測距センサとIMUセンサを用いた指輪型デバイスにおける顔認証システムの提案

宮下 海[1,a)]　雨坂 宇宙[1,b)]　山本 匠[1,c)]　花山 勝吾[1,d)]　杉浦 裕太[1,e)]

概要：スマートリングは，主に決済やスマートロックなどに利用できる便利なウェアラブルデバイスであるが，個人認証機能の搭載例は少なくセキュリティ上の懸念が残されている．心拍数や動作特性を利用する認証では，認証に時間がかかるなどの問題があり，指紋認証や顔認証もデバイスのサイズや消費電力，プライバシーの問題が課題となっている．そこで，我々は測距センサと IMU センサを搭載した指輪型デバイスを用いることで，スマートリングに搭載可能なほど小型かつ省電力で，カメラ不使用によりプライバシーリスクを低減した顔認証システムを提案する．11 名でのユーザ実験を行い提案システムの精度を評価した結果，安定した環境では 86.73 %の平均認証精度および 13.12 %の平均 EER を達成した．

1. はじめに

スマートリングは，主に健康管理やスマートロックを目的としたウェアラブルデバイスとして普及している [1][2]．スマートリングにおける個人認証を実用化することで，スマートリングを用いた大学授業の出席管理や電子決済に応用させることも期待される．しかし，スマートリングに個人認証システムが搭載されている例は稀である．さらに，個人認証システムが搭載されているスマートリングでも，利用されている認証要素は心拍数や運動特性などであり [3]，それらには認証時間の長さや再現攻撃を受けるリスクなどの欠点がある．また，認証手法として広く普及している指紋認証は，指紋が薄い人や指に汗をかきやすい人の利用が難しく [4]，季節によって皮膚の状態が変動し認証精度が左右されやすい．さらに，指紋認証と同様に広く普及している顔認証は，一般的に小型のデバイスに搭載することはコストや消費電力の制約から難しい．そのうえ，カメラを用いた顔認証ではプライバシー上の問題がある [5]．

そこで我々は，距離センサと IMU センサを用いた簡易的な顔認証システムを提案する．これらのセンサを用いることで，省電力で小型なデバイスを設計することが可能になり，従来のカメラを用いた顔認証よりもプライバシー問題の影響が少ない．我々の提案手法では，センサを搭載したスマートリングでユーザの顔を左右往復方向にスキャンすることで，顔構造を取得する．本研究では，簡易的な指輪型デバイスを作製し提案手法の評価実験を行った．実験参加者に異なる明るさの場所でデータを計測してもらい，そのデータを用いて行った認証の精度を検証した．実験の結果，安定環境下での認証システムの平均精度および平均 EER が，それぞれ 86.73 %，13.12 % となった．

図 1　システムの流れ
Fig. 1　System Flow.

2. 関連研究

2.1 ウェアラブルデバイスにおける個人認証

これまでにも多くのウェアラブルデバイスにおける個人認証システムが研究されている．SigningRing[6] は，IMU センサ内蔵のスマートリングを装着したユーザが署名をす

[1] 慶應義塾大学
[a)] miyakai0123@keio.jp
[b)] amesaka@keio.jp
[c)] imuka06x17@keio.jp
[d)] shogo-hana@keio.jp
[e)] sugiura@keio.jp

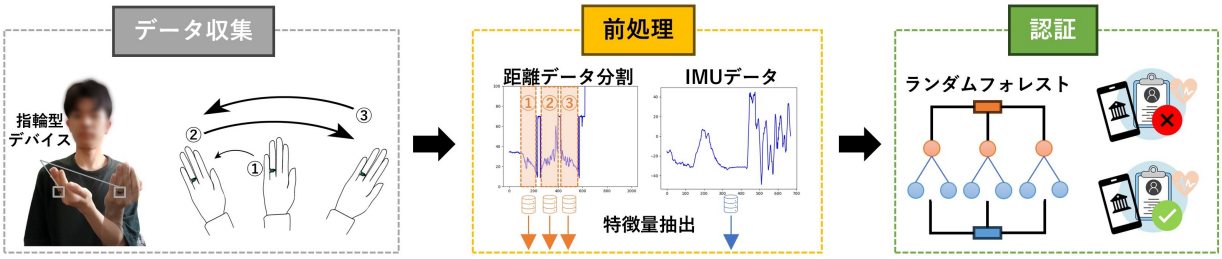

図 2 システム概要
Fig. 2 System Overview.

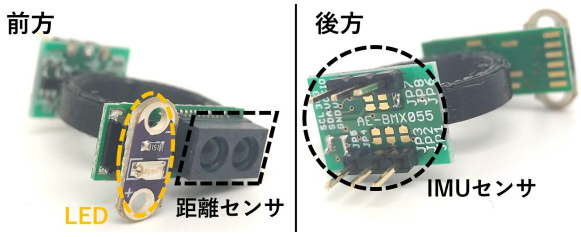

図 3 指輪型デバイス
Fig. 3 Ring Device.

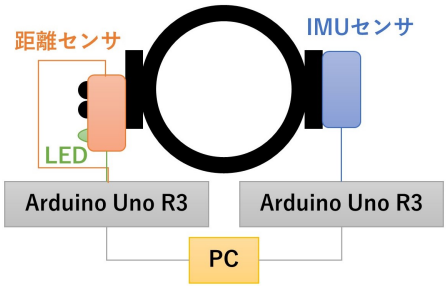

図 4 デバイスの構成
Fig. 4 Device Configuration.

るように空中で指を動かすことで変化する IMU センサ値を用いた個人認証システムである．SmartEar[7] は，加速度センサ内蔵のイヤホンをユーザがリズミカルにタップすることで表れる動作特性を用いて，個人認証を実現しているシステムである．Iwakiri ら [8] はリング型デバイスを用いて指の音響伝播特性を用いた個人認証システムを提案している．しかし，動作特性を用いる個人認証にはリプレイ攻撃に弱いという欠点があり，音響伝播特性を用いる個人認証にはマイクやスピーカなどの消費電力が高いという欠点がある．本研究では顔の形状とスキャン動作の特性の双方を認証に用いることで攻撃耐性を強化し，さらに省電力なセンサを活用することでスマートリングへ搭載可能とすることを目標としている．

2.2 カメラ不使用の顔認証

カメラを使用せずに顔構造を取得することで顔認証を行う研究が行われている．カメラを用いる代わりに，アクティブ音響センシングを用いるもの [9][10][11] や RFID タグを用いるもの [12] などが提案されている．これらは顔の凹凸を検知するためなりすまし攻撃に対して堅牢であり，消費電力が低いという利点がある．本研究では，測距センサで顔の凹凸を検知することでなりすまし攻撃への耐性を強化し，省電力なセンサを使用することでシステム全体の消費電力を抑制することを目指す．

3. 提案手法

提案手法の流れを図 2 に示す．ユーザは図 3 のような指輪型デバイスを自分の指に装着し，3.1 節に示すスキャン方法によってユーザ自身の顔構造およびスキャン動作を示す距離データと IMU データを取得する．取得された距離データおよび IMU データは 3.2 節に示すように前処理が行われ，認証要素として利用される．

3.1 使用するデバイスとスキャン方法

図 4 にデバイス構成を示す．3D プリンタで作製したリングに三角測量方式の測距センサ（GP2Y0E02A：SHARP 社），IMU センサ（AE-BMX055：BOSCH 社），LED ライト（LilyPad 社）が 1 個ずつ取り付けられている．デバイスはリングの内径が 16 mm，18 mm，20 mm の 3 種類を用意した．測距センサおよび IMU センサから取得したセンサ値は Arduino Uno R3 を用いてノートパソコン（ASUS：ZenBook Flip S UX371EA）に送信される．サンプリングレートは測距センサ，IMU センサともに約 100 Hz であった．

スキャン方法の要件は，同一のユーザによる毎回のスキャン動作の再現性が高いこと，スキャン範囲内の顔構造が個人間で異なることである．そこで本研究では，腕旋回スキャンを採用した（図 2 データ収集）．ユーザは，まず右腕の脇を閉め，上腕を身体の側面に沿わせる．次に，肘の位置を固定しながら前腕を傾けることでスキャン開始位置を決定する．スキャン開始後，開始位置から左方向，右方向，左方向の順に，肘を中心に腕を円弧状に動かす．

測距センサは，リングと顔の距離を計測することで顔構造を取得するのに用いる．使用する測距センサの特性上，測定範囲外に顔が出ている場合にはセンサ値が 60 cm ～ 70 cm で振動し，再び測定範囲内に顔が入ると急激にセンサ値が低下した後に正確なセンサ値を示す．そこで，ス

キャン動作によって測距センサの測定範囲外に顔が出てセンサ値が 60 cm を超えると LED が点灯し，そのタイミングで方向転換を行うようにした．そして 1.5 秒以上センサ値が 60 cm を超えている場合にスキャンが終了したとし，LED が点滅を開始するようになっている．なお IMU センサは，ユーザのスキャン動作の特性を取得するのに用いる．使用する IMU センサは加速度・角速度・地磁気を 3 軸ずつ測定することができる．

3.2 データ前処理方法

取得した距離データおよび IMU データは，図 5 のように前処理が施される．取得した距離データに対しては，まず 5 フレームごとに平滑化処理を施す（図 5 a）．次に，距離データをスキャン動作に応じて 3 分割する（図 5 b ①〜③）．そして，①〜③それぞれの区間について，最大値・最小値・平均値・中央値・母分散を算出する（図 5 c）．取得した IMU データに対しては，センサ値が不安定な最初の 10 フレームを削除し（図 5 d），そこからロール・ピッチ・ヨーを計算し（図 5 e），それぞれに対して最大値・最小値・平均値・中央値・母分散を算出する（図 5 f）．

3.3 学習器および評価指標

学習データに前処理を完了したデータ群を，分類器にランダムフォレストを用いて入力データが本人のものか他人のものかの二値分類を行う．ランダムフォレストのパラメータは，すべて sklearn.ensemble の RandomForestClassifier[13] のデフォルト値となっている（max_depth: 指定なし，max_features: $\sqrt{30}$，min_samples_leaf: 1，criterion: ジニ係数）．認証システムは，入力データが本人のものである予測確率がある特定の閾値以上の場合，そのデータが本人だと分類する．ここで，二値分類における予測確率の閾値が 0.5 のときの分類精度を評価指標とする．また，閾値を 0 から 1 の間で 0.05 ずつ変化させながら各閾値に対する FAR および FRR を計算し，それらをプロットすることで FAR 曲線および FRR 曲線を求め，両曲線の交点である EER を算出し，評価指標とした．FAR 曲線，FRR 曲線，EER の関係を図 6 に示す．FAR（他人受入率）とは，他人のデータを本人のデータと誤る割合で低いほど他人からのなりすまし攻撃に強くなり，FRR（本人拒否率）とは，本人のデータを他人のデータと誤る割合で低いほど認証成功確率が高くなる．EER（等価エラー率）とは FAR と FRR が一致するときの割合のことであり，一般に低いほどその認証システムの精度が高いことを意味する．

4. 評価

4.1 概要

データ収集を行う照明環境による認証精度への影響を調査するため，11 人のユーザを対象としたユーザスタディを実施した．参加者は全員が右利き（平均年齢 23.6 歳，標準偏差 2.77 歳）であった．使用したリングはユーザの指の大きさに合わせて使い分けた．内径 16 mm のリングを使用した参加者は 9 名，内径 18 mm のリングを使用した参加者は 1 名，内径 20 mm のリングを使用した参加者は 1 名だった．参加者は利き手によらず右手の薬指にリングを装着した．

スキャン開始位置は，図 7 a のようにのように測距センサの発光部が赤色に円状に点灯しているのを実験参加者が目視で確認できる位置とした．このようにすることで，図 7 b のようにスキャン開始位置が実験参加者の目に合うように調整することができた．なお，実験で使用した測距センサの赤外線レーザー波長は 850 nm ± 70 nm であり，人体への重大な影響はないことを確認した．また本実験の実施について，著者の所属する研究機関である慶應義塾大学の研究倫理委員会から承認を得ている．

照明環境は 2 つ用意し，それぞれ室内で直射日光の入らない照明を落とした部屋（照明環境 (A)），室内で直射日光が入る照明を落とした部屋（照明環境 (B)）であった．照明環境 (A) および (B) の実験時の平均照度はそれぞれ 35 lux ± 16 lux，1200 lux ± 500 lux であった．実験参加者 1 人当たりの測定データ数は，照明環境 (A) では 15，照明環境 (B) では 5 とした．実験参加者は 1 回の測定が完了するごとに実験デバイスを一度外し，指と手首をほぐしてから再度装着してから次の測定を行うようにした．また，実験の前に参加者にはスキャン動作の練習をしてもらった．

認証精度の評価方法は 3 種類用意した．1 つ目は，照明環境 (A) のみのデータセットを用い，各実験参加者について本人データ 15 セットおよび他人データ 15 セットを用意し，計 30 データを用いた一つ抜き交差検証を 10 回繰り返し，その平均値を計算することにより分類精度を評価した（評価方法 (1)）．本人データは実験で取得したすべてのデータを対象とし，他人データは本人以外の計 150 データから無作為に抽出した 15 データを対象とした．2 つ目は，各実験参加者について照明環境 (A) の本人データ 15 セットおよび照明環境 (A) の他人データ 15 セットを訓練データとし，照明環境 (B) の本人データ 5 セットおよび照明環境 (B) の他人データ 5 セットをテストデータとして精度を評価した（評価方法 (2)）．評価方法 (1) と同様に，本人データは実験で取得したすべてのデータを対象とし，他人データは照明環境 (A) については本人以外の計 150 データから無作為に抽出した 15 データを対象とし，照明環境 (B) については本人以外の計 50 データから無作為に抽出した 5 データを対象とした．3 つ目は，各実験参加者について照明環境 (A) および (B) の本人データ計 20 セット，照明環境 (A) の他人データ 15 セット，および照明環境 (B) の他人データ 5 セットを用意し，計 40 データを用いた一つ

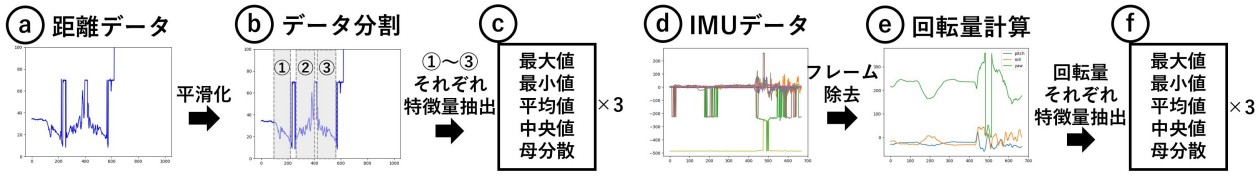

図 5 データ前処理の流れ
Fig. 5 Flow of Data Preprocessing.

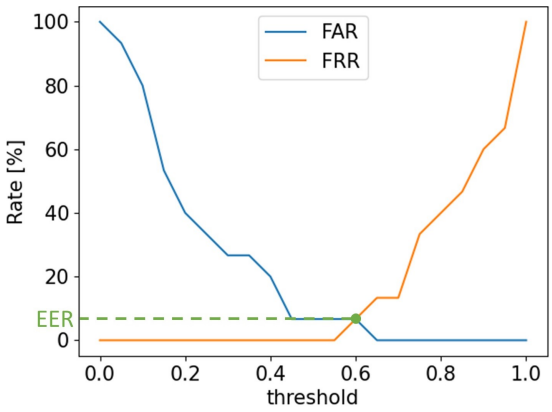

図 6 FAR 曲線，FRR 曲線，EER の関係
Fig. 6 Relationship between FAR Curve, FRR Curve, and EER.

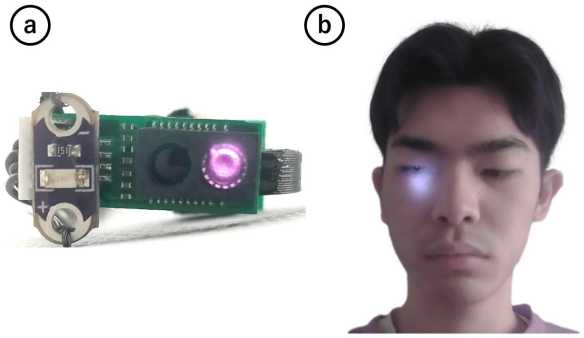

図 7 スキャン開始位置
Fig. 7 Scan-Starting Position.

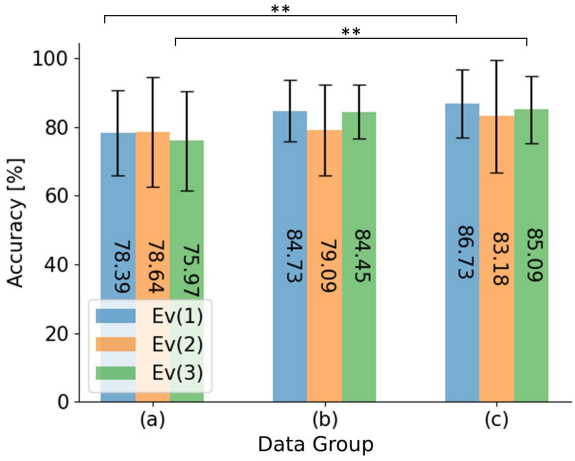

図 8 平均精度
Fig. 8 Accuracy Average.

抜き交差検証を 10 回繰り返し，その平均値を計算することにより分類精度を評価した（評価方法 (3)）．対象となるデータの選定方法は評価方法 (2) と同様である．

3.2 節のような前処理が施されたデータ群は，ランダムフォレストによって本人のものか他人のものかに分類され，学習に使用するデータは (a) 距離データのみ，(b) IMU データのみ，(c) 距離データ＋ IMU データの 3 条件とし，認証精度および EER を評価方法とデータ群で比較した．

4.2 結果

4.2.1 精度

各条件下での平均認証精度を図 8 に示す．

評価方法 (1) を用いた場合，データ群 (a)，(b)，(c) を用いたときの平均認証精度はそれぞれ 78.39 % ± 12.39 %，84.73 % ± 8.96 %，86.73 % ± 9.96 %，評価方法 (2) を用いた場合，データ群 (a)，(b)，(c) を用いたときの平均認証精度はそれぞれ 78.64 % ± 15.96 %，79.09 % ± 13.14 %，83.18 % ± 16.42 %，評価方法 (3) を用いた場合，データ群 (a)，(b)，(c) を用いたときの平均認証精度はそれぞれ 75.97 % ± 14.40 %，84.45 % ± 7.84 %，85.09 % ± 9.85 % となった．有意差検定の結果は，評価方法 (1) と (3) において，データ群 (a) と (c) に有意差が認められた．

データ群の比較については，有意差は認められないがどの評価方法においてもデータ群 (a) よりもデータ群 (b) の平均精度が高くなっていることから，距離データと IMU データでは IMU データの方が認証要素としての貢献度が高くなっていることがわかる．また，データ群 (b) とデータ群 (c) の平均精度の差について，すべての評価方法のうち (2) を用いた場合が最大となった．評価方法 (2) は全体的に他の評価方法よりも平均精度が低いことも考慮に入れると，IMU データでうまく認証が行えない場合に距離データがその認証精度を向上させる働きがあると思われる．以上のことから，提案手法において距離データも IMU データも認証には必要な情報であると考えられる．

照明環境の比較については，データ群 (a) における評価方法 (1) と (2) で平均精度に 1 % 未満の差しかないことから，1170 lux 程度の照度の差では距離データの測定に大きな影響はないと考えられる．しかし，データ群 (b) および (c) では評価方法 (1) と (2) で平均精度に約 4 % の差が確認されたため，IMU センサの測定状態に各測定での差異が

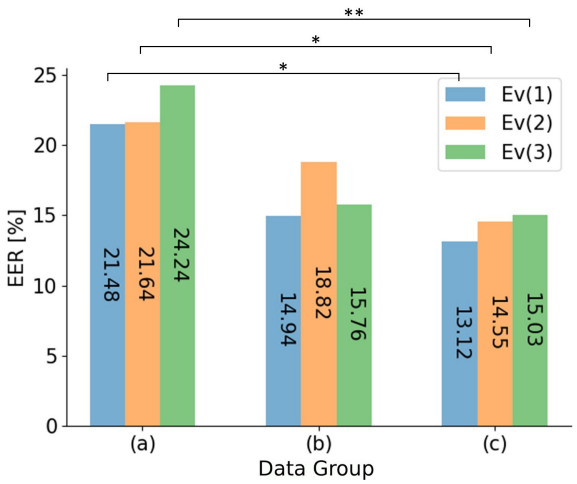

図 9 平均 EER
Fig. 9 EER Average.

あったと推測できる．IMU センサの照度の違いによる測定誤差は原理上発生しないため，要因として挙げられるのは，実験環境を変更した際に生じる実験参加者のスキャン動作の個人内誤差による影響だと考えられる．また，訓練データに照明環境 (B) のような明るい環境下で計測したデータを含めることは，どのデータ群においても評価方法 (1) と (3) で平均精度に大きな差が認められないことから，大きな問題にはならないと思われる．しかし，評価方法 (3) のほうが平均精度が若干低いことから，照明環境 (A) のようになるべく暗い環境下でデータを計測をするべきだと考えられる．

4.2.2 EER

各条件下での平均 EER を図 9 に示す．

評価方法 (1) を用いた場合，データ群 (a)，(b)，(c) を用いたときの平均認証精度はそれぞれ 21.48 % ± 11.93 %，14.94 % ± 9.21 %，13.12 % ± 9.77 %，評価方法 (2) を用いた場合，データ群 (a)，(b)，(c) を用いたときの平均 EER はそれぞれ 21.64 % ± 17.93 %，18.82 % ± 15.73 %，14.55 % ± 17.04 %，評価方法 (3) を用いた場合，データ群 (a)，(b)，(c) を用いたときの平均認証精度はそれぞれ 24.24 % ± 14.32 %，15.76 % ± 7.80 %，15.03 % ± 9.25 % となった．有意差検定の結果は，すべての評価方法においてデータ群 (a) と (c) に有意差が認められた．

5. 議論・制約・今後の展望

5.1 スキャン方法

本手法ではスキャン方法として腕旋回スキャンを採用したが，評価実験の際に腕旋回スキャン動作が困難に感じている参加者が一部いた．動作の再現性が高いという観点で考案した腕旋回スキャンだが，動作が困難に感じる場合は再現性が低くなってしまう可能性がある．

ここで，評価方法 (1)，データ群 (c) を用いた場合の各実験参加者の平均認証精度を図 10 に示す．スキャン動作

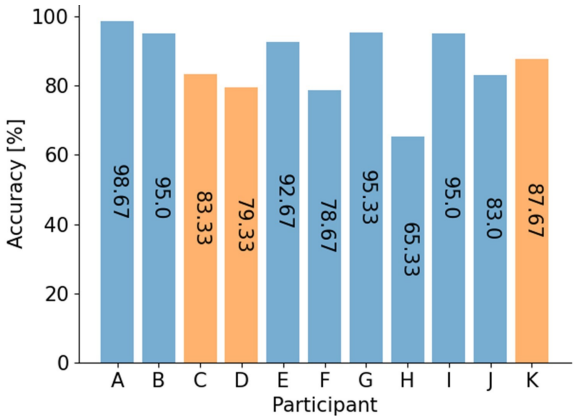

図 10 実験参加者ごとの平均認証精度
Fig. 10 Accuracy Average per participant.

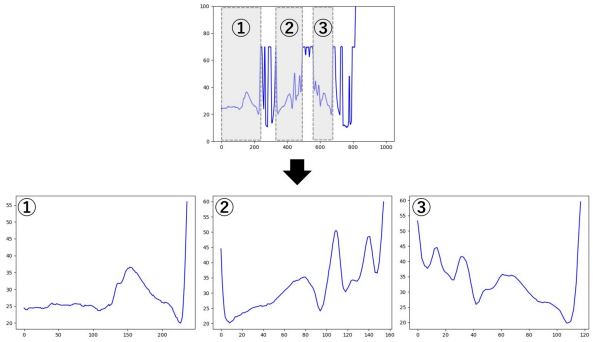

図 11 距離データ分割成功例
Fig. 11 Successful Example of Distance Data Segmentation.

が難しいと回答した実験参加者（棒が橙色）のデータの平均認証精度は 83.44 % ± 4.17 %，そうでない実験参加者（棒が青色）のデータの平均認証精度は 87.96 % ± 11.42 % となった．実験参加者 F や H のように，スキャン動作が難しいと回答していなくても精度が低くなっているデータも存在することを考慮に入れると，スキャン動作の得手不得手は認証精度にさほど大きな影響は及ぼさないと考えられる．

しかし，スキャン動作が困難に感じるとその分ユーザビリティが低下してしまうため，別のスキャン動作を考案する必要がある．動作の再現性を維持しつつユーザビリティを高めるために，例えばデバイスは動かさずに顔や首を動かす動作が挙げられる．

5.2 距離データ分割方法

3.2 節で前述したとおり，取得した距離データはスキャン動作に応じて 3 分割される．図 11 に距離データが分割されている様子を示す．この分割アルゴリズムでは，50 フレーム以内にセンサ値が 60 cm を超えているフレームを分割点としている．この分割点が，ユーザがちょうどスキャン動作において方向転換を行うタイミングと一致しているのが理想的である．しかし，図 11 のように分割が成功する場合が多いが，図 12 のように分割が失敗する場合があ

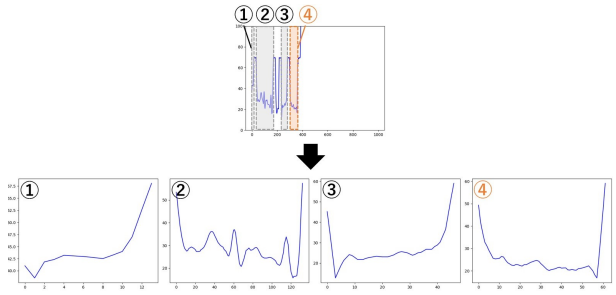

図 12 距離データ分割失敗例
Fig. 12 Failed Example of Distance Data Segmentation.

る．失敗例を観察すると，距離データ計測時に想定よりも断続的にセンサ値が 60 cm 以上となっている，すなわちスキャン範囲に顔が入っていない場合に，その分多くの波形に分割されていることがわかる．

考えられる解決策の一つは，分割点として判定するためのセンサ値が 60 cm を超えているフレーム数を増加させることである．そうすれば，測定時に誤って顔がスキャン範囲外に出てしまった部分の誤差を軽減することができる．しかし，そのフレーム数を大きくしすぎると，スキャン時の方向転換のタイミングを認識できなくなってしまうため，分割数が 3 未満となる可能性がある．そのため，分割点として判定するためのセンサ値が 60 cm を超えているフレーム数をいくつにすべきかは，パラメータスタディを行って議論すべきである．

または，想定通りに距離データが分割されなかった場合にユーザにもう一度スキャン動作を行ってもらうようにするという解決策も挙げられる．ユーザがこの指示に従うようにすれば，距離データの分割を誤ることはなくなる．しかし，再度のスキャン動作はユーザビリティを低下させてしまう可能性があるため，距離データ分割アルゴリズムの改善が重要である．

6. おわりに

本論文では，測距センサと IMU センサを用いた指輪型デバイスにおける顔認証システムを提案した．実験で確認できた認証システムの最良の場合の平均精度および平均 EER が，それぞれ 86.73 %，13.12 % となった．今後は，ユーザビリティ向上のために，位置合わせを含むスキャン方法の見直し，認証精度向上のための前処理アルゴリズムや認証システムの改善を行っていく．

謝辞

本研究の一部は, JST さきがけ (課題番号：JPMJPR2134) の支援を受けたものである．

参考文献

[1] Motiv: Motiv ring: 24/7 smart ring: Fitness + sleep tracking motiv ring, https://mymotiv.com/. (2024 年 7 月 10 日閲覧).
[2] EVERING: Keyless, https://evering.jp/keyless. (2024 年 7 月 10 日閲覧).
[3] Koetsier, J.: 指輪型スマートデバイス Motiv で激変する「次世代の個人認証」, https://forbesjapan.com/articles/detail/34274. (2024 年 7 月 10 日閲覧).
[4] H L, G., M N, N., Flammini, F., K P, V. and B C, S.: Analysis of Finger Vein Recognition using Deep Learning Techniques: Finger Vein Recognition, *Proceedings of the 2022 7th International Conference on Machine Learning Technologies*, ICMLT '22, New York, NY, USA, Association for Computing Machinery, pp. 136–140 (online), DOI: 10.1145/3529399.3529422 (2022).
[5] Rui, Z. and Yan, Z.: A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification, *IEEE Access*, Vol. 7, pp. 5994–6009 (online), DOI: 10.1109/ACCESS.2018.2889996 (2019).
[6] Cao, Y., Dhekne, A. and Ammar, M.: SigningRing: Signature-based Authentication using Inertial Sensors on a Ring Form-factor, *Proceedings of the Workshop on Body-Centric Computing Systems*, BodySys '24, New York, NY, USA, Association for Computing Machinery, p. 11–16 (online), DOI: 10.1145/3662009.3662019 (2024).
[7] Bi, H., Sun, Y., Liu, J. and Cao, L.: SmartEar: Rhythm-Based Tap Authentication Using Earphone in Information-Centric Wireless Sensor Network, *IEEE Internet of Things Journal*, Vol. 9, No. 2, pp. 885–896 (online), DOI: 10.1109/JIOT.2021.3063479 (2022).
[8] 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, New York, NY, USA, Association for Computing Machinery, pp. 17–21 (online), DOI: 10.1145/3594738.3611357 (2023).
[9] Chen, H., Wang, W., Zhang, J. and Zhang, Q.: EchoFace: Acoustic Sensor-Based Media Attack Detection for Face Authentication, *IEEE Internet of Things Journal*, Vol. 7, No. 3, pp. 2152–2159 (online), DOI: 10.1109/JIOT.2019.2959203 (2020).
[10] Zhou, B., Xie, Z., Zhang, Y., Lohokare, J., Gao, R. and Ye, F.: Robust Human Face Authentication Leveraging Acoustic Sensing on Smartphones, *IEEE Transactions on Mobile Computing*, Vol. 21, No. 8, pp. 3009–3023 (online), DOI: 10.1109/TMC.2020.3048659 (2022).
[11] Wang, R., Huang, L. and Wang, C.: Low-effort VR Headset User Authentication Using Head-reverberated Sounds with Replay Resistance, *2023 IEEE Symposium on Security and Privacy (SP)*, pp. 3450–3465 (online), DOI: 10.1109/SP46215.2023.10179367 (2023).
[12] Xu, W., Liu, J., Zhang, S., Zheng, Y., Lin, F., Han, J., Xiao, F. and Ren, K.: RFace: Anti-Spoofing Facial Authentication Using COTS RFID, *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, pp. 1–10 (online), DOI: 10.1109/INFOCOM42981.2021.9488737 (2021).
[13] Scikit: RandomForestClassifier, https://scikit-learn.org/1.5/modules/generated/sklearn.ensemble.RandomForestClassifier.html. (2024 年 10 月 28 日閲覧).