

# 握りこぶしの 3次元情報を利用した個人認証システムの提案

馬場 博久<sup>1</sup> 福元 伸也<sup>1</sup> 鹿嶋 雅之<sup>1</sup> 佐藤 公則<sup>1</sup> 渡邊 睦<sup>1</sup>

**概要:** 情報化の発展に伴い、セキュリティをより強固にすることが期待されている。現在は PIN(Personal Identification Number) コードなどを用いた認証方法があるが、漏洩や盗難によって悪用される可能性が高い。そこで手軽で、第三者が認証することを防止できる認証手段として、人間の身体的特徴や行動的特徴を用いた生体認証の研究が進んでいる。しかし、複製により認証を突破されてしまう問題がある。本研究では、生体情報として握りこぶしを利用した個人認証方法の提案を行う。撮影には深度センサおよび RGB カメラを内蔵した Intel 社の RealSense を用い、個人の特徴を検出し個人認証を行う。

**キーワード:** バイオメトリクス, 画像処理, 画像特徴抽出

## Study on Personal Authentication System by 3D information of Fist

BABA HIROHISA<sup>1</sup> FUKUMOTO SHINYA<sup>1</sup> KASHIMA MASAYUKI<sup>1</sup> SATO KIMINORI<sup>1</sup> WATANABE MUTSUMI<sup>1</sup>

**Abstract:** Now rigid security is required by an authentication system as computerization. Although there are many researches of authentication systems using physical or behavioral features such as the iris or finger prints, they have risks which duplication unlock the systems. We define fist as physical feature and use it for a personal authentication system. This paper shows the authentication system by fist images and 3D information using RealSense.

**Keywords:** Biometrics, Image Processing, Image Feature Extraction

### 1. 研究の背景と目的

近年、より強固なセキュリティシステムの需要が増え、人間個人の固有な特徴を使った個人認証であるバイオメトリクス認証の研究が盛んに行われている。バイオメトリクス個人認証は、認証に使われる部位が本人から切り離すことが出来ない、高いセキュリティを持つ、実装コストが安価であるといった優位性があり普及が進んでいる。これは指紋や静脈などの人間の部位の一部を用いた身体的特徴による認証と、筆跡や発話や歩き方といった個人の癖を特徴とした行動的特徴による認証の2つに大きく分けられる。

身体的特徴による認証は、個人で異なる生体的な特徴を

用いており精度も良い。しかし、シリコンなどで偽造された指紋や、他人の虹彩が印刷されたコンタクトレンズなどを用いて認証システムを突破されてしまうという欠点がある。行動的特徴を用いた認証は、筆跡や発話などの個人の癖などの動的な特徴を用いるもので利便性が高い。しかし、他人の模倣によって本人が拒否される可能性や、類似性の高い他人が居た場合の識別方法の確立が不可欠であることなど、改善すべき点も多い。

本研究では、身体的特徴の1つである、握りこぶしを用いて個人認証を行う。自然な状態で握りこぶしを作ると、人それぞれ握る強さや拳の大きさ、親指の位置などが異なり個人の特徴が現れやすい。そこでデブスカメラと RGB カメラの両方を内蔵した Intel 社の RealSense SR300 を用いて握りこぶしから特徴を抽出するシステムを構築する。

<sup>1</sup> 鹿児島大学院 理工学研究科  
Kagoshima University

RealSense を用いる利点として、軽量で必要な動作が少ない点や、デプスカメラに内蔵される赤外線センサを用いるため暗い場所でも用いることができる点が挙げられる。本論文では、取得した情報から特徴を抽出し、複数の処理にかけることで算出されるスコアを組み合わせることで個人認証をする手法を提案する。

## 2. 生体認証に関する関連研究

### 2.1 掌形認証

手を撮影した画像を用いて個人認証を行う研究がある。掌の面積や幅、全体の周囲の長さなど多くの特徴を用いる。西田らの研究では、本人拒否率 30.0%，他人受入率 0.29% という結果を得ている [9]。この研究では多くの特徴を用いているため、特徴量の最適化を行い、本人拒否率を下げることが必要である。

### 2.2 ペンの持ち方特徴による認証

ペンの持ち方に注目し、その様子をカメラで撮影した画像を用いて個人認証を行う研究がある。この研究では、ペンの持ち方やペン自体の向きなどの多数の特徴を抽出し認証を行う。村松らの研究では、特徴から非類似度を統合することで認証しており、他人の握り方を真似した成りすまし攻撃に対して誤り率 4.1% を得ている [7]。また、田中らの研究では、Microsoft 社の Kinect を用いて、動画像と取得した点群から個人認証を行っており、等価エラー率 (Equal Error Rate:EER) は 14.3% を得ている [8]。しかし、これらはペンを持つ必要があり、また処理時間も掛かる。

### 2.3 握りこぶしの全周囲画像を用いた個人認証

本研究の先行研究として渡邊らが、握りこぶしの 5 視点画像を全周囲画像として個人認証を行う研究を行っている [1]。撮影画像に対し、AKAZE 特徴点マッチングや、本論文でも後述するプロフィールマッチング、特徴線マッチングといった手法を適用し、それぞれのスコアの組み合わせにより個人認証を行っている。この手法は、2次元の画像処理を基に精度検証を行っており、EER=8.6% という精度を出している。しかしながら、この研究では実験の際に特殊な環境構築 (図 1, 2) が必要である。本研究はこの手法に RealSense から得た 3次元情報を付加した認証方法を検証すると同時に、特殊な環境に依存しない実験環境の小規模化も行う。

## 3. RealSense を用いた握りこぶしによる個人認証システム

### 3.1 撮影環境

本研究では、握りこぶしの撮影に RGB カメラとデプスカメラの両方で撮影する必要があるため、両方を内蔵している Intel 社の RealSense SR300 を用いた (図 3)。

撮影する際には、RealSense から手を 300mm 離れた所に置いてもらい距離を一定にする。カメラからの距離を正確にするために、RGB カメラとデプスカメラの映像を同時に表示し、カメラから近傍点までの距離をデプスカメラの映像上に表示する。また、RGB カメラとデプスカメラの撮影範囲を一致させるため、デプスカメラの映像上に矩形を描写し、その範囲内に手を配置してもらい、撮影を行う。

### 3.2 深度センサを用いた 3次元情報の計測

ここでは RealSense に内蔵する深度センサを用いて、握りこぶしの 3次元情報を計測する方法について述べる。この 3次元情報は後述する個人認証の特徴量の 1つとして用いる。

RealSense の API (Application Programming Interface) には、手のジェスチャの検出機能や、指の関節点の座標の取得機能などがある。本研究ではこれらを組み合わせることで、手の 3次元情報を取得する。

#### 3.2.1 ジェスチャ検出

RealSense を用いてジェスチャ検出を行う。はじめから手の座標を取得しても良いが、握りこぶしのジェスチャを検出した方がデータの正確さが増すと考えたためである。また、座標を取得する際に、急に握りこぶしをかざすとオ

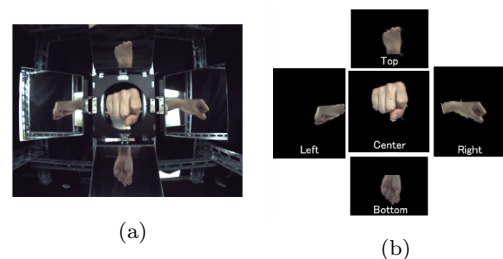


図 1 (a) 全周囲撮影画像 (b) 注目領域の抽出

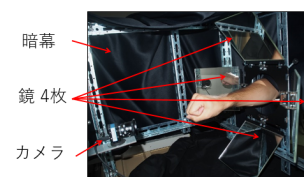


図 2 撮影環境



図 3 撮影環境 (a) RealSense 本体 (b) 撮影風景

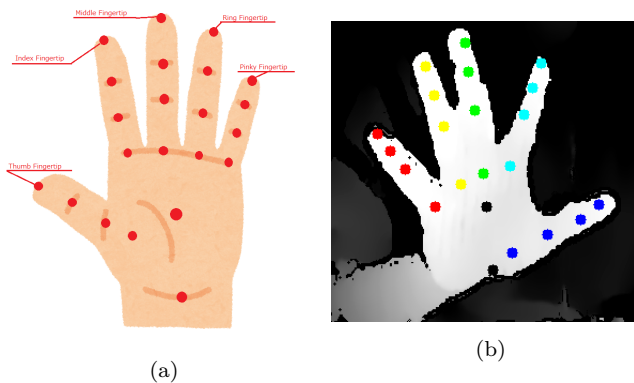


図 4 RealSense による関節点の取得 (a) 関節点 22 点 (b) 実際に取得した 22 点

クルージョンが発生するため、正確な座標が取得できない場合がある。これを解決するために、手を開いた状態から握っている状態への遷移を撮影する。

処理内容としては、手のひらのジェスチャを検出すると、自動で握りこぶしのジェスチャを検出する状態に切り替わり、次に握りこぶしを検出すると終了する。

### 3.2.2 関節点座標の類似度

ジェスチャ検出と同時に、手の指の関節点座標の取得も行う。取得する点はそれぞれの指から 4 点、そして手の重心点と手首の位置の点の合わせて 22 点で、それぞれ XYZ 座標を取得する。図 4 に関節点 22 点の位置を示す。

取得した 22 点の XYZ 座標それぞれを 1 次元のデータ配列とみなして、 $22 \times 3$  のデータを作成し、他の手のデータとの類似度を計算する。この類似度は後述する個人認証の特徴の 1 つとして用いる。

類似度の計算には以下の計算式 (1) を用いる。

$$score = \frac{\sum(x - \bar{x})(y - \bar{y})}{\sqrt{\sum(x - \bar{x})^2 \sum(y - \bar{y})^2}}. \quad (1)$$

### 3.3 プロフィールマッチング

本研究では、先行研究 [1] でも用いたプロフィールマッチングを行う。これは登録画像と入力画像から Y 軸方向・X 軸方向に対してそれぞれ画素値の総和を求め (図 5, 6), この和のデータをプロフィールとする。このデータを時系列データとみなし、DP マッチング [2] を行う。DP マッチングとは、参照データと入力データのデータ系列がどれほど類似しているかを数値化する手法である。DP マッチングの算出結果はパターン間の最適距離 0 以上となるため、式 (2) にパターン間の最適距離を distance として代入し、評価値を算出する。ただし、c は正規化のための任意の値とする。

$$score = \exp\left(\frac{1 \times distance^2}{2 \times c^2}\right). \quad (2)$$

### 3.4 特徴線マッチング

プロフィールマッチングと同様に特徴線マッチングも

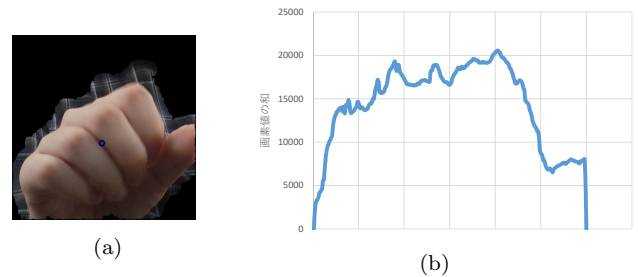


図 5 プロフィールマッチング (a)Y 軸方向 (b) 画素値の和

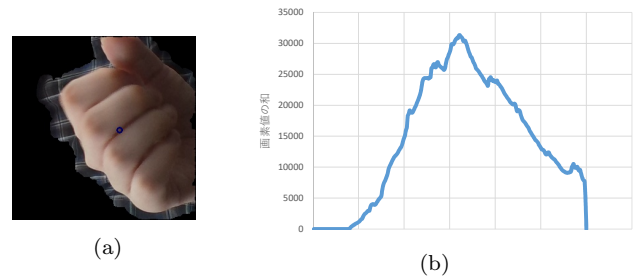


図 6 プロフィールマッチング (a)X 軸方向 (b) 画素値の和

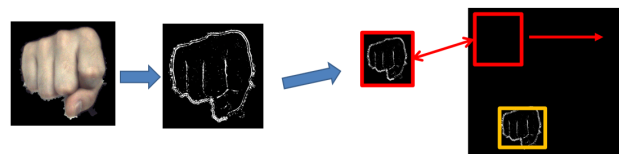


図 7 特徴線マッチング

行う (図 7)。特徴線マッチングでは、LoG(Laplacian of Gaussian) フィルタを用いてエッジ検出を行う。ラプラシアンフィルタは 2 次微分と同様の働きをし、値が急激に変化する画素がエッジに相当する。しかし、2 次微分であるためノイズが強調されてしまう。これを解決するために予めガウシアンフィルタをかけて平滑化した後にラプラシアンフィルタをかける LoG フィルタを用いた。

まず登録画像と入力画像の注目領域に LoG フィルタをかけ、2 値化画像を作成する。閾値は 80 で固定した。入力画像の 2 値化画像を X 軸に -5 から 1 ピクセルずつ 5 ピクセルまで平行移動し、これを Y 軸にも同様に行う。登録画像と平行移動後の入力画像を比較していく。ピクセル毎に論理積 (AND) を取り、エッジに相当する白画素の重複画素数をカウントする。白画素の重複画素数を正規化するために、ピクセル毎に論理和 (OR) を取った数を分母に、白画素の重複画素数を分子に取り、重複率を算出する (式 3)。平行移動の振れ幅が 10 ピクセルずつであるため、100 個の重複率を算出できるが、この中で重複率の高い順に 5 つを取り、この値をマッチングの評価値とする。

$$F = \frac{\text{重なるピクセル数}}{\text{登録画像白ピクセル} \vee \text{入力画像白ピクセル}}. \quad (3)$$

### 3.5 スコアの組み合わせによる個人認証

RealSense で取得した点の類似度、プロフィールマッチング、特徴線マッチングの 3 つの評価値に条件や閾値を設

け、それぞれ組み合わせることで個人認証する手法を構築する。本論文では、RealSense から得た各点座標 XYZ の類似度の平均を R(平均)、総積を R(総積)、X 軸方向・Y 軸方向のプロフィールマッチングスコアの平均を P(平均)、総積を P(総積)、特徴線マッチングで取得した重複率の高い 5 つのスコアの平均を F(平均)、総積を F(総積) として、これらの組み合わせで個人認証する。

#### 4. 特異値分解を用いた ICP アルゴリズム

本節では、前述した RealSense から取得した関節点 22 点を ICP アルゴリズム [6] に適用することで、2 つのデータの類似度を計算する。

類似度の計算に用いる 2 つの手のデータはそれぞれの対応が既知のため、特異値分解 (Singular Value Decomposition:SVD) を利用する。特異値分解とは、ある行列を特別な行列に分解する線形代数の方法の 1 つである。

処理手順について述べる。まずはじめにそれぞれの点群の重心を計算し、それぞれの点の座標を重心中心に変換する。次に座標行列を互いに掛け合わせた行列  $W$  を特異値分解する (式 (4))。特異値分解によって得られた行列  $U$  と行列  $V$  を用いて、それぞれの点のノルム誤差を最小にする並進行列  $t$  と回転行列  $R$  を式 (5) より求める。ただし、 $\mu_x$  と  $\mu_p$  はそれぞれの点群の重心座標を示す。

$$W = U \sum V^T. \quad (4)$$

$$R = UV^T, t = \mu_x - R\mu_p. \quad (5)$$

収束判定値と最大反復回数を指定し、収束するまで上記の処理を繰り返す。本研究では 1 つの点群がもう一方の点群に移動する際の推定移動量・変化量を求め、2 つのデータの類似度を検討する。

#### 5. 握りこぶし計測実験

実験には協力者 7 人、一人当たり 10 回分の握りこぶしを撮影し、個人認証に用いるために総当たりで比較する。実験では、同じ照明環境下で楽な姿勢から手をカメラに向けてもらう。握り方には個性を持たせるため敢えて特別な指示は出していない。次節からは、それぞれのシステムにおけるスコアと認証精度を記し、最後にすべてのスコアの組み合わせによる本システム全体の認証精度を記す。

RealSense を用いて握りこぶしを撮影し、3 次元情報と握りこぶし画像を取得する。得た情報に第 3.2 項で記した処理をかけることでスコアを算出した。スコアの分布図を図 8, 9 に示す。

取得画像から注目領域を抽出し、第 3.3 項で記した処理をかけ、総当たりのマッチングスコアを求めた。スコアの分布図を図 10, 11 に示す。

プロフィールマッチングと同様に、第 3.4 項で記した処理をかけ、総当たりでマッチングスコアを求めた。スコア

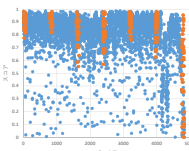


図 8 R(平均) スコア分布

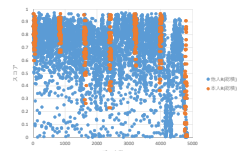


図 9 R(総積) スコア分布

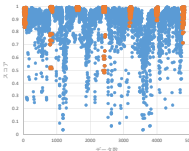


図 10 P(平均) スコア分布

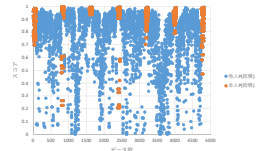


図 11 P(総積) スコア分布

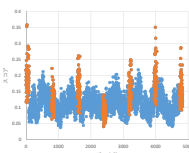


図 12 F(平均) スコア分布

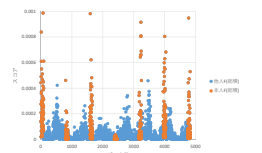


図 13 F(総積) スコア分布

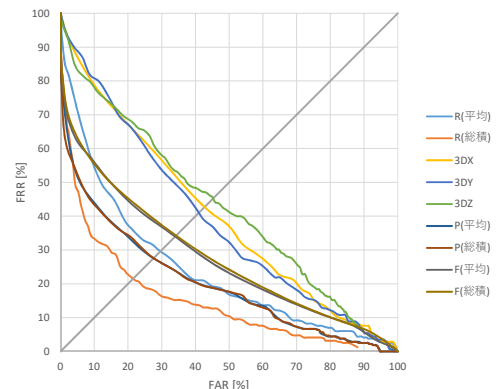


図 14 DET カーブ

の分布図を図 12, 13 に示す。

##### 5.1 それぞれのマッチングスコア

求めたスコアの結果と 0 から 1 などの範囲で設けた閾値を比較することで本人拒否率 (False Rejection Rate:FRR) と他人受入率 (False Acceptance Rate:FAR) の変動を求め、FRR を縦軸に、FAR を横軸にとった DET (Decision Error Tradeoff) カーブを図 14 に示す。FRR=FAR の直線とそれぞれの DET カーブの交点が等価エラー率 (Equal Error Rate:EER) である。EER は認証技術の精度の目安であり、この値が小さいほど精度が高い。図 14 から、システム単体での EER はそれぞれ表 1 の通りである。単体では R(総積) での値が一番よく、21.9%であった。

##### 5.2 スコアの組み合わせによる個人認証

求めたスコアの結果をもとに、閾値や条件を設けて組み合わせることで個人認証方法を構築する。閾値には等誤り率 (Crossover Error Rate:CER) と呼ばれる、FRR と FAR

表 1 単体での EER(%)

スコア名	EER(%)	スコア名	(%)
R(平均)	29.8	R(総積)	21.9
P(平均)	24.4	P(総積)	28.3
F(平均)	34.8	F(総積)	33.3

表 2 閾値 CER

スコア名	閾値	スコア名	閾値
R(平均)	0.83	R(総積)	0.625
P(平均)	0.95	P(総積)	0.9
F(平均)	0.12	F(総積)	2.29E-05

表 3 閾値 CER

組合せ	本人拒否率 (%)	他人受入率 (%)
R(平均) $\wedge$ P(平均) $\wedge$ F(平均)	63.3	2.2
{R(平均) $\vee$ P(平均)} $\wedge$ F(平均)	40.8	13.8
{R(平均) $\wedge$ P(平均)} $\vee$ F(平均)	21.6	38.6
R(平均) $\vee$ P(平均) $\vee$ F(平均)	2.5	66.9
{P(平均) $\vee$ F(平均)} $\wedge$ R(平均)	37.9	15.1
{P(平均) $\wedge$ F(平均)} $\vee$ R(平均)	19.5	33.7
R(総積) $\wedge$ P(総積) $\wedge$ F(総積)	59.4	1.4
{R(総積) $\vee$ P(総積)} $\wedge$ F(総積)	41.0	11.6
{R(総積) $\wedge$ P(総積)} $\vee$ F(総積)	18.6	36.8
R(総積) $\vee$ P(総積) $\vee$ F(総積)	2.1	63.0
{P(総積) $\vee$ F(総積)} $\wedge$ R(総積)	30.3	11.2
{P(総積) $\wedge$ F(総積)} $\vee$ R(総積)	14.8	26.5

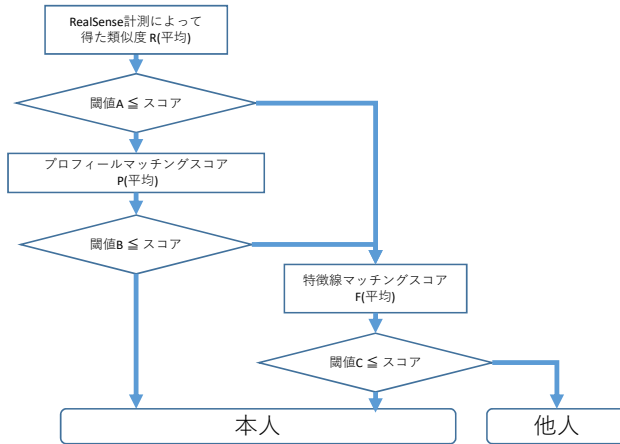


図 15 組合せ例

が等しいときの値を用いる。本論文では下記のような組み合わせで検証を行った。それぞれの組み合わせにおいて用いた閾値 CER を表 2 に、組み合わせ方法例を図 15 に示す。

- R(平均)  $\wedge$  P(平均)  $\wedge$  F(平均)
- {R(平均)  $\vee$  P(平均)}  $\wedge$  F(平均)
- {R(平均)  $\wedge$  P(平均)}  $\vee$  F(平均) (図 15)
- R(平均)  $\vee$  P(平均)  $\vee$  F(平均)
- {P(平均)  $\vee$  F(平均)}  $\wedge$  R(平均)
- {P(平均)  $\wedge$  F(平均)}  $\vee$  R(平均)
- R(総積)  $\wedge$  P(総積)  $\wedge$  F(総積)
- {R(総積)  $\vee$  P(総積)}  $\wedge$  F(総積)
- {R(総積)  $\wedge$  P(総積)}  $\vee$  F(総積)
- R(総積)  $\vee$  P(総積)  $\vee$  F(総積)
- {P(総積)  $\vee$  F(総積)}  $\wedge$  R(総積)
- {P(総積)  $\wedge$  F(総積)}  $\vee$  R(総積)

### 5.2.1 認証精度

組合せによって求めた認証精度を表 3 に示す。表 3 の結果から、本論文で良い値を示した組み合わせは {P(総積)  $\wedge$  F(総積)}  $\vee$  R(総積) で、本人拒否率 14.8%，他人受入率 26.5% であった。

## 6. ICP マッチングによる認証実験

スコアの組み合わせによる認証方法とは別に、ICP アル

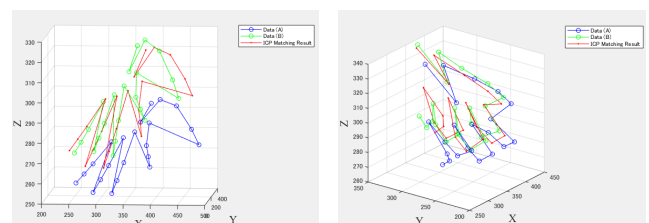
ゴリズムを用いたマッチング結果による個人認証方法について述べる。本論文では、点群 A に対して点群 B がマッチングするまでの総移動量 (x[mm] y[mm] z[mm] deg) を用いて認証する方法を検証する。これは他人の手形状とマッチングを行う際に点群の移動量および変化量が多くなると考えたためである。

### 6.1 実データによる ICP マッチング

実験には協力者 7 人、それぞれ手を開いた状態と閉じた状態の 2 種類のデータを RealSense を用いて 10 回ずつ撮影し、毎回関節点 22 点を取得する。それぞれの 22 点分の点群を総組合せで ICP マッチングし、初期位置からの移動距離と回転角度を計算する。その結果の絶対値を取り、10 から 200 までの移動値の閾値を設定し DET カーブを用いて精度の確認を行った。ICP マッチングの処理結果例を図 16 に示す。青が入力点群 1、緑が比較する点群 2、赤が青を緑に重ね合わせるための移動・変換を終えた後の処理結果である。

### 6.2 認証精度

図 17 に ICP による認証精度を表す DET カーブを示す。手を開いた (手のひら) 状態では EER=19.4%，手を握った (握りこぶし) 状態では EER=26.2% という結果を得られた。また処理時間は手のひらが 4588.97 秒、握りこぶしが 7200.85 秒かかった。1 つの組み合わせに 1 秒前後かかっていることがわかる。



(a)

(b)

図 16 ICP マッチングの結果 (a) 手のひら (b) 握りこぶし

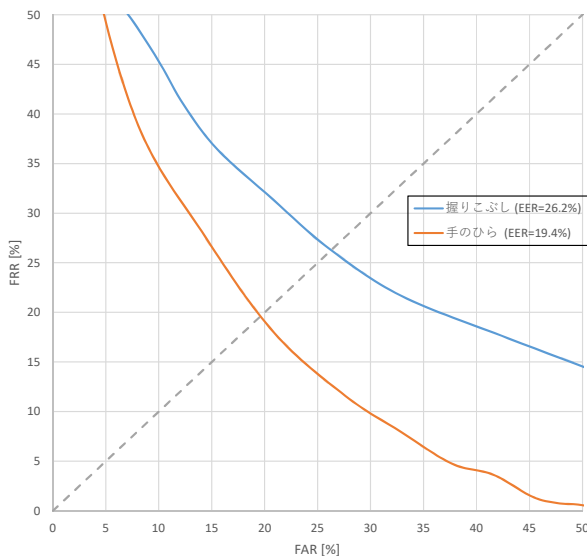


図 17 DET カーブ

## 7. 考察

本研究で試した組み合わせの中では、 $\{P(\text{総積}) \vee R(\text{総積})\} \vee F(\text{総積})$  の組み合わせの認証精度が一番良かった。しかし、他の認証の研究や先行研究の結果と比較すると精度は未だ十分とはいえない。主な原因として、環境変化による画像の輝度値の変化や、RealSense の計測精度に依存しているシステム上の問題が挙げられる。

また、ICP マッチングを用いた認証方法では、手のひらの状態の点群を用いた方が 6.8%精度が高い結果となった。これは用いた点群が統一性の無い不規則なもので、手のひらの方が若干の平面性があるためと考えられる。

## 8. 結論

本論文では、新しいセキュリティ対策手法として、RealSense から握りこぶしの 3 次元情報を取得する環境の構築と、その情報を用いた個人認証方法を考案し、渡邊ら [1] が反省点として挙げていたシステムの軽量化・小規模化も行った。実験協力者 7 人、1 人あたり 10 枚分の握りこぶしを利用した実験を行い、 $\{P(\text{総積}) \wedge F(\text{総積})\} \vee R(\text{総積})$  とスコアの組み合わせにおいて、本人拒否率 14.8%，他人受入率 26.5% という結果が得られた。また、握りこぶしの 3 次元点群を用いた ICP マッチングによる個人認証方法では、手のひらで EER=19.4%，握りこぶしで EER=26.2% という結果が得られた。

今後の課題として、計測データの精度向上、それに基づくそれぞれの認証精度の向上、データ数を増やした場合の精度検証、経時変化でのロバスト性の検証が挙げられる。特に計測データの精度は本システム全体に影響するため、より正確なデータを取得するアルゴリズムの開発や環境

構築が重要である。具体的には、RealSense の認識依存になっているジェスチャ検出に、正確な握りこぶしを認識するアルゴリズムの組み込みや、対応点を中心とした点群位置合わせへの改良などが挙げられる。

## 参考文献

- [1] 渡邊太一, 福元伸也, 鹿嶋雅之, 佐藤公則, 渡邊睦: 握りこぶしの全周囲画像を用いた個人認証に関する研究 (バイオメトリクス), 電子情報通信学会技術研究報告, 電子情報通信学会 (2017).
- [2] 内田誠一: DP マッチング概説: 基本と様々な拡張, 電子情報通信学会技術研究報告, PRMU(2006).
- [3] 佐藤公則, 大野敬弘, 鹿嶋雅之, 渡邊睦: 手の形状を利用した非接触型セキュリティキー入力システムの開発, 画像電子学会誌 (2009).
- [4] Carfagni et al: On the performance of the Intel SR300 depth camera: metrological and critical characterization, IEEE Sensors Journal(2017).
- [5] De Smedt et al: SHREC'17 Track: 3D Hand Gesture Recognition Using a Depth and Skeletal Dataset, 10th Eurographics Workshop on 3D Object Retrieval(2017).
- [6] Rusinkiewicz, Szymon and Levoy, Marc: Efficient variants of the ICP algorithm, 3-D Digital Imaging and Modeling(2001).
- [7] 村松大吾, 阿部貢士, 堀内翔, 小方博之: ペン持ち方情報をを用いたバイオメトリック個人認証, 電子情報通信学会論文誌 (2009).
- [8] 田中緑, 中井満: 筆記中の手の深度動画像を用いた個人認証, バイオメトリクスと認識・認証シンポジウム (2017).
- [9] 西田隆: 掌形画像を用いた個人認証システムの開発, 電子情報通信学会総合大会講演論文集 (2009).
- [10] 福田京四朗, 南谷崇成, 崔英泰, 渡部大志: SHOT を利用した 3D 耳介認証の試み, 電子情報通信学会技術研究報告 (2017).
- [11] 渡部大志, 黄しちゅう, 相馬貢士, 崔英泰, 酒井勝弘, 中村納: 1 枚の登録画像による耳介認証の平面外回転へのロバスト化, 映像情報メディア学会誌 (2011).
- [12] 橋本学: 物体認識のための 3 次元特徴量の基礎と動向, ビジョン技術の実利用ワークショップ (2014).
- [13] Intel:Hand Tracking Tutorial
- [14] 増田健: ICP アルゴリズム, 研究報告コンピュータビジョンとイメージメディア (2009).