ドアノブの開扉ジェスチャを用いた個人認証システムの提案

関口 将護 * 加藤 進吾 * 志築 文太郎 †

概要. 我々は，ドアノブを捻る動作（開扉ジェスチャ）によって個人認証を行うシステムを実装した．本システムは，スマートロックを対象とした行動生体認証に基づく個人認証システムであり，ユーザがドアノブを捻る際の手の動きを利用する．具体的には，静電容量方式センサ，圧力センサ，加速度センサ，ジャイロセンサおよび地磁気センサから得られるデータに基づいてユーザを認証する署名を生成する．本システムは，解錠のために物理鍵およびパスワードを必要としない．そのため，顔および指紋を利用した生体認証に比べ，プライバシの危険性も少ない．本システムを実現するため，10 名の実験参加者がデザインした開扉ジェスチャの動きを計測したデータを用いて，認証を行った．その結果，平均適合率 0.834，平均偽陽性率 0.014 の認証精度を得た．

1 はじめに

スマートロックは，デジタルキーパッド，バイオメトリクスセンサ，スマートカードリーダおよびモバイル端末によって操作可能であり，ドアのセキュリティを向上させている．しかし，スマートロックに利用されている知識ベース（PIN およびパスワード）および生体ベース（指紋および顔）の認証はいくつかの欠点を抱えている．知識ベースの認証方式では，入力中にショルダーハックを受けやすいほか，桁数が長いと覚えにくいなどの欠点がある [2]．生体ベースの認証方式では，指紋および顔の認証に利用するデータが複製され，悪用される可能性がある．そのためユーザは，自身のプライバシへの懸念から，生体ベースの認証方式の使用を躊躇う可能性がある [7]．これらの理由から知識ベースおよび生体ベースの認証方式は，様々な攻撃に対して脆弱であるため，使い勝手が悪いという研究結果がある [2, 4]．

そこで本研究では，開扉ジェスチャを利用した個人認証システムを提案する．本システムでは，ユーザが任意に決定した開扉ジェスチャを利用し，その行動特徴を基に認証が行われる．この行動特徴は，知識ベースのような複雑なパスワードの生成が不要で，かつ直接的な生体情報でないためデータの複製によるプライバシの危険性が低い．これを実現するため，実験参加者に開扉ジェスチャをデザインしてもらい，デザインされた開扉ジェスチャの分析を行った．また，実際に認証を行い，分析結果を基に認証結果に対する考察を行った．本研究の貢献を以下に示す．

- 模倣ジェスチャへの耐性：類似の開扉ジェスチャにおいても，ユーザ間に有意差があることを実験により示した．
- 利用するジェスチャの汎用性：開扉ジェスチャの複雑さに関わらず，ほぼ同精度にて識別できることを示した．

2 関連研究

本システムは，ドアの開扉ジェスチャを用いた個人認証システムである．そこで，ドアの開扉ジェスチャおよびこれに類似した動作を用いた，個人認証および入退出管理技術に対する，本研究との位置付けを示す．

Gupta ら [3] は，ドアノブに慣性計測装置（IMU）を取り付け，開扉する際の手の動きの軌跡およびその速度から，個人認証を試みた．Rodriguez ら [5] は，IMU に加えて，掃引型静電容量方式センサおよび音響センサを取り付け，開扉する際のセンサの値から個人認証を試みた．Futami ら [1] は，ドアノブに角速度センサを取り付け，ドアノブの支柱を軸とした回転およびドア本体の支柱を軸とした回転から，個人識別を試みた．本研究の個人認証システムも，ドアノブにセンサを設置し，かつドアノブの動きを認証に利用するため，これらの研究を参考にシステムを構築する．一方で，本研究では IMU および静電容量方式センサだけでなく圧力センサを加えた 3 つのセンサを利用して認証を行う．また，認証に用いる区間にドア本体の動きを含まず，ドアノブの動きのみを切り取ることで，引き戸または押し戸に関わらず，認証を行うことができる．

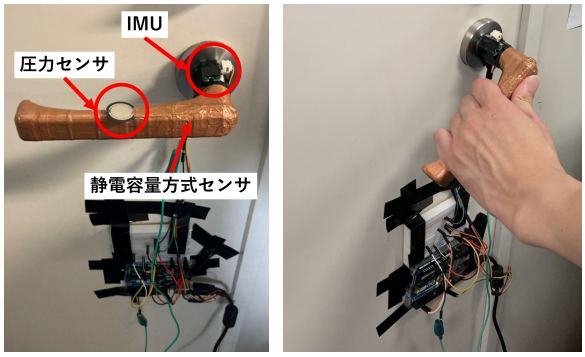
3 提案手法による実験

本節では，提案手法の実装に用いたデバイス，データ収集のための実験手順および機械学習による認証結果を述べる．

* 筑波大学 情報理工学位プログラム
† 筑波大学 システム情報系

3.1 デバイス

ドアノブは，ハンドル部分の幅が 13.5cm，径が 1-2cm，軸部分の径が 2cm，床から軸中心部までの高さが 100cm であり，左開きのものを利用した．開扉ジェスチャの動きの計測には，静電容量方式センサ，圧力センサおよび IMU を利用した（図 1a）．静電容量センサには，ドアノブに対し銅テープを巻き付けたものを利用した．そこに 1 MΩ の抵抗器を接続させることでドアノブ表面をセンサとして利用した．また放電のため，受信側に 1 kΩ の抵抗器を並列に接続した．利用したドアは，導電性を持ち，磁気を帯びていた．ドアノブ部分は非導電性かつ非磁性であったが，ドア本体からの影響を考え，銅テープを巻き付ける前に，絶縁テープを巻きつけた．圧力センサには，Alpha の MF01A-N-221-A04 を利用し，ドアノブのハンドル部分の頂部中央に設置した．IMU には，秋月電子通商の AE-LSM9DS1-I2C を利用し，ドアノブの軸部分の頂部中央に設置した．各センサの受信には，Arduino Uno R3 を利用した．



(a) 実験装置の外観．　**(b)** ジェスチャの実演の例．

図 1: 実験装置によるジェスチャの動きの計測．

3.2 データ収集のための実験手順

著者らと同じ研究室に所属する，21 歳以上 28 歳以下（M=23.3 歳，SD=2.06）の大学生および大学院生 10 名（P1–P10）がボランティアとして参加した．すべての参加者は男性，利き手は 9 名が右利き，1 名が両利きであると回答した．参加者は，「本研究のシナリオの認証のために，実生活で使いたいジェスチャをデザインしてください」という指示のもと，開扉ジェスチャのデザインを行った．また，デザインしたジェスチャ1 種類ごとに，20 回の開扉ジェスチャを実演した（図 1b）．その結果，参加者は親指をドアノブの軸に触れさせるもの（G1），握力に強弱をつけるもの（G2），ドアノブに 2 回触れるもの（G5，G9），触れる指に順番をつけたもの（G7），逆手でドアノブに触れるもの（G8）および特徴のないもの (G3，G4，G6，G10) をデザインした．

3.3 機械学習による認証結果

岡田らの研究 [6] を参考に，センサを用いて計測した 11 種類（静電容量方式センサ，圧力センサ，3 軸加速度センサ，3 軸ジャイロセンサ，3 軸磁気センサ）のデータから，平均，分散，標準偏差，尖度および歪度の 5 種の特徴量にジェスチャの長さを加えた，合計 56 次元（=11×5+1）の特徴量ベクトルを得た．このデータを用いて，Random Forest による 10 分割交差検証を行った結果を，表 1 に示す．この結果は，認証に利用することを想定しているため，1 対多数の分類である One-vs-Rest を用いた．また，平均正答率は約 0.956 であった．表 1 より，特徴のない類似のジェスチャ（G3，G4，G6，G10）も適合率 0.94 以上で分類ができること，複雑なジェスチャ（G1，G2-2，G5）および単純なジェスチャ（G3，G4，G6，G10）がほぼ同精度で分類ができることが分かった．一方で，著しく精度の悪いジェスチャもあることが分かった（G2-1，G7，G8）．

4 まとめと今後の予定

本研究では，行動生体認証に基づく開扉ジェスチャを用いた個人認証システムの手法を提案した．現在までに，参加者がデザインする開扉ジェスチャの動きの計測実験を行った．開扉ジェスチャの動きの計測は，静電容量方式センサ，圧力センサおよび IMU を利用した．認証実験の結果，平均して再現率 0.834，偽陽性率 0.014 の認証精度を得た．また，特徴のない類似のジェスチャ（G3，G4，G6，G10）も適合率 0.94 以上で分類ができること，複雑なジェスチャ（G1，G2-2，G5）および単純なジェスチャ（G3，G4，G6，G10）がほぼ同精度で分類ができることが分かった．

今後は，精度の悪いジェスチャの分析およびジェスチャの再現性の検証を行うことで，本研究が提案する認証システムの実現を目指す．

表 1: One-vs-Rest による参加者別の認証精度評価．ジェスチャG1 は P1 のデザインしたジェスチャを示す．ただし，P2 は 2 つのジェスチャをデザインしたため，G2-1 および G2-2 とした．

ジェスチャ	G1	G2-1	G2-2	G3	G4	G5	G6	G7	G8	G9	G10	平均
適合率	1.000	0.481	1.000	1.000	1.000	1.000	0.947	0.357	0.571	0.818	1.000	0.834
F 値	0.857	0.553	0.963	1.000	0.889	0.947	0.923	0.294	0.296	0.581	0.824	0.739
偽陽性率	0.000	0.072	0.000	0.000	0.000	0.000	0.005	0.046	0.015	0.010	0.000	0.014

参考文献

[1] K. Futami, A. Fukao, and K. Murao. A method to recognize entering and leaving person based on door opening and closing movement using angular velocity sensor. UbiComp/ISWC '19 Adjunct, pp. 57–60. Association for Computing Machinery, 2019.

[2] S. Gupta, A. Buriro, and B. Crispo. Demystifying authentication concepts in smartphones: Ways and types to secure access. *Mobile Information Systems*, 2018:2649598:1–2649598:16, 2018.

[3] S. Gupta, A. Buriro, and B. Crispo. 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, pp. 15–22. Association for Computing Machinery, 2019.

[4] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner. Smart Locks: Lessons for securing commodity internet of things devices. ASIA CCS '16, pp. 461–472. Association for Computing Machinery, 2016.

[5] S. D. Rodriguez, L. Mecke, and F. Alt. SenseHandle: Investigating human-door interaction behaviour for authentication in the physical world. SOUPS 2022. USENIX Symposium on Usable Privacy and Security, 2022.

[6] 岡田 一志, 大井 翔, 松村 耕平, 野間 春生. ペングリップ型デバイスを用いた個人認証の提案. 情報処理学会 インタラクション 2019 論文集, pp. 641–643, 2019.

[7] 中西 功. バイオメトリクスのモダリティに関する課題と将来展望. 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, 16(3):185–195, 2023.