per transformation. The FFT window has a 50% overlap, resulting in frequency data being obtained approximately every 43 ms.

4.2.3 Preprocessing and feature extraction. Because the frequency data contain noise, so we performed preprocessing on the data. First, the data in the frequency band from 20 kHz to 48 kHz are extracted. The extracted data are then smoothed in the time domain using an exponential moving average with a smoothing factor of 1/3. At this stage, the data have 4,779 dimensions, and consists of 35 frames along the time axis. Next, feature extraction is performed to reduce the dimension of the frequency data. Using cepstral analysis, we applied liftering to the first 224 dimensions and extracted 224-dimensional features using a 224-point filter bank.

Finally, the first frame's frequency values, which correspond to the frequency values of the ungrasped state, are saved as a baseline; they are used to take the difference from the frequency values of all frames before preprocessing. Next, we perform temporal segmentation to extract only the portions of the collected data where the grasping action occurs. As shown in Figure 3, the frequency characteristic values decrease (i.e., darker in this figure) at the moment of grasping and remain constant during the stationary state. Therefore, we define the frame at which the absolute value of the temporal difference in the mean frequency characteristic values exceeds a threshold, and the temporal difference is negative, as the moment when grasping begins. The threshold is set to the standard deviation of the temporal differences. From the frame identified as when the moment of grasping, we extract 20 frames (approximately 1.76 s) starting from 5 frames before this moment. The features obtained through the above processing were converted into 224×224 spectrograms using Matplotlib (Figure 3). The colors in the spectrogram correspond to the values of the frequency characteristics. We used the standard Matplotlib colormap, Viridis, to convert values to colors. These generated images were then used as inputs for the machine learning model.

4.2.4 Machine learning. Like several prior studies on acoustic sensing [23, 27, 28, 52, 56], we utilized a convolutional neural network (CNN) for machine learning. Various CNN models can be applied in

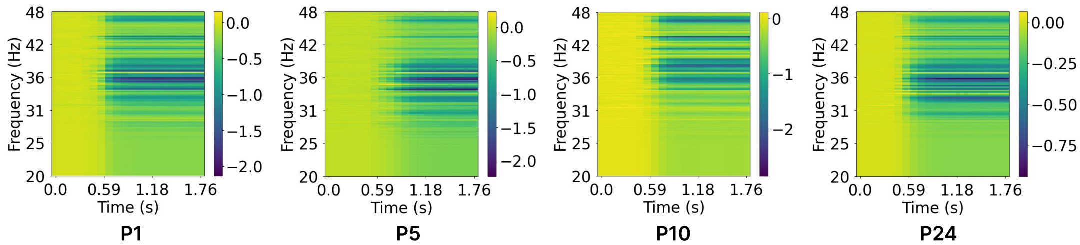

Figure 3: Example spectrograms when the door handle is grasped (P1, P5, P10, and P24 from left to right). The horizontal axis represents time, and the vertical axis represents frequency. The color indicates the magnitude of the values.

image recognition by converting frequency data into spectrogram images. The machine learning tasks included performing N-class classification and One-vs-Rest classification for N classes to investigate the performance of user authentication. We implemented CNN models used in our evaluation using Keras.

5 Evaluation

We conducted an experiment to evaluate the system's identification accuracy. The participants were 25 students (23 males, two females, P1–P25) aged 21–24 years (average age 22.6 years) from our laboratory. Among the participants, one was left-handed, while the rest were right-handed.

5.1 Procedure

Each participant stood in front of a door (Figure 2c) and grasped and released the door handle 100 times. Before the experiment began, participants were informed that the experiment was intended to collect data for an authentication system. Participants were then instructed to grasp the door handle with a consistent grip and strength. At the start of the experiment, participants stood at a fixed distance from the door, marked by tape on the floor, and held a mouse in their right hand. They were instructed to click the mouse, grasp the door handle with their left hand (Figure 2b), hold still, and release it 3 s after the mouse clicked upon verbal instruction. Each trial, consisting of grasping and releasing the door handle, was repeated 20 times per session for five sessions. Participants took at least 1-min break between session. Data collection was conducted for three seconds from the mouse click, obtaining 35 frames for each grasp-and-release action. Throughout the experiment, we collected 2,500 data points (20 trials $\times$ 5 sessions $\times$ 25 participants).

5.2 Evaluation Metrics

We conducted two evaluations: a 25-class classification to evaluate the system's identification accuracy and a One-vs-Rest binary classification to evaluate the accuracy against unknown users. In the 25-class classification, the system identifies known users, to manage room access. In this evaluation, the F1 score is used as the metric. In the One-vs-Rest classification, the system authenticates known users and rejects unknown users, a step intended for security applications. The EER is used as the metric in this evaluation, which is the error rate when the model's threshold is adjusted so the false acceptance rate (FAR), which is the rate at which imposters are misclassified as genuine users, equals the false rejection rate (FRR), which is the rate at which genuine users are misclassified as imposters.

5.3 Results

Identification Accuracy. First, we evaluated the performance of a 25-class classification for user identification. From the collected data, the first four sessions (80 samples) for each user were used as training data, and the last session (20 samples) was used as test data. Multiple models were used for 25-class classification to determine the best model by comparison.

The models we tested are shown in Table 1. We customized the output layer for use in the 25-class classification. A fully connected layer with 25 nodes was added to all models. The SoftMax function was used as the activation function, and categorical cross-entropy was used as the loss function. For all models, the learning rate was set to 0.0001, the batch size to 16, and the number of epochs to 50. As a result, the model with the highest F1 score was VGG16. The F1 score of VGG16 was 93.0%, and the accuracy was 93.1%.

Authentication Accuracy. Next, we evaluated the authentication accuracy for unknown users. Among the 25 participants, one was treated as a genuine user, and the remaining 24 were treated as imposters. The genuine user's first four sessions were used as training data, and the last session was used as test data. From all 16 imposters, six samples of each imposter were randomly selected , resulting in 96 data points for the training data. The data from the remaining eight imposters were used as test data. Thereafter, the test and training data were split among different imposters across 10 trials for each user, and the average EER was calculated. The model was based on VGG16, which achieved the highest accuracy in the 25-class classification. The model was added with a fully connected layer with two nodes. The sigmoid function was used as the activation function, and binary cross-entropy was used as the loss function. The learning rate was set to 0.0001, the batch size to 16, and the number of epochs to 50. As a result, the average EER of the 250 binary classification models was 4.76% (SD=28.53). The EER for each user is shown in Table 2.

6 Discussion

In this paper, we explored the potential of an authentication system using active acoustic sensing with a door handle. This paper is the first to investigate the potential of authentication using only the user's grasp on a door handle. Utilizing a microphone and speaker attached to the door handle, we achieved an F1 score of 93.0% and

Table 1: Model comparison results of 25-class classification.

Model	F1 (%)	Model	F1 (%)	Model	F1 (%)
DenseNet121	91.9	MobileNet	90.1	VGG16	93.0
InceptionResnetv2	90.0	MobileNetv2	92.4	VGG19	91.4
Inceptionv3	84.7	NasNet	87.6	Xception	86.7
ResNet50	45.8	ResNetV2	88.7		

Table 2: EER for each user in binary classification.

Participant	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
EER (%)	1.00	5.79	0.00	9.50	4.50	9.50	2.00	0.50	6.00	0.00	0.53	8.00	2.50
Participant	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	
EER (%)	3.50	2.50	1.00	7.50	6.00	5.50	10.50	0.50	11.67	9.50	3.00	8.00	

an accuracy of 93.1% in a 25-class classification task involving 25 participants. This result supports the hypothesis that active acoustic sensing applied to a door handle could authenticate the user's grasp of it. The 93.1% accuracy in the 25-class classification is comparable to the user identification accuracy (93–98%) reported in a previous study with the same number of participants of authentication systems using active acoustic sensing [42].

In addition, the EER was 4.76% in a binary classification task using test data that included unknown users assumed to be imposters. While direct comparisons are difficult, our method appears to achieve an accuracy comparable to previous studies on door handle-based authentication, such as Sekiguchi *et al.* [41] (11 participants, 81.6% precision rate, and 1.5% FAR) and SmartHandle [12] (11 participants, 87.27% true acceptance rate, and 1.39% FAR). This result indicates that user identification would be possible only by grasping the door handle. However, some participants, such as P20 and P22, exhibited lower accuracy (Table. 2). This is likely due to similarity in data among users. To improve accuracy, there is potential to enhance robustness against unknown users by using CNN for feature extraction and employing cosine distance for classification. Moreover, improving the 4.76% EER of using this method as a practical security technology is considered necessary. In SkullID [42], a study on an authentication method using active acoustic sensing with smart glasses, accuracy was improved by combining data from multiple microphones placed at different locations. Similarly, attaching multiple microphones to other parts of the door handle could improve accuracy.

While this study conducted security experiments using data from unknown imposters, the robustness against presentation attacks, assuming the leakage of spectrogram data, has not been evaluated. In addition, although data collection for the same participants was conducted on the same day, the composition of the human body changes over time, which could potentially lead to a decline in the performance of this method. Hence, conducting additional security evaluation experiments for this system is considered necessary. Moreover, it is expected that the accuracy will decrease as the number of participants increases.

7 Conclusion

We developed an authentication system using active acoustic sensing based solely on how users grasp a door handle, and we conducted accuracy evaluations. This system's accuracy achieved an F1 score of 93.0% in the 25-class classification, demonstrating sufficient accuracy for user identification. Further, an average EER of 4.76% was achieved in the One-vs-Rest classification using unknown users as test data. This paper demonstrates the feasibility of authentication based solely on how users grasp a door handle. It contributes to the advancement of smart locks that do not require any particular actions for unlocking.

Acknowledgments

We would like to extend our heartfelt gratitude to Takashi Amesaka from Keio University for his continuous guidance and valuable insights throughout the course of this research.

References

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 3751–3763.

[2] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Communication of the ACM* 42, 12 (1999), 40–46.

[3] Takashi Amesaka, Hiroki Watanabe, Masanori Sugimoto, and Buntarou Shizuki. 2022. Gesture Recognition Method Using Acoustic Sensing on Usual Garment. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 2, Article 41 (2022), 27 pages.

[4] Takashi Amesaka, Hiroki Watanabe, Masanori Sugimoto, Yuta Sugiura, and Buntarou Shizuki. 2023. User Authentication Method for Hearables Using Sound Leakage Signals. In *Proceedings of the 2023 ACM International Symposium on Wearable Computers (ISWC '23)*. Association for Computing Machinery, 119–123.

[5] Takayuki Arakawa, Takafumi Koshinaka, Shohei Yano, Hideki Irisawa, Ryoji Miyahara, and Hitoshi Imaoka. 2016. Fast and accurate personal authentication using ear acoustics. In *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*. 1–4.

[6] Kusanagi Daichi, Aoyama Shoichiro, Ito Koichi, and Aoki Takafumi. 2017. A practical person authentication system using second minor finger knuckles for door security. *IPSJ Transactions on Computer Vision and Applications* 9, 8 (03 2017).

[7] Phillip L. De Leon, Michael Pucher, Junichi Yamagishi, Inma Hernaez, and Ibon Saratxaga. 2012. Evaluation of Speaker Verification Security and Detection of HMM-Based Synthetic Speech. *IEEE Transactions on Audio, Speech, and Language Processing* 20, 8 (2012), 2280–2290.

[8] Kyosuke Futami, Akari Fukao, and Kazuya Murao. 2019. A method to recognize entering and leaving person based on door opening and closing movement using angular velocity sensor. In *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers*. Association for Computing Machinery, 57–60.

[9] Yang Gao, Yincheng Jin, Jagmohan Chauhan, Seokmin Choi, Jiyang Li, and Zhanpeng Jin. 2021. Voice In Ear: Spoofing-Resistant and Passphrase-Independent Body Sound Authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 1, Article 12 (2021), 12:1–12:25 pages.

[10] Yang Gao, Wei Wang, Vir V. Phoha, Wei Sun, and Zhanpeng Jin. 2019. EarEcho: Using Ear Canal Echo for Wearable Authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 3, Article 81 (2019), 24 pages.

[11] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. 2018. Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access. *Mobile Information Systems* 2018, 1 (2018), 2649598:1–2649598:16.

[12] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. 2019. SmartHandle: A Novel Behavioral Biometric-based Authentication Scheme for Smart Lock Systems. In *Proceedings of the 2019 3rd International Conference on Biometric Engineering and Applications (ICBEA 2019)*. Association for Computing Machinery, 15–22.

[13] Zhaoyang Han, Liang Liu, and Zhe Liu. 2019. An efficient access control scheme for smart lock based on asynchronous communication. In *Proceedings of the ACM Turing Celebration Conference - China* (Chengdu, China) *(ACM TURC '19)*. Association for Computing Machinery, Article 61, 5 pages.

[14] Zhaoyang Han, Liang Liu, and Zhe Liu. 2019. An efficient access control scheme for smart lock based on asynchronous communication. In *Proceedings of the ACM Turing Celebration Conference - China* (Chengdu, China) *(ACM TURC '19)*. Article 61, 5 pages.

[15] Georg Heigold, Ignacio Moreno, Samy Bengio, and Noam Shazeer. 2016. End-to-end text-dependent speaker verification. In *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE Press, 5115–5119.

[16] Atsutoshi Ikeda, Shinichi Kosugi, and Yasuhiro Tanaka. 2019. Propagating Vibration Analysis of Leg towards Ankle Joint Angle Estimation. In *Proceedings of the 24th International Conference on Intelligent User Interfaces: Companion* (Marina del Ray, California) *(IUI '19)*. Association for Computing Machinery, New York, NY, USA, 11–12.

[17] Irwansyah, Sho Otsuka, and Seiji Nakagawa. 2022. Evaluation of Bone-Conducted Cross-Talk Sound in the Head for Biometric Identification. In *Proceedings of the 2021 International Conference on Computer, Control, Informatics and Its Applications (IC3INA '21)*. Association for Computing Machinery, 76–80.

[18] Kaito Isobe and Kazuya Murao. 2021. Person-identification Method using Active Acoustic Sensing Applied to Nose. In *Proceedings of the 2021 ACM International Symposium on Wearable Computers (ISWC '21)*. Association for Computing Machinery, 138–140.

[19] Kaito Isobe and Kazuya Murao. 2023. Personal Identification Method using Active Acoustic Sensing applied to the Nose pad of Eyeglasses. In *Adjunct Proceedings of the 2022 ACM International Joint Conference on Pervasive and Ubiquitous Computing and the 2022 ACM International Symposium on Wearable Computers (UbiComp/ISWC '22 Adjunct)*. Association for Computing Machinery, 345–348.

[20] Shunsuke Iwakiri and Kazuya Murao. 2023. User Authentication Method for Wearable Ring Devices using Active Acoustic Sensing. In *Proceedings of the 2023 ACM International Symposium on Wearable Computers (ISWC '23)*. Association for Computing Machinery, 17–21.

[21] R G Maduranga M Jayamaha, Maduri R R Senadheera, T Nuwan C Gamage, K D Pavithra B Weerasekara, Gayan A Dissanayaka, and G. Nuwan Kodagoda. 2008. VoizLock - Human Voice Authentication System using Hidden Markov Model. In *2008 4th International Conference on Information and Automation for Sustainability*. 330–335.

[22] Hiroyuki Kato and Kentaro Takemura. 2016. Hand Pose Estimation Based on Active Bone-Conducted Sound Sensing. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* (Heidelberg, Germany) *(UbiComp '16)*. Association for Computing Machinery, New York, NY, USA, 109–112.

[23] Jiwan Kim and Ian Oakley. 2022. SonarID: Using Sonar to Identify Fingers on a Smartwatch. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, Article 287, 287:1–287:10 pages.

[24] Yuki Kubo, Kana Eguchi, and Ryosuke Aoki. 2020. 3D-Printed Object Identification Method using Inner Structure Patterns Configured by Slicer Software. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20)*. Association for Computing Machinery, 1–7.

[25] Yuki Kubo, Kana Eguchi, Ryosuke Aoki, Shigekuni Kondo, Shozo Azuma, and Takuya Indo. 2019. FabAuth: Printed Objects Identification Using Resonant Properties of Their Inner Structures. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. Association for Computing Machinery, 1–6.

[26] Yuki Kubo, Yuto Koguchi, Buntarou Shizuki, Shin Takahashi, and Otmar Hilliges. 2019. AudioTouch: Minimally Invasive Sensing of Micro-Gestures via Active Bio-Acoustic Sensing. In *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '19)*. Association for Computing Machinery, Article 36, 36:1–36:13 pages.

[27] Chi-Jung Lee, Ruidong Zhang, Devansh Agarwal, Tianhong Catherine Yu, Vipin Gunda, Oliver Lopez, James Kim, Sicheng Yin, Boao Dong, Ke Li, Mose Sakashita, Francois Guimbretiere, and Cheng Zhang. 2024. EchoWrist: Continuous Hand Pose Tracking and Hand-Object Interaction Recognition Using Low-Power Active Acoustic Sensing On a Wristband. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 403, 403:1–403:21 pages.

[28] Ke Li, Ruidong Zhang, Bo Liang, François Guimbretière, and Cheng Zhang. 2022. EarIO: A Low-power Acoustic Sensing Earable for Continuously Tracking Detailed Facial Movements. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 2, Article 62 (2022), 62:1–62:24 pages.

[29] Rui Liu, Cory Cornelius, Reza Rawassizadeh, Ronald Peterson, and David Kotz. 2018. Vocal Resonance: Using Internal Body Voice for Wearable Authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 1, Article 19 (2018), 23 pages.

[30] Li Lu, Jiadi Yu, Yingying Chen, Hongbo Liu, Yanmin Zhu, Yunfei Liu, and Minglu Li. 2018. LipPass: Lip Reading-based User Authentication on Smartphones Leveraging Acoustic Signals. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. 1466–1474.

[31] Shivangi Mahto, Takayuki Arakawa, and Takafumi Koshinak. 2018. Ear Acoustic Biometrics Using Inaudible Signals and Its Application to Continuous User Authentication. In *2018 26th European Signal Processing Conference (EUSIPCO)*. 1407–1411.

[32] Delina Beh Mei Yin, Mohamad Izzuddin Kamal, Nurul Sharaz Azmanuddin, Siti Haryani Shaikh Ali, Abu Talib Othman, and Rita Zaharah Wan Chik. 2016. Electronic Door Access Control using MyAccess Two-Factor Authentication Scheme featuring Near-Field Communication and Eigenface-based Face Recognition using Principal Component Analysis *(IMCOM '16)*. Association for Computing Machinery, New York, NY, USA, Article 1, 8 pages.

[33] Adiyan Mujibiya, Xiang Cao, Desney S. Tan, Dan Morris, Shwetak N. Patel, and Jun Rekimoto. 2013. The Sound of Touch: On-Body Touch and Gesture Sensing Based on Transdermal Ultrasound Propagation. In *Proceedings of the 2013 ACM International Conference on Interactive Tabletops and Surfaces* (St. Andrews, Scotland, United Kingdom) *(ITS '13)*. Association for Computing Machinery, New York, NY, USA, 189–198.

[34] Arinobu Niijima and Yuki Kubo. 2023. Assisting with Fingertip Force Control by Active Bio-Acoustic Sensing and Electrical Muscle Stimulation. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, Article 743, 743:1–74313 pages.

[35] L. O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 12 (2003), 2021–2040.

[36] Yuya Okawa and Kentaro Takemura. 2015. Haptic-Enabled Active Bone-Conducted Sound Sensing. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology* (Daegu, Kyungpook, Republic of Korea) *(UIST '15 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 87–88.

[37] Makoto Ono, Buntarou Shizuki, and Jiro Tanaka. 2013. Touch & activate: adding interactivity to existing objects using active acoustic sensing. In *Proceedings of the 26th Annual ACM Symposium on User Interface Software and Technology (UIST '13)*. Association for Computing Machinery, New York, NY, USA, 31–40.

[38] Makoto Ono, Buntarou Shizuki, and Jiro Tanaka. 2015. Sensing Touch Force using Active Acoustic Sensing. In *Proceedings of the Ninth International Conference on Tangible, Embedded, and Embodied Interaction* (Stanford, California, USA) *(TEI '15)*. Association for Computing Machinery, 355–358.

[39] N.K. Ratha, R.M. Bolle, V.D. Pandit, and V. Vaish. 2000. Robust fingerprint authentication using local structural similarity. In *Proceedings Fifth IEEE Workshop on Applications of Computer Vision*. 29–34.

[40] Sarah Delgado Rodriguez, Lukas Mecke, and Florian Alt. 2022. SenseHandle: Investigating Human-Door Interaction Behaviour for Authentication in the Physical World. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*. 7–9.

[41] Shogo Sekiguchi, Shingo Kato, Yoshiki Nishikawa, and Buntarou Shizuki. 2024. Authentication Method Using Opening Gestures. In *HCI for Cybersecurity, Privacy and Trust*. Springer Nature Switzerland, 186–203.

[42] Hyejin Shin, Jun Ho Huh, Bum Jun Kwon, Iljoo Kim, Eunyong Cheon, HongMin Kim, Choong-Hoon Lee, and Ian Oakley. 2024. SkullID: Through-Skull Sound Conduction based Authentication for Smartglasses. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*. Association for Computing Machinery, Article 834, 824:1–834:19 pages.

[43] Kamath K.M Shreyas, Srijith Rajeev, Karen Panetta, and Sos S Agaian. 2017. Fingerprint authentication using geometric features. In *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*. 1–7.

[44] Kentaro Takemura, Akihiro Ito, Jun Takamatsu, and Tsukasa Ogasawara. 2011. Active Bone-Conducted Sound Sensing for Wearable Interfaces. In *Proceedings of the*

24th Annual ACM Symposium Adjunct on User Interface Software and Technology (Santa Barbara, California, USA) *(UIST ’11 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 53–54.

[45] Shejin Thavalengal, Petronel Bigioi, and Peter Corcoran. 2015. Iris authentication in handheld devices - considerations for constraint-free acquisition. *IEEE Trans. on Consum. Electron.* 61, 2 (may 2015), 245–253.

[46] Christian Tietz, Eric Klieme, Rachel Brabender, Teresa Lasarow, Lukas Rambold, and Christoph Meinel. 2020. Under Pressure: Pushing Down on Me - Touch Sensitive Door Handle to Identify Users at Room Entry. In *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications - Volume 3: SECRYPT,*. INSTICC, SciTePress, 565–571.

[47] Jesús Vegas, César Llamas, Manuel A. González, and Carmen Hernández. 2021. Identifying users from the interaction with a door handle. *Pervasive and Mobile Computing* 70 (2021), 101293. https://doi.org/10.1016/j.pmcj.2020.101293

[48] Mei Wang and Weihong Deng. 2021. Deep face recognition: A survey. *Neurocomputing* 429 (2021), 215–244.

[49] Zi Wang, Sheng Tan, Linghan Zhang, Yili Ren, Zhi Wang, and Jie Yang. 2021. EarDynamic: An Ear Canal Deformation Based Continuous User Authentication Using In-Ear Wearables. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 1, Article 39 (2021), 39:1–39:27 pages.

[50] Hiroki Watanabe, Hiroaki Kakizawa, and Masanori Sugimoto. 2021. User Authentication Method Using Active Acoustic Sensing. *Journal of Information Processing* 29 (2021), 370–379.

[51] Hiroki Watanabe, Tsutomu Terada, and Masahiko Tsukamoto. 2017. Gesture Recognition Method Utilizing Ultrasonic Active Acoustic Sensing. *Journal of Information Processing* 25 (2017), 331–340.

[52] Yadong Xie, Fan Li, Yue Wu, Huijie Chen, Zhiyuan Zhao, and Yu Wang. 2022. TeethPass: Dental Occlusion-based User Authentication via In-ear Acoustic Sensing. In *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*. 1789–1798.

[53] Tomohiro Yokota and Tomoko Hashida. 2016. Hand Gesture and On-Body Touch Recognition by Active Acoustic Sensing throughout the Human Body. In *Proceedings of the 29th Annual Symposium on User Interface Software and Technology* (Tokyo, Japan) *(UIST ’16 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 113–115.

[54] Jiadi Yu, Li Lu, Yingying Chen, Yanmin Zhu, and Linghe Kong. 2021. An Indirect Eavesdropping Attack of Keystrokes on Touch Screen through Acoustic Sensing. *IEEE Transactions on Mobile Computing* 20, 2 (2021), 337–351.

[55] Cheng Zhang, Qiuyue Xue, Anandghan Waghmare, Ruichen Meng, Sumeet Jain, Yizeng Han, Xinyu Li, Kenneth Cunefare, Thomas Ploetz, Thad Starner, Omer Inan, and Gregory D. Abowd. 2018. FingerPing: Recognizing Fine-Grained Hand Poses Using Active Acoustic On-Body Sensing. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI ’18)*. Association for Computing Machinery, New York, NY, USA, 437:1–437:10.

[56] Ruidong Zhang, Ke Li, Yihong Hao, Yufan Wang, Zhengnan Lai, François Guimbretière, and Cheng Zhang. 2023. EchoSpeech: Continuous Silent Speech Recognition on Minimally-obtrusive Eyewear Powered by Acoustic Sensing. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI ’23)*. Association for Computing Machinery, Article 852, 852:1–852:18 pages.