行動センシングにおける意図的改ざん対策のための センシングデバイス装着位置識別・装着者認証

鈴木 達[1,a)]　王 卓立[2,b)]　雨坂 宇宙[3,c)]　杉浦 裕太[1,d)]

概要：近年ウェアラブルセンサを用いた行動センシングは，日常動作やスポーツパフォーマンスの記録などを中心に様々な応用が期待されている．我々は行動証明への利用という目標を設定しており，そのためには高い識別性能と，データ取得の過程で不正がないことを保証する仕組みが求められる．本研究ではセンシング過程においてユーザが装着位置や装着者を改ざんすることを不可能にするため，ウェアラブルセンサの装着位置識別と使用中におけるユーザ認証を目的としている．本研究ではそれぞれのタスクに対して深層学習モデルを構築し，その有効性を検証した．装着位置識別モデルでは全クラスで F1 スコア 0.90 以上を達成した．また装着者認証モデルでは 2-fold 交差検証をランダムに 5 回実行し，等価エラー率 3.6% を実現した．さらに未知の他人が本人をなりすますような動作をしたときの検証を実施し，なりすまし攻撃に対する耐性を調査した．本提案手法は行動証明システムにおける改ざんの困難性の確保に対して貢献するものである．

1. 序章

近年, ウェアラブルデバイスの普及により行動データの取得が容易になり, 動作再構成の研究も進んでいる [1], [2], [3]. これらのデータは健康管理やリハビリに加え，社会的証明への活用も期待される． 我々は特に「行動証明」への活用に着目する．これは特定のユーザがある行動を確かに行ったこと，あるいは行わなかったことを客観的に示すものであり，活動履歴を保証する場面で重要な役割を果たす．

具体的な利用場面として，運動習慣による保険料優遇など，活動実績に対しインセンティブを与えるサービスが挙げられる [4], [5], [6]．こうしたサービスでは，他人のデータ利用や装着位置の偽装といった不正リスクが考えられる．これに対し，装着位置・装着者認証を導入することで不正を検知し，不当なインセンティブ受給を阻止できる．

行動証明には動作識別の高精度化とデータの改ざん防止という 2 つの要件が求められる．改ざんのリスクは，(1) キャリブレーション時の意図的な不正，(2) 利用時の装着位置ずらしや認証後の使用者交代，(3) 出力データの改変，の 3 点に大別される．(1) は第三者監視下の運用，(3) はセキュリティ技術で対策可能であるため，本研究では (2) の利用時に生じる「他者利用」や「誤装着」への対策に焦点を当てる． 本研究では基盤技術としてウェアラブルセンサからの IMU データを用いた装着者認証および装着位置識別の実現を目指す．システムの利用シナリオとしては第三者立会いの下で取得したデータを基に学習を行う．その後，図 1 の通り，行動・装着者・位置情報を紐付けて出力することで改ざん困難性を保証する．本研究では装着位置識別と装着者認証の 2 つのタスクに対しそれぞれ認証モデルを構築した．Transformer を用いた装着位置識別では未知のデータに対して，全クラスで F1 スコア 0.90 以上と高い性能を，CNN を用いた装着者認証では等価エラー率 3.6%を実現した．また未知の人物からのなりすましデータ

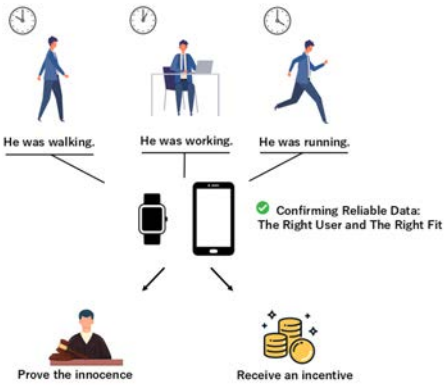

図 1　想定する行動証明システムの概要

[1] 慶應義塾大学 理工学部情報工学科
[2] 慶應義塾大学大学院 理工学研究科 開放環境科学専攻
[3] 大阪大学 大学院基礎工学研究科 システム創成専攻
[a)] tatsuru2896@keio.jp
[b)] zhuoli.wang@keio.jp
[c)] t.amesaka.es@osaka-u.ac.jp
[d)] sugiura@keio.jp

に対するモデルの耐性の調査も行った．これらは行動証明システムにおける改ざんを困難なものにすることに貢献できるものとなる．

2. 関連研究

2.1 センシングデバイスの装着者認証

ウェアラブルセンシングデバイスを用いた装着者識別に関する研究は広く行われている．その中で主流となっているのは行動や生体情報のパターン計測を用いた生体認証である．Cheung らや Vhaduri らの研究では心拍数をベースとして心拍数だけでは認証できない場合，ユーザが動いているときは歩行データ，動いていないときは呼吸音を交えて考慮し認証する手法を提案した [7], [8], [9]．しかしこの手法ではウェアラブルデバイスに対して心拍数や呼吸音などの計測機能を要求することになる．

その他の手法として Lee らや Liu やは歩行動作から個人を認証する方法を提案している [10], [11]．特に Liu らの研究では路面の種類，センサの装着位置や向きが変化しても安定した性能を示した．これらの認証技術は高い精度を保証する一方でユーザが正しい位置にデバイスを装着していることが前提になっており，我々が目標とする行動証明に使用するには信頼性が乏しいという課題がある．

さらに Guinea らは特定の動作を要求せずに，市販のスマートウォッチを用いて IMU データから個人認証をする方法を提案している [12]．この研究では時系列データを画像に変換し，CNN を用いた深層学習を行うことでこれを実現している．しかしこの研究は既知のユーザを分類する Closed-Set 認証であり，未知のユーザに対する性能は評価されていない．

2.2 センシングデバイスの装着位置識別

ウェアラブルデバイスの装着位置識別を行った研究として，Kunze らは歩行中の加速度パターンから識別を行った [13]．この研究ではまずユーザが歩いているかどうかを検出し，その歩行中の加速度データを使用して手首，頭部，左大腿部のポケット，左胸ポケットの４クラス識別をする手法を提案した．しかし，歩行中以外の識別に未対応であることと，識別クラスの少なさが課題である．

加速度データのみを使用して装着位置識別を行った研究として Sztyler らの研究がある [14]．この研究ではデバイスの位置情報から活動認識の精度が向上することを示した．ただしこの手法は認識精度を改善することを主目的としており，誤装着や信頼性担保までは目的として考慮されていない．本研究では，ウェアラブルデバイスを用いたモーションキャプチャの行動管理システムへの応用を最終目標とし，装着位置識別を信頼性確保の手段として位置づけ，装着者識別と組み合わせた堅牢なシステムの構築を目指す．

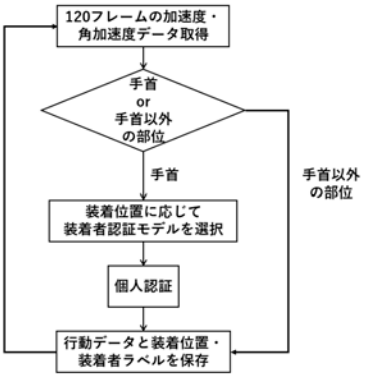

図 2 認証の流れ

他のアプローチとして，カメラ映像を活用して装着者や位置を識別する手法 [15], [16] や，心電図と脈拍の差を用いる手法 [17] も提案されている．しかし，前者はカメラ設置環境への依存やプライバシーの懸念があり，後者は心電図センサという特殊な機器の装着が必要となるため，いずれも日常的な利用シーンにおける課題が残る．

3. 提案手法

本研究では，行動証明における改ざん検出の基盤として，IMU データを用いた装着位置識別および装着者認証を提案する．前者はスマートウォッチ利用を想定した 3 クラス（左右手首・その他）分類，後者は特定ユーザか否かの二値分類である．本研究では両タスクを独立して行うことで，データ増加時の計算コスト増大を抑制する..

システム構成は図 2 の通り，まず装着位置識別を行い，指定位置であることを確認した後，特化型の装着者認証モデルを適用する．このアプローチを採用した理由は装着位置によるデータの統計的性質の差異が大きく，位置混在下での個人識別が困難なためである．例えば手首のデータと腰のデータでは，同じ被験者からのデータでも統計的性質が全く異なる．先に位置を特定し扱うデータの性質を揃えることで，認証モデルの単純化と高精度化を実現する．

4. 実装

4.0.1 データ収集

本研究では，Xsens を用いて取得したモーションキャプチャデータを使用した．センサデータは図 3 に示した 17 カ所と，得られたデータから間接的に計算した点を含めた計 23 箇所から成る．各センサからは，60 Hz で三軸加速度 (a_x, a_y, a_z) および三軸角加速度 (g_x, g_y, g_z) をグローバル座標系で計測し，2 秒間のデータにあたる 120 フレーム分を並べることで時系列データを作成した．この形式でストライドを 30 に設定し，時系列データ群を作成し

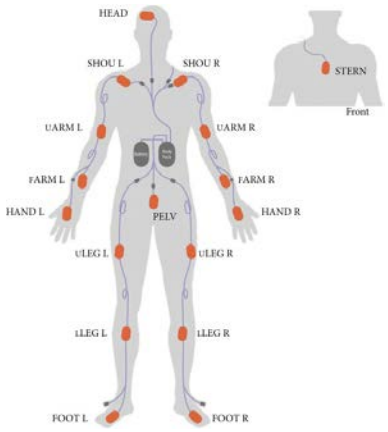

図 3 センサ装着位置 [18]

た．この時系列データに対して装着位置ラベルおよび被験者ラベルを付与し，データセットを構築した．

本研究では 30 名の被験者から歩行中におけるモーションキャプチャデータを取得した．そのうち 22 名から通常の歩行動作のデータを取得した．またそのうち 3 人をターゲットとし，それぞれに対して 15 人分のなりすましデータを取得した．

なりすましデータ取得時には，まずターゲットの歩き方の動画を視聴してもらった上で練習を繰り返した．その様子を動画で撮影し見比べながら修正を行った．この作業後 Xsens を使ってデータを取得した．

4.1 機械学習モデル

本研究で作成した装着位置識別モデルと装着者認証モデルは，学習データに存在しないユーザのデータに対しても頑健に対応できるシステムを構築することを目標としている．したがって単純な多クラス分類器としてではなく，未知のデータに対する頑健性を重視したモデル構築を行う．

4.1.1 装着位置識別モデル

入力された時系列データが右手首，左手首，その他のいずれかの部位に装着されたものかを識別するタスクである．装着位置識別モデルの概要を図 4 に示す．モデルのアーキテクチャには時系列データ内の長期的な時間依存関係の学習に優れた Transformer を使用した．それと並行して高速フーリエ変換を用いて時系列データから周波数領域特徴量を取得し，Transformer 層から得られた時間領域特徴量と結合して特徴ベクトルを作成した．

得られた特徴ベクトルから Triplet Loss を用いて距離学習を行った．学習時には各クラスのプロトタイプを算出しておき，判定時には前の層からの特徴ベクトルとのユークリッド距離が最も近いクラスに分類する．本研究では近かったとしても閾値よりも遠い場合はいずれのクラスにも属さない (unknown) と判断する．

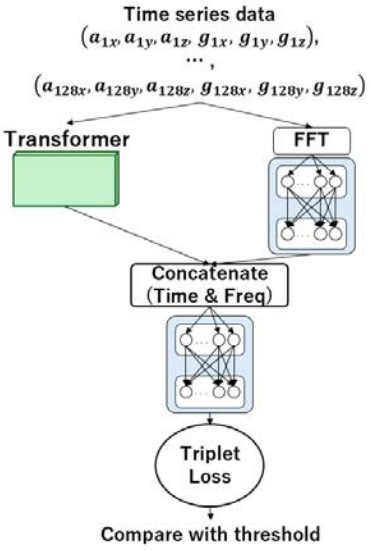

図 4 装着位置識別モデルの概要

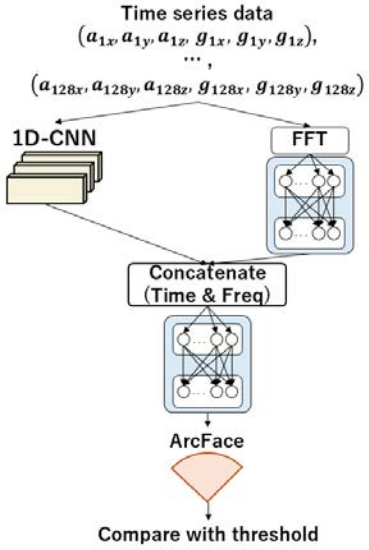

図 5 装着者認証モデルの概要

4.1.2 装着者認証モデル

装着者認証は装着位置が特定された後，そのデータが登録された本人のものか他人のものかを判定するタスクである．今回はスマートウォッチでのシステムの使用を想定し，これらのデバイスは手首に装着されるのが一般的なため，モデルの構築と評価は右手首及び左手首のデータに限定して行った．

装着者認証モデルの概要を図 5 に示す．学習は CNN をバックボーンとするモデルに対し，ArcFace を用いた深層距離学習を行った．データ不均衡に対しては WeightedRandomSampler によるオーバーサンプリングを適用し，さらに VAE で生成した疑似データをネガティブクラスに追加するデータ拡張を行った．損失関数には CrossEntropyLoss を，最適化手法には Adam を用いた．

特徴抽出では，CNN モデルから算出した時間領域特徴

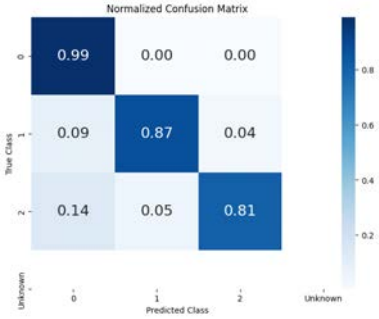

図 6　装着位置識別モデルの未知データによる評価

表 1　各クラスごとの認証結果

	適合率	再現率	F1 スコア	データ数
0: その他	0.9933	0.9951	0.9942	2337
1: 右手首	0.9104	0.9039	0.9071	1113
2: 左手首	0.9351	0.9066	0.9206	1113
Unknown	0.0000	0.0000	0.0000	0
Accuracy	0.9873	-	-	4563

量に加え，FFT と全結合層を経た周波数特徴量を算出し結合した．これを最終的な埋め込みベクトルとして ArcFace 層に入力することで距離学習を行った．

認証の判定はモデルが出力する特徴ベクトルと，学習により得られたターゲットの代表ベクトルとのコサイン類似度に基づいて行った．閾値は本人拒否率 (FRR) と他人受入率 (FAR) が等しくなる等価エラー率 (EER) の時点の値を動的に採用した．

モデルの評価手法として，2-fold 交差検証を採用し，ランダムにシードを変更して 5 回繰り返して行った．各試行において，学習データにはターゲットの 70%のデータと，分割されたグループの他人データを使用した．評価には残りの 30%の本人データと，未知の他人データを使用した．また，なりすましデータに対する評価を行う際，なりすまし動作を行った被験者の通常歩行時のデータは学習データに一切含まれず，完全な Open-Set 認証としての性能検証を行った．

5. 結果

5.1 装着位置識別

未知の時系列データに対する装着位置識別の結果を図 6 に示す．また各クラスごとの性能評価を表 1 に示す．これらの結果を見ると未知の時系列データに対する全体の正答率は 98.7%に達し，全クラスにおいて F1 スコアが 0.90 を超えるなど，全体として非常に高い識別性能を示した．

図 6 の混同行列を見ると手首以外の部位の識別性能が非常に高いことが分かる．この結果から本モデルは手首装着時とそれ以外の部位装着時で得られる IMU データの統計的な性質の根本的な違いを効果的に学習していることが分かる．したがってユーザが想定と別の部位にデバイスを装着した場合でも，高精度で検知し不正利用防止のための技術として極めて有効であることが分かった．

次に右手首と左手首の識別について注目する．図 6 を見ると両クラス間の相互の誤分類率は非常に低く抑えられており，F1 スコアがそれぞれ 0.9071，0.9206 と高い値を達成した．一方でそれぞれのクラスにおいてその他の部位と誤認識するケースがあることが分かる．本研究ではその他の部位を単一のクラスとして扱ったため，具体的にどの部位と混同したのかが特定できていない．この誤分類の詳細な分析はさらなる精度の向上を目指す上で今後の重要な課題である．

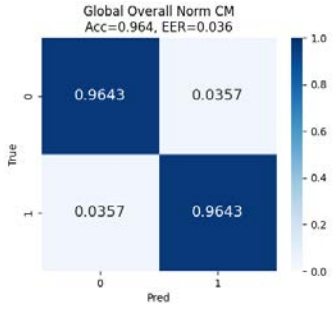

図 7　装着者認証モデルの総合混同行列 (正規化済み)

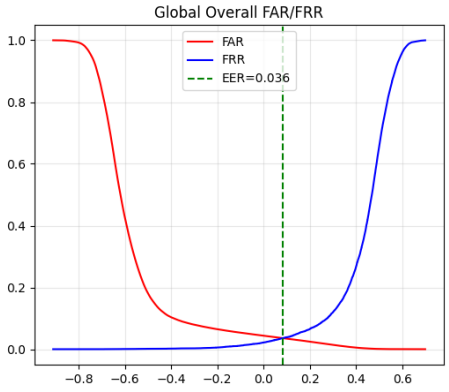

図 8　FAR と FRR のトレードオフ曲線と等価エラー率 (EER)

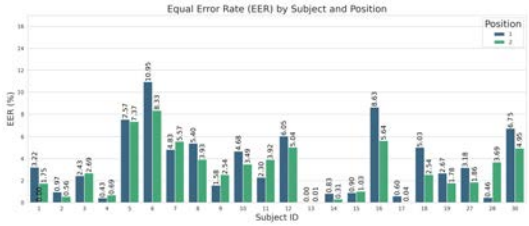

図 9　被験者ごとの等価エラー率 (EER)

5.2 装着者認証

5.2.1 通常の歩行動作データによる認証

図 7 に通常の歩行動作データにおける全試行の結果を統合した正規化混同行列を示す．この結果，本モデルは他人を 96.43%の確率で拒否し，本人を 96.43%の確率で受け入

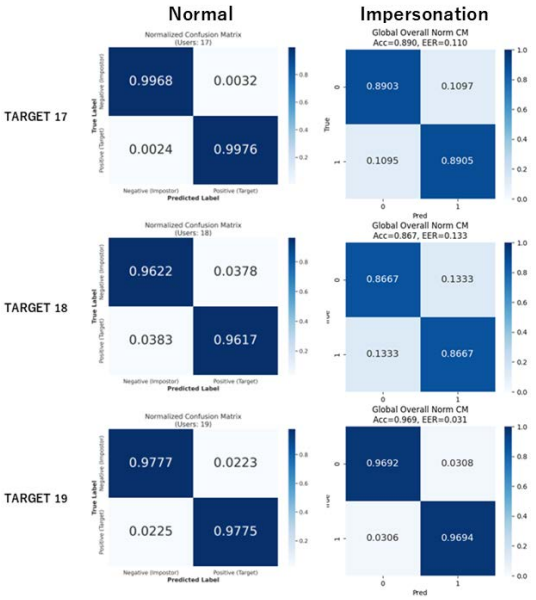

図 10 通常時となりすまし時の総合混同行列の比較

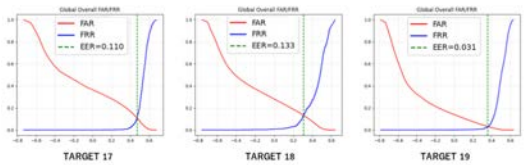

図 11 なりすまし実験における FAR と FRR のトレードオフ曲線

れる性能を達成した．またいずれの参加者も 90 %以上の精度で認証出来ていて，平均認証精度も 96.66% ± 2.69%となっている．次にモデルの総合的な識別性能を評価するため，図 8 に FAR と FRR のトレードオフ曲線を，図 9 に参加者ごとの等価エラー率 (EER) を示す．図 8 を見るとFAR 曲線は閾値が低い領域で急激に低下し，FRR 曲線は閾値が高い領域まで低く維持されている．したがってできるだけ FAR を小さく設定したいという場面でも，FRR の変化が大きくないので利便性への影響は少ないことが分かる．

次に図 9 を見ると全体の EER は 3.6 %という低い値であり，本モデルが高い識別性能を持つことが実証された．ただユーザごとに見ると，EER が最も高い参加者でも 10.95%となっており，被験者によって少々性能にばらつきが生じる結果となった．

5.2.2 なりすましデータによる検証

図 10 は通常歩行データとなりすましデータに対する 3 人のターゲットの個人認証モデルの結果を示している．これを見ると TARGET17, TARGET18 では通常歩行の時に比べ性能が悪化していることが分かる．また図 11 に示したなりすましデータに対する FAR と FRR のトレードオフ曲線を見ると，図 8 と比べて FAR 曲線の収束が遅いことが分かる．加えて図 11 に示したターゲットごとの等価エラー率は図 9 と比べて増加しており，これらのことからモデルが判断基準としている特徴量が模倣動作によって一定程度再現可能であることを示している．認証システムとしては生体認証のように他人が模倣したとしても，それに左右されない特徴量を基に判断することが求められるため，この点については今度の研究課題である．

6. 議論

6.1 本モデルの有効性

本研究で提案した装着位置識別モデル及び装着者認証モデルは，通常時のデータに対してはいずれも高い識別性能を示した．装着位置識別モデルでは全クラスの F1 スコアが 0.90 を超え，特に手首とそれ以外の部位を高精度で区別できることが確認された．また装着者認証モデルでは通常の歩行データを使用した際には，等価エラー率が 3.6%にとどまり，ユーザごとの安定した性能が得られた．

この高い性能を実現できた要因としてタスクの分割が挙げられる．まず装着位置識別を先に行うことで，装着者認証では部位間の統計的性質の際を考慮する必要がなくなり，モデルはユーザ固有の微小な特徴の識別に集中できた．

ただ，なりすましデータに対しては脆弱性が見られる．この原因として現在のモデルが判断基準としている特徴が模倣動作によって再現可能であることを示している．したがって認証システムとして使用するには模倣動作によって再現が困難な特徴量を探索することが必要になる．

6.2 制約と今後の課題

本研究にはいくつかの制約が存在する．第一に本実験は歩行のみのデータを対象としており，静的な状態 (座位や立位) での認証性能は未検証である．動的特徴量が乏しい場合には性能が低下する可能性があるため，静的データを含むモデルの評価や動作を指定しない状態において頑健な特徴量の探索が必要である．

第二に本研究で用いたデータは高精度モーションキャプチャシステム (Xsens) によるものであり，一般的なスマートウォッチ等の IMU センサと比べて高品質である．したがって普及デバイス由来のノイズを多く含むデータで同等の性能が得られるかについては検証が必要である．総じて本研究の成果は行動証明システムの信頼性向上に資する有望な基盤技術である一方，今後は静的状態や攻撃耐性，実用デバイスでの性能検証を通じて実運用に耐えうる更なる頑健性の確立が求められる．

7. 結論

本研究では，行動証明におけるデータ改ざんの困難性を実現することを目的に，装着位置および装着者の変更を検

出する機械学習モデルを提案しその有効性を検証した．深層学習を基盤としたモデル設計を行い．装着位置識別モデルではすべてのクラスにおいて F1 スコア 0.90 を超え，装着者認証モデルでは等価エラー率 3.6%という高い性能を達成した．

一方で本研究の課題としてはなりすましデータによって等価エラー率や精度，FAR の収束度合いが悪化してしまったことである．今後は模倣動作によって再現されない特徴の探索が求められる．さらに本研究の制約として，静的状態における認証性能の未検証，スマートウォッチ等の実運用環境におけるノイズを含むデータでの検証が未実施であることが挙げられる．今後はこれらの課題に取り組むことで，行動証明システムにおける改ざんの困難性をさらに高めていく予定である．

謝辞

本研究の一部は，JST AIP 加速課題（課題番号：JPMJCR25U4）の支援を受けたものである．

参考文献

[1] Vimal Mollyn, Riku Arakawa, Mayank Goel, Chris Harrison, and Karan Ahuja: IMUPoser: Full-Body Pose Estimation using IMUs in Phones, Watches, and Earbuds, *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, Art. 529, 12 pages, Association for Computing Machinery, Hamburg, Germany (2023). (https://doi.org/10.1145/3544548.3581392)

[2] Vasco Xu, Chenfeng Gao, Henry Hoffmann, and Karan Ahuja: MobilePoser: Real-Time Full-Body Pose Estimation and 3D Human Translation from IMUs in Mobile Consumer Devices, *Proceedings of the 37th Annual ACM Symposium on User Interface Software and Technology*, Art. 70, 11 pages, Association for Computing Machinery, Pittsburgh, PA, USA (2024). (https://doi.org/10.1145/3654777.3676461)

[3] Nathan DeVrio, Vimal Mollyn, and Chris Harrison: SmartPoser: Arm Pose Estimation with a Smartphone and Smartwatch Using UWB and IMU Data, *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology*, Art. 79, 11 pages, Association for Computing Machinery, San Francisco, CA, USA (2023). (https://doi.org/10.1145/3586183.3606821)

[4] Vitality, 住友生命 (https://vitality.sumitomolife.co.jp/)

[5] 第一生命. (https://www.dai-ichi-life.co.jp/sp/campaign/kenko.html)

[6] あるく保険, 東京海上日動あんしん生命. (https://www7.tmn-anshin.co.jp/yakkan/pdf/A0105170802.pdf)

[7] William Cheung and Sudip Vhaduri: Context-Dependent Implicit Authentication for Wearable Device Users, *Proceedings of the 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–7, IEEE, (2020). (https://doi.org/10.1109/PIMRC48278.2020.9217224)

[8] Sudip Vhaduri and Christian Poellabauer: Multi-Modal Biometric-Based Implicit Authentication of Wearable Device Users, *IEEE Transactions on Information Forensics and Security*, Vol. 14, No. 12, pp. 3116–3125, IEEE, (2019). (https://doi.org/10.1109/TIFS.2019.2911170)

[9] Sudip Vhaduri, Sayanton Dibbo Vhaduri and William Cheung: HIAuth: A Hierarchical Implicit Authentication System for IoT Wearables Using Multiple Biometrics, *IEEE Access*, Vol. 9, pp. 116395–116406, IEEE, (2021). (https://doi.org/10.1109/ACCESS.2021.3105481)

[10] Soobin Lee, Seungjae Lee, Eunkyoung Park, Jongshill Lee and In Young Kim: Gait-Based Continuous Authentication Using a Novel Sensor Compensation Algorithm and Geometric Features Extracted From Wearable Sensors, *IEEE Access*, Vol. 10, pp. 120122–120135, IEEE, (2022). (https://doi.org/10.1109/ACCESS.2022.3221813)

[11] Yushi Liu, Kamen Ivanov, Junxian Wang, Fuhai Xiong, Jiahong Wang, Min Wang, Zedong Nie, Lei Wang and Yan Yan: Topological Data Analysis for Robust Gait Biometrics Based on Wearable Sensors, *IEEE Transactions on Consumer Electronics*, Vol. 70, No. 2, pp. 4910–4921, IEEE, (2024). (https://doi.org/10.1109/TCE.2024.3396177)

[12] Sanchez Guinea, A.; Heinrich, S.; Mühlhäuser, M. Activity-Free User Identification Using Wearables Based on Vision Techniques. *Sensors 2022, 22, 7368.* (https://doi.org/10.3390/s22197368)

[13] Klaus Kunze, Patrick Lukowicz, Harald Junker, Gerhard Tröster: Where am I: Recognizing On-body Positions of Wearable Sensors, In: Thomas Strang, Christian Linnhoff-Popien (eds) *Location- and Context-Awareness. LoCA 2005. Lecture Notes in Computer Science*, Vol. 3479, Springer, Berlin, Heidelberg, pp. 214–229, (2005). (https://doi.org/10.1007/11426646_25)

[14] Timo Sztyler, Heiner Stuckenschmidt: On-body localization of wearable devices: An investigation of position-aware activity recognition, *Proc. 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 1–9, (2016). DOI: 10.1109/PERCOM.2016.7456521

[15] Carlos Ruiz, Shijia Pan, Hae Young Noh, Pei Zhang: WhereWear: Calibration-free Wearable Device Identification through Ambient Sensing, *Proc. The 5th ACM Workshop on Wearable Systems and Applications (WearSys '19)*, pp. 29–34, (2019). DOI: 10.1145/3325424.3329667

[16] Adeola Bannis, Shijia Pan, Carlos Ruiz, John Shen, Hae Young Noh, Pei Zhang: IDIoT: Multimodal Framework for Ubiquitous Identification and Assignment of Human-carried Wearable Devices, *ACM Trans. Internet Things*, Vol. 4, No. 2, Art. 11, 25 pages (2023). DOI: 10.1145/3579832

[17] Kazuki Yoshida, Kazuya Murao: Estimating load positions of wearable devices based on difference in pulse wave arrival time, *Proc. ACM Int. Symp. Wearable Computers (ISWC '19)*, pp. 234–243, 10 pages, London, United Kingdom (2019). DOI: 10.1145/3341163.3347743

[18] Xsens (2017). Quick setup: getting started with xsens mvn.