

ドアノブの握り方に基づくアクティブ音響センシングを用いた個人認証システムの検討

小西 智樹^{1,a)} 崔 明根^{2,3} 雨坂 宇宙^{2,4} 志築 文太郎³

概要：本研究においては、ドアノブの握り方から個人認証を行うシステムを実装した。具体的には、アクティブ音響センシングを用いて取得した、ユーザがドアノブを握る際の周波数特性の違いに基づきユーザを推定する。一般に人によって手の大きさや動作は異なるため、ドアノブの握り方の模倣も困難であると考えられる。本システムの性能を検証するために、10 人の実験参加者からドアノブを握る際の周波数特性のデータを収集した。収集したデータを用いて分類モデルを作成した結果、本システムは高い性能においてドアノブを握る実験参加者を推定できることが明らかになった。

1. はじめに

近年、解錠に物理的な鍵を用いないスマートロックの普及が進んでいる。一般的なスマートロックは、知識ベース (PIN およびパスワード)、所有ベース (スマートフォンおよびカードキー)、または生体ベース (指紋 [1], [2], 声紋 [3], [4], [5], および顔認証 [6], [7]) の認証技術を用いてユーザを認証する [8]。しかし、これらの技術はいくつかの欠点を抱えている。知識ベースの認証技術は攻撃を受けやすく [9], 桁数が多いとユーザにとって使いにくくなる [10], [11]。所有ベースの認証技術はスマートフォンやカードキーを紛失した場合に不正利用されるリスクがある。生体ベースの認証技術は顔写真、音声、および指紋フィルムなどを用いたリプレイ攻撃に対して脆弱である。

本研究においては、ユーザがドアを開けるために鍵を取り出したり、パスワードを入力したりするなどの特別な動作を行わずにドアを解錠することを目的として、行動生体認証 [12] を活用する。行動生体認証は、パソコンやスマートフォンの操作、歩行、およびタイピングなどのユーザの行動における癖や傾向を用いてユーザを認証する技術である。行動生体認証の利点として、他人による模倣が困難であること、およびユーザに明示的な行動を求めないことが挙げられる。行動生体認証の例として、キーストローク [13], [14], [15], マウス動作 [16], [17], タッチまたはスワイプ動作 [18], [19], 歩容 [20], [21], および眼

球運動 [22], [23], [24] などを用いた研究がある。ドアノブに対する行動生体認証に関する研究はいくつか存在するが [25], [26], ドアノブを下ろす動作が必要であり、ショルダーハッキングのリスクが高い。また, Sekiguchi ら [26] はドアを開けるジェスチャをデザインすることにより個人認証を行っているが、ユーザ間においてジェスチャが重複した際の性能については調査されていない。

そこで本研究においては、ドアノブを握る動作のみを用いてユーザを認証するシステムを開発する。本システムは、非可聴域のアクティブ音響センシングを用いて、ドアノブを握る際の周波数特性の違いに基づいてユーザを認証する。アクティブ音響センシングとは、対象となる物体に音響信号を流し、その応答を解析することにより物体の形状、状態、および境界条件の変化を認識する手法である [27]。我々は、アクティブ音響センシングをドアノブに対して適用することにより、ドアノブを握るユーザの認証に利用できると考えた。実験において 10 人のユーザから取得したデータを用いて機械学習モデルを作成し、その性能を評価した。本研究の貢献を以下に示す。

- ドアノブの握り方に基づくアクティブ音響センシングを用いた個人認証システムを実装した。
- 本システムが高い性能においてドアノブを握る実験参加者を分類できることを示した。

2. 関連研究

本研究においては、ドアノブの握り方に基づき個人を認証することを目的としており、そのためにアクティブ音響センシングを用いる。本節においては、ドアノブを用いた個人認証システムおよびアクティブ音響センシングの関連

¹ 筑波大学 情報理工学位プログラム

² 日本学術振興会

³ 筑波大学 システム情報系

⁴ 慶應義塾大学 理工学部

^{a)} konishi@iplab.cs.tsukuba.ac.jp

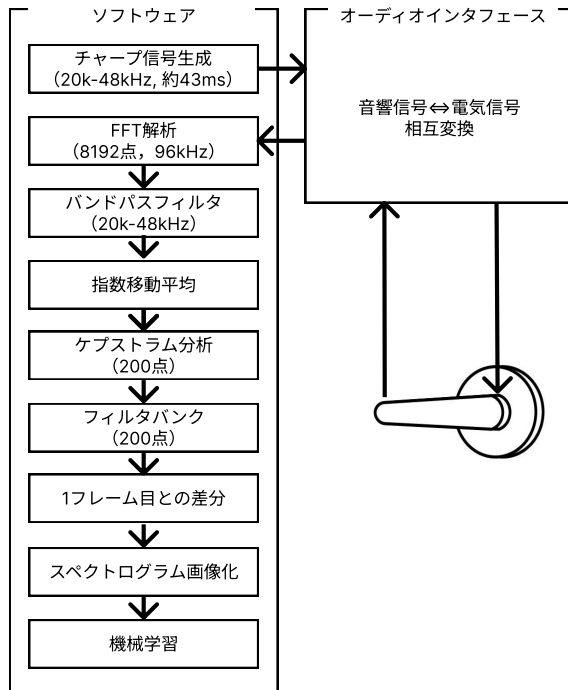


図 1: システム概要図.

研究について概観し、本研究の位置付けを述べる.

2.1 ドアノブを用いた個人認証システム

ドアノブを用いた個人認証システムとして、ドアノブを下げる動作、ドアの開閉動作、およびドアノブを握る手の画像を用いたものがある [25], [26], [28], [29], [30]. SmartHandle [25] は、IMU, ジャイロスコープ, および磁力計を用いてドアを開ける際の手の動きを取得し、ユーザを認証する手法である. SenseHandle [28] は、IMU, 周波数掃引容量センサ, および可聴域の音響センシングを用いてドアの開閉動作からユーザを認証する手法である. Kusanagi ら [29] はドアノブの上に設置したカメラを用いて取得した中手骨指節関節の画像からユーザ認証を行った. Futami ら [30] は、ドアノブに角速度センサを用いて、部屋の入退室動作からユーザを識別した. Sekiguchi ら [26] は、ドアノブに取り付けた静電容量センサ, 圧力センサ, および IMU を用いてユーザがデザインしたドアノブの下げ方を認識し、ユーザ認証を行った.

一方我々はドアノブの握り方のみを用いてユーザを認証する. そのために、ドアノブを握る際の周波数特性の違いを利用する. 本手法は認証の際にドアを開いたりドアノブを下ろしたりする動作が不要であり、また特別なジェスチャを用いないためショルダーハッキングのリスクがない.

2.2 アクティブ音響センシングを用いた個人認証システム

アクティブ音響センシングによって得られる音響信号は、物体の形状, 状態, および組成などによって変化する



図 2: 実験に使用したドアノブ. 左側にマイク, 右側にスピーカを取り付けている.

るため、第三者による模倣が困難である. そのため、個人認証の研究に多く用いられている. アクティブ音響センシングを用いた個人認証システムはウェアラブルデバイスの文脈, 特にイヤホンにおいて多く行われている [31], [32], [33], [34], [35], [36], [37], [38]. Watanabe ら [39] は、スマートウォッチを想定したデバイスに取り付けたマイクおよびスピーカを用いて、9 人の参加者に対して 91.2%の精度においてユーザを識別した. Liu ら [40] は、喉に装着したマイクを用いて人の体内に伝わる声の響きを取得し、29 人の参加者に対して 91.4%の精度においてユーザを識別した. Isobe ら [41], [42] は、スマートグラスの鼻パッドにマイクおよびスピーカを取り付け、装着者を識別した. SkullID [43] は、スマートグラスのつるにマイクおよびスピーカを取り付け、装着者を識別した. Iwakiri ら [44] は、スマートリングを想定したデバイスに取り付けたマイクおよびスピーカを用いて、7 人の参加者に対して 2.7%の等価エラー率においてユーザを識別した. LipPass [45] は、スマートフォンのマイクおよびスピーカを用いてユーザが話す際の唇の動きの違いに基づいて 48 人のユーザを 90.2%の精度において識別した.

我々は、アクティブ音響センシングをドアノブに適用し、ユーザの手の周波数特性の違いおよび握り方に基づく周波数特性の違いを用いてユーザを認証するシステムを実装する.

3. 実装

本研究においては、ドアノブの握り方に基づいて個人認証を行うことを目的とする. そのために、アクティブ音響センシングを用いてドアノブを握る際の周波数特性の違いからユーザを推定するシステムを実装した. 本システムは、ドアノブに取り付けられたスピーカからチャープ信号を出力し、マイクから取得した音響信号をフーリエ変換して周波数特性を取得する. そして、取得した周波数特性を機械学習モデルに入力し、ユーザを推定する. 本節においてはシステムの実装の詳細を述べる.

3.1 ハードウェア

今回用いたドアノブはレバーハンドル式のものである(図 2)。ドアノブに取り付けるマイクおよびスピーカはピエゾ素子(THRIVEK2512BP1, $25 \times 12 \times 0.23$ mm)を用いた。マイクおよびスピーカはドアノブを握る動作の邪魔にならないようにドアノブの両端の側面に取り付けられ、ビニールテープを用いて固定された(図 2)。ピエゾ素子は 2 芯シールド(モガミ電線 超極細フレキシブル 2 芯シールド AWG36)を通してラインプラグ(Pro Audition AS-106)と接続され、オーディオインターフェース(Steinberg UR24C)を通してコンピュータ(OS: Windows 11, CPU: Intel Core i7-1065G7 1.50 GHz, RAM: 32 GB)に接続された。

3.2 ソフトウェア

ソフトウェアはアクティブ音響センシングの先行研究 [27], [46] と同じく、チャープ信号生成部分、フーリエ変換部分、前処理および特徴量抽出部分、ならびに機械学習部分の 4 つから構成されている(図 1)。

3.2.1 チャープ信号生成

チャープ信号生成部分においては 20 k–48 kHz の正弦波線形チャープ信号を生成し、出力している。チャープ信号は約 43 ms の周期において単調増加している。これは、一度のフーリエ変換に対して 2 回分のチャープ信号が含まれる周期である。信号のサンプリングレートは 96 kHz である。

3.2.2 フーリエ変換

マイクから得られた音響信号を周波数データに変換するために高速フーリエ変換(FFT)を行う。FFT は、96 kHz にてサンプリングされた音響信号に対し、8192 点毎に行う。FFT 窓は 50% オーバーラップさせており、約 86 ms 毎に周波数データを取得する。

3.2.3 前処理および特徴量抽出

生の周波数データにはノイズが含まれているため、前処理を行う。得られた周波数データから 20 k–48 kHz の周波数帯域のデータをバンドパスフィルタを用いて抽出し、得られたデータを平滑化係数 1/3 の指数移動平均を用いて時間方向に平滑化する。この時点においてデータは 4779 次元である。次に、周波数データから次元数を削減するために特徴量抽出を行う。ケプストラム分析を用いて先頭から 200 次元のリフタリングを行い、200 点のフィルタバンクを用いて 200 次元の特徴量を抽出する。最後に、握っていない状態の周波数の値を 0 として基準にするために、各データのすべてのフレームから握っていない状態である 1 フレーム目値の差分を取る。

次に、収集したデータから握る動作が行われている部分のみを抽出するために時間方向の切り出しを行う。図 3 に示すように、周波数特性の値は、握り始めた瞬間に小さく

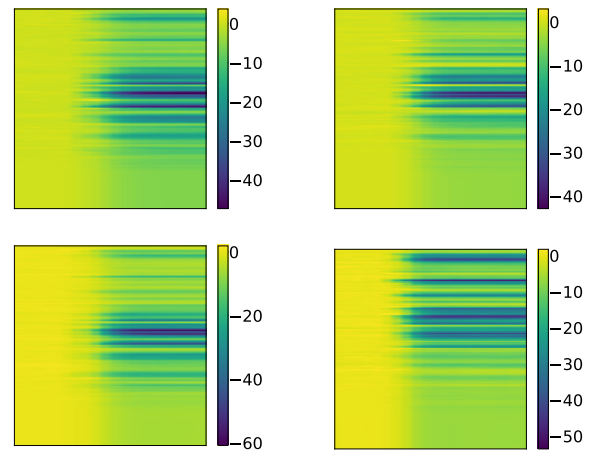


図 3: ドアノブを握った際のスペクトログラムの例。横軸が時間、縦軸が周波数である。色によって値の大きさが表されている。左上: ユーザ A, 右上: ユーザ D, 左下: ユーザ G, 右下: ユーザ J。

なり、静止状態においては一定の値を取る。そのため、周波数特性の値の平均において、その時間方向の差分の絶対値が閾値を上回り、かつ時間方向の差分が負の値を取るフレームを、握り始めた瞬間として定義する。閾値は、時間方向の差分の標準偏差とした。このようにして得られた握り始めた瞬間のフレームの 5 フレーム前から 20 フレーム分を切り出す。

以上の処理によって得られた特徴量を Python の Matplotlib を用いて 224×224 のスペクトログラムに変換(図 3)した。スペクトログラムの色は周波数特性の値に対応している。値から色への変換には matplotlib の標準カラーマップである viridis を用いた。このようにして得られた画像を機械学習モデルへの入力とする。

3.2.4 機械学習

本研究は、いくつかの音響センシングの先行研究 [47], [48], [49], [50] と同じく、畳み込みニューラルネットワーク(CNN)を用いた機械学習を行った。機械学習は、10 クラス分類およびユーザ認証性能を調査するための 10 クラス分の One-vs-Rest を行った。周波数データをスペクトログラム画像に変換することにより、画像認識の分野において用いられている様々なモデルを適用することができる。機械学習は Python の Keras を用いて実装した。

4. 実験

本手法の機械学習モデル作成およびその推定精度の評価を行うためにデータ収集を行った。実験参加者は研究室内の 21–23 歳(平均 22.3 歳)の学生 10 人(男性 9 人, 女性 1 人)であった。

4.1 実験手順

各実験参加者は、ドアの前に立ち、ドアノブを握ってか

表 1: 10 クラス分類におけるモデル比較結果.

model	F1
DenseNet121	0.918
EfficientNetB0	0.018
EfficientNetV2B2	0.070
Inception v2	0.877
Inception v3	0.849
MobileNet	0.912
MobileNet v2	0.937
NasNet	0.847
ResNet50	0.503
ResNet v2	0.874
VGG16	0.929
VGG19	0.868
Xception	0.885

ら離す動作を合計 100 回行った。実験開始前に、実験参加者に対して本実験が個人認証を目的としたシステムのデータ収集の実験であることを説明した。次に、できるだけ同じ握り方および強さによってドアノブを握るように指示した。実験開始時、実験参加者には床に貼られたテープを目印にドアと常に一定の距離を保ち、右手にマウスを持ってもらった。次に、実験参加者には、マウスをクリックした後に左手を用いてドアノブを握り、静止してもらい、マウスクリックから 3 秒後に口頭による指示によってドアノブを離してもらった。一度ドアノブを握ってから離すまでの試行を計 20 回繰り返すことを 1 セッションとし、合計 5 セッションを行った。セッション間には最低 1 分間の休憩を取ってもらった。

データ収集はマウスクリックから 3 秒間行い、ドアノブを握ってから離す動作ごとに 35 フレームのデータを取得した。実験全体において、合計 35,000 (= 20 回 × 5 セッション × 10 人) 個のデータを取得した。

4.2 実験結果

本システムの性能を評価するために、10 人の実験参加者から取得したデータを用いて機械学習モデルを作成した。データのうち、前半の 4 セッション分 (800 個) を学習データ、後半の 1 セッション分 (200 個) をテストデータとした。

まず、モデルを決定するために複数のモデルを用いて 10 クラス分類を行い、性能を比較した。使用したモデルは表 1 に示すものであり、全てのモデルに対してノード数 10 の全結合層を追加した。また、活性化関数として softmax 関数を用い、損失関数として categorical crossentropy を用いた。全てのモデルに対して学習率は 0.0001、バッチサイズは 32、エポック数は 50 とした。結果、最も F1 値が高かったモデルは MobileNet v2 であり、値は 0.937 であった。以降本システムにおいて MobileNet v2 を使用する。

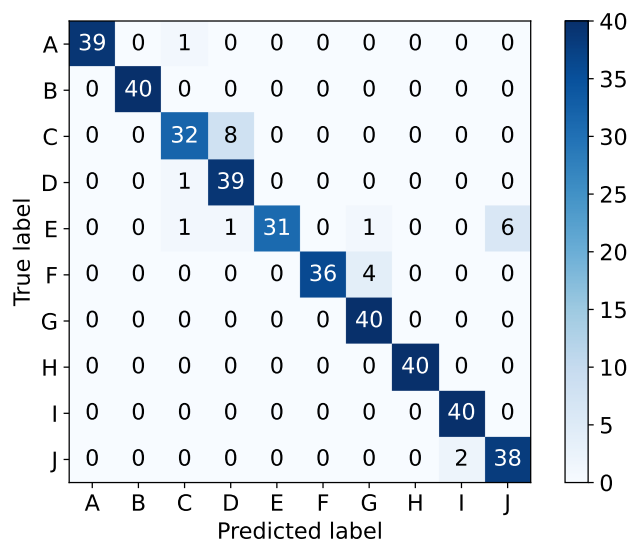


図 4: 10 クラス分類を行った結果の混同行列.

表 2: One-vs-Rest における EER.

ユーザ	A	B	C	D	E
EER	0.044	0.000	0.133	0.028	0.014
ユーザ	F	G	H	I	J
EER	0.006	0.028	0.000	0.003	0.028

最も精度が高かったモデルである MobileNet v2 を用いて 10 クラス分類および One-vs-Rest のそれぞれのモデルを作成し、性能を評価した。結果を図 4 および表 2 に示す。One-vs-Rest においては、活性化関数として sigmoid 関数を用い、損失関数として各クラスの binary crossentropy の平均を用いた。10 クラス分類における精度の平均は 93.8%, FAR (他人受入率) の平均は 0.694%, および FRR (本人棄却率) の平均は 6.25% であった。また、One-vs-Rest における精度の平均は 94.2%, EER (等価エラー率) の平均は 2.83% であった。

5. 議論

実験において、10 人のユーザに対する本システムの性能を調査した。この結果を受け、本研究の議論および今後の課題を述べる。

5.1 認証性能

4.2 節の結果より、本手法がドアノブを握る動作のみを用いて 0.694% の FAR においてユーザ推定が可能であることが明らかになった。この結果を先行研究である SmartHandle [25] と比較する。SmartHandle [25] はドアノブを下ろす動作を加速度センサ、地磁気センサ、およびジャイロスコープの 3 つから取得し、個人認証を行っている。一方、本研究においてはドアノブを握る動作のみを用いている。本手法の 0.694% の FAR は、SmartHandle [25]

の 0.59% の FAR にわずかに劣るものの、本手法はショルダーハッキングの心配がない。また、周波数特性にはドアノブの握り方だけでなくユーザの手表面の音響特性による生体情報も含まれるため先行研究よりも堅牢な手法であると考えられる。

5.2 セキュリティへの活用

本手法を実際にセキュリティ技術として使用するためには本手法の精度を更に改善する必要がある。図 4 および図 2 のユーザ C に見られるようにユーザにより精度にばらつきがある。これは、本実験において収集したデータに周波数特性が似ているユーザが存在しているためであると考えられる。Watanabe ら [39] の研究において、ピエゾ素子を皮膚に対してより密着させた状態の方が個人認証の精度が優れていることが示されている。これは、デバイスと皮膚の接触面積が大きくなるからであると考えられており、本実験においてもドアノブをしっかりと握るよう指示を行いデータを収集することにより精度が向上する可能性がある。

また、本手法はピエゾ素子をドアノブに貼り付けた状態においてデータ収集を行っているが、実際の使用場面においてはピエゾ素子をドアノブ内部に埋め込む、もしくはドアノブカバーの裏側に貼るなどの必要がある。この場合、ドアノブもしくはドアノブカバーの材質が機械学習の精度に大きく関わると考えられるため、調査が必要である。

6. 制限および今後の展望

本節においては、本手法の制限および今後の展望を述べる。

6.1 攻撃者に対するセキュリティ実験

アクティブ音響センシングを用いた認証方法は、ユーザの周波数特性のデータが攻撃者に知られた場合にスピーカを用いたリプレイ攻撃が行われる可能性がある。そのため、先行研究 [36], [43] と同じくリプレイ攻撃に対する本システムのセキュリティ性能を調査する必要があると考えられる。

6.2 期間が空いた場合の性能

実験において、同一の参加者のデータの収集は同じ日に行われたが、人間の体の構成成分は時間とともに変化し、それが本手法の性能の低下を引き起こす可能性がある [39]。先行研究 [32], [39] においては数ヶ月後にデータ収集を行い、システムの性能を調査していたが、本研究においても同じく期間が空いた場合の性能を調査する必要がある。

6.3 様々な環境における性能

先行研究 [41], [42] において、マイクおよびスピーカが

触れる部分の皮膚が湿っていた際に認証性能が低下することが示されている。本研究においても手の乾燥状態の違いに対する認証性能を調査する必要があると考えられる。

また、本研究においては 1 種類のレバーハンドルのみを用いているが、様々な形および材質のドアノブにおいて本手法が適用可能かを調査する必要があると考えられる。

7. おわりに

本研究は、ユーザがドアを開けるために鍵を取り出した後、パスワードを入力したりするなどの特別な動作を行わずにドアを解錠することを目的としている。そのために、我々はアクティブ音響センシングをドアノブに対して適用し、ドアノブの握り方に基づき個人を認証するシステムを実装した。本システムの性能を検証するために 10 人の実験参加者からドアノブを握る際の周波数特性のデータを収集した。収集したデータを用いて分類モデルを作成した結果、10 クラス分類において精度が 93.8%, FAR が 0.694%, および FRR が 6.25% であった。また、One-vs-Rest において精度が 94.2%, EER が 2.83% であった。

今後は、実験参加者の数を増やし、様々な環境における実験を行うことによって本手法の有効性を検証する。また、リプレイ攻撃に対するセキュリティ実験を行うことにより、本手法の認証性能の堅牢性を検証する。

参考文献

- [1] Ratha, N., Bolle, R., Pandit, V. and Vaish, V.: Robust fingerprint authentication using local structural similarity, *Proceedings Fifth IEEE Workshop on Applications of Computer Vision*, pp. 29–34 (2000).
- [2] Shreyas, K. K., Rajeev, S., Panetta, K. and Agaian, S. S.: Fingerprint authentication using geometric features, *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1–7 (2017).
- [3] Heigold, G., Moreno, I., Bengio, S. and Shazeer, N.: End-to-end text-dependent speaker verification, *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE Press, pp. 5115–5119 (2016).
- [4] Jayamaha, R. G. M. M., Senadheera, M. R. R., Gamage, T. N. C., Weerasekara, K. D. P. B., Dissanayaka, G. A. and Kodagoda, G. N.: VoizLock - Human Voice Authentication System using Hidden Markov Model, *2008 4th International Conference on Information and Automation for Sustainability*, pp. 330–335 (2008).
- [5] De Leon, P. L., Pucher, M., Yamagishi, J., Hernaez, I. and Saratzaga, I.: Evaluation of Speaker Verification Security and Detection of HMM-Based Synthetic Speech, *IEEE Transactions on Audio, Speech, and Language Processing*, Vol. 20, No. 8, pp. 2280–2290 (2012).
- [6] Song, I., Kim, H.-J. and Jeon, P. B.: Deep learning for real-time robust facial expression recognition on a smartphone, *2014 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 564–567 (2014).
- [7] Wang, M. and Deng, W.: Deep face recognition: A survey, *Neurocomputing*, Vol. 429, pp. 215–244 (2021).
- [8] O’Gorman, L.: Comparing passwords, tokens, and

- biometrics for user authentication, *Proceedings of the IEEE*, Vol. 91, No. 12, pp. 2021–2040 (2003).
- [9] Yu, J., Lu, L., Chen, Y., Zhu, Y. and Kong, L.: An Indirect Eavesdropping Attack of Keystrokes on Touch Screen through Acoustic Sensing, *IEEE Transactions on Mobile Computing*, Vol. 20, No. 2, pp. 337–351 (2021).
 - [10] Gupta, S., Buriro, A. and Crispo, B.: Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access, *Mobile Information Systems*, Vol. 2018, No. 1, pp. 2649598:1–2649598:16 (2018).
 - [11] Adams, A. and Sasse, M. A.: Users are not the enemy, *Communication of the ACM*, Vol. 42, No. 12, pp. 40–46 (1999).
 - [12] Liebers, J., Gruenefeld, U., Buschek, D., Alt, F. and Schneegass, S.: Introduction to Authentication using Behavioral Biometrics, *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, New York, NY, USA, Association for Computing Machinery (2023).
 - [13] Saini, B. S., Singh, P., Nayyar, A., Kaur, N., Bhatia, K. S., El-Sappagh, S. and Hu, J.-W.: A Three-Step Authentication Model for Mobile Phone User Using Keystroke Dynamics, *IEEE Access*, Vol. 8, pp. 125909–125922 (2020).
 - [14] Krishnamoorthy, S., Rueda, L., Saad, S. and Elmiligi, H.: Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning, *Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications*, ICBEA '18, Association for Computing Machinery, pp. 50–57 (2018).
 - [15] Zamsheva, M., Deutschmann, I., Julitz, D. and Bienenert, A.: Person Authentication with BehaviorSense using Keystroke Biometrics, *Proceedings of the 2020 International Conference on Pattern Recognition and Intelligent Systems*, PRIS '20, Association for Computing Machinery (2020).
 - [16] Jorgensen, Z. and Yu, T.: On mouse dynamics as a behavioral biometric for authentication, *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, Association for Computing Machinery, pp. 476–482 (2011).
 - [17] Pusara, M. and Brodley, C. E.: User re-authentication via mouse movements, *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, VizSEC/DMSEC '04, Association for Computing Machinery, pp. 1–8 (2004).
 - [18] Abbas, G., Humayoun, S. R., AlTarawneh, R. and Ebert, A.: Simple shape-based touch behavioral biometrics authentication for smart mobiles, *Proceedings of the 2018 International Conference on Advanced Visual Interfaces*, AVI '18, pp. 50:1–50:3 (2018).
 - [19] Holz, C. and Knaust, M.: Biometric Touch Sensing: Seamlessly Augmenting Each Touch with Continuous Authentication, *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*, UIST '15, Association for Computing Machinery, pp. 303–312 (2015).
 - [20] Muaaz, M. and Mayrhofer, R.: An Analysis of Different Approaches to Gait Recognition Using Cell Phone Based Accelerometers, *Proceedings of International Conference on Advances in Mobile Computing and Multimedia*, MoMM '13, Association for Computing Machinery, pp. 293–300 (2013).
 - [21] Muaaz, M. and Mayrhofer, R.: Orientation Independent Cell Phone Based Gait Authentication, *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia*, MoMM '14, Association for Computing Machinery, pp. 161–164 (2014).
 - [22] Kinnunen, T., Sedlak, F. and Bednarik, R.: Towards task-independent person authentication using eye movement signals, *Proceedings of the 2010 Symposium on Eye-Tracking Research & Applications*, ETRA '10, Association for Computing Machinery, pp. 187–190 (2010).
 - [23] Sluganovic, I., Roeschlin, M., Rasmussen, K. B. and Martinovic, I.: Using Reflexive Eye Movements for Fast Challenge-Response Authentication, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, Association for Computing Machinery, pp. 1056–1067 (2016).
 - [24] Zhang, Y., Hu, W., Xu, W., Chou, C. T. and Hu, J.: Continuous Authentication Using Eye Movement Response of Implicit Visual Stimuli (2018).
 - [25] Gupta, S., Buriro, A. and Crispo, B.: SmartHandle: A Novel Behavioral Biometric-based Authentication Scheme for Smart Lock Systems, *Proceedings of the 2019 3rd International Conference on Biometric Engineering and Applications*, ICBEA 2019, Association for Computing Machinery, pp. 15–22 (2019).
 - [26] Sekiguchi, S., Kato, S., Nishikawa, Y. and Shizuki, B.: Authentication Method Using Opening Gestures, *HCI for Cybersecurity, Privacy and Trust*, Springer Nature Switzerland, pp. 186–203 (2024).
 - [27] Ono, M., Shizuki, B. and Tanaka, J.: Touch & activate: adding interactivity to existing objects using active acoustic sensing, *Proceedings of the 26th Annual ACM Symposium on User Interface Software and Technology*, UIST '13, New York, NY, USA, Association for Computing Machinery, pp. 31–40 (2013).
 - [28] Rodriguez, S. D., Mecke, L. and Alt, F.: SenseHandle: Investigating Human-Door Interaction Behaviour for Authentication in the Physical World, *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pp. 7–9 (2022).
 - [29] Daichi, K., Shoichiro, A., Koichi, I. and Takafumi, A.: A practical person authentication system using second minor finger knuckles for door security, *IPSJ Transactions on Computer Vision and Applications*, Vol. 9, No. 8 (2017).
 - [30] Futami, K., Fukao, A. and Murao, K.: A method to recognize entering and leaving person based on door opening and closing movement using angular velocity sensor, *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, pp. 57–60 (2019).
 - [31] Gao, Y., Jin, Y., Chauhan, J., Choi, S., Li, J. and Jin, Z.: Voice In Ear: Spoofing-Resistant and Passphrase-Independent Body Sound Authentication, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 5, No. 1 (2021).
 - [32] Gao, Y., Wang, W., Phoha, V. V., Sun, W. and Jin, Z.: EarEcho: Using Ear Canal Echo for Wearable Authentication, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 3, No. 3 (2019).
 - [33] Wang, Z., Tan, S., Zhang, L., Ren, Y., Wang, Z. and Yang, J.: EarDynamic: An Ear Canal Deformation Based Continuous User Authentication Using In-Ear Wearables, *Proceedings of the ACM on Interactive,*

- Mobile, Wearable and Ubiquitous Technologies*, Vol. 5, No. 1 (2021).
- [34] Irwansyah, Otsuka, S. and Nakagawa, S.: Evaluation of Bone-Conducted Cross-Talk Sound in the Head for Biometric Identification, *Proceedings of the 2021 International Conference on Computer, Control, Informatics and Its Applications*, IC3INA '21, Association for Computing Machinery, pp. 76–80 (2022).
 - [35] Mahto, S., Arakawa, T. and Koshinak, T.: Ear Acoustic Biometrics Using Inaudible Signals and Its Application to Continuous User Authentication, *2018 26th European Signal Processing Conference (EUSIPCO)*, pp. 1407–1411 (2018).
 - [36] Xie, Y., Li, F., Wu, Y., Chen, H., Zhao, Z. and Wang, Y.: TeethPass: Dental Occlusion-based User Authentication via In-ear Acoustic Sensing, *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, pp. 1789–1798 (2022).
 - [37] Amesaka, T., Watanabe, H., Sugimoto, M., Sugiura, Y. and Shizuki, B.: User Authentication Method for Hearables Using Sound Leakage Signals, *Proceedings of the 2023 ACM International Symposium on Wearable Computers*, ISWC '23, Association for Computing Machinery, pp. 119–123 (2023).
 - [38] Arakawa, T., Koshinaka, T., Yano, S., Irisawa, H., Miyahara, R. and Imaoka, H.: Fast and accurate personal authentication using ear acoustics, *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, pp. 1–4 (2016).
 - [39] Watanabe, H., Kakizawa, H. and Sugimoto, M.: User Authentication Method Using Active Acoustic Sensing, *Journal of Information Processing*, Vol. 29, pp. 370–379 (2021).
 - [40] Liu, R., Cornelius, C., Rawassizadeh, R., Peterson, R. and Kotz, D.: Vocal Resonance: Using Internal Body Voice for Wearable Authentication, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 2, No. 1, pp. 19:1–19:23 (2018).
 - [41] Isobe, K. and Murao, K.: Person-identification Method using Active Acoustic Sensing Applied to Nose, *Proceedings of the 2021 ACM International Symposium on Wearable Computers*, ISWC '21, Association for Computing Machinery, pp. 138–140.
 - [42] Isobe, K. and Murao, K.: Personal Identification Method using Active Acoustic Sensing applied to the Nose pad of Eyeglasses, *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, pp. 345–348 (2023).
 - [43] Shin, H., Huh, J. H., Kwon, B. J., Kim, I., Cheon, E., Kim, H., Lee, C.-H. and Oakley, I.: SkullID: Through-Skull Sound Conduction based Authentication for Smartglasses, *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '24, Association for Computing Machinery, pp. 824:1–834:19 (2024).
 - [44] Iwakiri, S. and Murao, K.: User Authentication Method for Wearable Ring Devices using Active Acoustic Sensing, *Proceedings of the 2023 ACM International Symposium on Wearable Computers*, ISWC '23, Association for Computing Machinery, pp. 17–21 (2023).
 - [45] Lu, L., Yu, J., Chen, Y., Liu, H., Zhu, Y., Liu, Y. and Li, M.: LipPass: Lip Reading-based User Authentication on Smartphones Leveraging Acoustic Signals, *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, pp. 1466–1474 (2018).
 - [46] Kubo, Y., Koguchi, Y., Shizuki, B., Takahashi, S. and Hilliges, O.: AudioTouch: Minimally Invasive Sensing of Micro-Gestures via Active Bio-Acoustic Sensing, *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '19, Association for Computing Machinery, pp. 36:1–36:13 (2019).
 - [47] Kim, J. and Oakley, I.: SonarID: Using Sonar to Identify Fingers on a Smartwatch, *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, Association for Computing Machinery, pp. 287:1–287:10 (2022).
 - [48] Zhang, R., Li, K., Hao, Y., Wang, Y., Lai, Z., Guimbretière, F. and Zhang, C.: EchoSpeech: Continuous Silent Speech Recognition on Minimally-obtrusive Eyewear Powered by Acoustic Sensing, *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, Association for Computing Machinery, pp. 852:1–852:18 (2023).
 - [49] Lee, C.-J., Zhang, R., Agarwal, D., Yu, T. C., Gunda, V., Lopez, O., Kim, J., Yin, S., Dong, B., Li, K., Sakashita, M., Guimbretiere, F. and Zhang, C.: EchoWrist: Continuous Hand Pose Tracking and Hand-Object Interaction Recognition Using Low-Power Active Acoustic Sensing On a Wristband, *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, Association for Computing Machinery, pp. 403:1–403:21 (2024).
 - [50] Li, K., Zhang, R., Liang, B., Guimbretière, F. and Zhang, C.: EarIO: A Low-power Acoustic Sensing Earable for Continuously Tracking Detailed Facial Movements, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 6, No. 2 (2022).