

圧力センサを用いた把持ジェスチャによる 携帯端末の個人認証手法

飛世速光¹ 村尾和哉² 寺田 努^{1,3} 磯 俊樹⁴ 塚本昌彦¹ 堀越 力⁴

概要：スマートフォンやタブレットなどの携帯端末には電話番号やメールアドレスなどの個人情報が保存されており、その携帯性から紛失や盗難する機会も多いため、特定の個人のみで端末の利用を制限する個人認証が必要となる。広く普及している個人認証手法として、パスワードやなぞるパターン、顔認証、指紋認証などが挙げられるが、片手での画面操作が煩雑であったり、ショルダーハッキングに脆弱、顔写真や指紋を入手すれば容易に認証可能であるという問題がある。そこで、煩雑な操作を必要とせず、安全性の高い個人認証手法として、圧力センサを用いた把持ジェスチャによる個人認証手法を提案する。把持ジェスチャは行動的特徴の一種であり、携帯端末を操作する際の端末を握る動作のことである。把持ジェスチャは携帯端末の操作中に自然に行えるジェスチャであり、セキュリティロックの解除に煩雑な操作を必要としない。また、把持ジェスチャは指の力の入れ具合で区別されるため、盗み見ることは困難であり、第三者による把持ジェスチャの再現性は低く、セキュリティロックの安全性も高いと考える。本研究では、携帯端末の側面に搭載した圧力センサアレイを用いて、ユーザの把持ジェスチャの把持力の分布を測定して個人認証を行うシステムを構築した。提案システムの評価実験の結果、本人が自由に設定したジェスチャで認証を行う場合で EER が最低 0.02 となり、提案システムが有効であることが確かめられた。

1. はじめに

近年、技術の発展と共にスマートフォンやタブレットといった高機能な携帯端末が広く普及してきている。それに伴い、携帯端末には多くの重要な情報が記憶されるようになり、悪意のあるユーザから情報を保護する必要性が年々高まっている。現在、携帯端末内の情報を保護する手法として、文字列パスワードによる個人認証が広く用いられている。この認証手法は、文字列の組み合わせ数の大きさが安全性の根拠となっているが、一般的な携帯端末用 OS のパスワードは 10 進数 4 桁と短い。理論上は一万通りの組合せが存在するが、生年月日や電話番号といったユーザの個人情報に関するパスワードや、「0000」や「1234」などの単純なパスワードは第三者によって推定されやすく、また、覗き見によって漏えいしやすいため、実際の安全性が高いとは言えない。一方、長く複雑で、ユーザが覚えにくいパスワードは、忘却や誤入力によりセキュリティロックが解除できなかったり、入力操作に時間を要するなど、安全性を高める一方でユーザビリティの低下を招く。

パスワードを用いる方法以外の個人認証方法として、指紋や声紋、眼球の虹彩などの身体的特徴から個人認証を行う方法や、ジェスチャや筆跡などの行動的特徴から個人認証を行う方法がある。身体的特徴を用いた認証はユーザ固有の情報であるため、パスワードや行動的特徴を用いた認証より安全性が高く、忘却することもなくセキュリティロックの解除操作も容易である。しかし、身体的特徴による個人認証は、身体的特徴の経年変化によって認証が出来なくなったり、複製によって破られたりする危険性がある。身体的特徴はユーザ固有の情報であり、パスワードのようにユーザの意思で変更できないため、一度でも複製されるとセキュリティロックの安全性を長期間回復できないといった致命的な問題も生じる。一方、行動的特徴は自由度の高さから他人が真似しづらいため安全性が高いと考えられる。しかしながら、既存の行動的特徴であるジェスチャは腕を振るなどの動作で認証するため広い空間が必要であり、公共空間で行うには周囲の人々の注目を集めるため敷居が高い。また、筆跡は両手を用いて文字などを描く必要があり、煩雑な操作が必要となる。

そこで本研究では、煩雑な操作を必要とせず、安全性の高い個人認証手法として、圧力センサを用いた把持ジェスチャによる個人認証手法を提案する。把持ジェスチャは行動的特徴の一種であり、携帯端末を操作する際の端末を握

¹ 神戸大学大学院工学研究科

² 立命館大学情報理工学部

³ 科学技術振興機構さきがけ

⁴ NTT ドコモ 先進技術研究所

る動作のことである。多くのユーザは端末を把持するため、把持ジェスチャは携帯端末の操作中に自然に行えるジェスチャであり、セキュリティロックの解除に煩雑な操作を必要としないと考えられる。例えば、携帯端末を鞆やポケット等から取り出す際、取り出し動作と同時に把持ジェスチャを行うだけで端末のセキュリティロックを解除でき、スムーズに携帯端末を利用できる。また、把持ジェスチャによるユーザの手の動きは非常に細かいため、どのようなジェスチャを行っているかは第三者から分かりづらく、セキュリティロックの安全性も高いと考える。本研究では、携帯端末の側面に搭載した圧力センサアレイを用いて、ユーザが把持ジェスチャを行った際の把持力の分布を測定して個人認証を行うシステムを構築し、把持ジェスチャによる個人認証の特性を評価した。

以下、2章で関連研究について述べ、3章で提案システムについて説明する。4章で提案手法の特性を評価する実験について述べ、最後に5章で本研究のまとめを行う。

2. 関連研究

行動的特徴から個人認証を行う手法として、Webカメラを入力媒体として指先をトラッキングし、認識した筆跡を用いることで個人認証を行う手法 [1] がある。この手法では、認証に用いる文字を何度でも変更できるため、複製された際に安全性が著しく低下するという生体認証の課題を解決しているが、Webカメラを用いているため携帯端末への応用は難しいと考えられる。携帯端末に搭載された加速度センサを用いて端末自体の動きを認識して個人認証を行う研究 [2] では、低いFRR(False Rejection Rate:本人拒否率)と高いFAR(False Acceptance Rate:他人許容率)をもつシステムを構築している。しかしこのシステムの評価実験は、振動のない安定した場所でユーザが静止しているといった環境で行われており、歩行時や電車やバスへの乗車時といった実環境で利用する際、加速度センサにユーザの意図しない加速度が多く加わることが想定され、実環境での利用は現実的でないと考えられる。携帯端末に搭載された静電容量式のタッチセンサを用いて、端末の把持パターンを認識する研究 [3,4] では、携帯端末に搭載されたカメラで写真を撮る場面、片手でメールを打つ場面など、数種類の場面での把持パターンを認識し、対応するアプリケーションを起動しているが、これらの研究で構築されたシステムでは認識する把持パターンが最大8種類と少ない。また、ユーザ間の差異を考慮していないため、異なる人物が行った同じ握り方を区別できるか不明であり、個人認証には向いていないと考えられる。圧力センサを用いた拳サイズのデバイスによって個人認証を行うシステム [5] では、把握動作を用いた高精度な個人認証を実現しているが、このシステムを携帯端末の個人認証に用いるためには、認証用のデバイスを携帯端末とは別に用意しなければならない



図1 圧力センサを搭載した携帯端末



図2 圧力センサアレイ [7]

ため、現実的ではない。また、圧力分布センサを搭載したWiiリモコンを用いて、PCの個人認証を行うシステム [6] では、自然な把持動作による個人認証が可能であるが、用いているデバイスは細長いWiiリモコンであり、把持動作も携帯端末とは異なるため、携帯端末での個人認証に用いることができるかどうかは明らかでない。また、このシステムでは、安定させて動作させるために20サンプル以上の学習データが必要であり、学習に手間がかかる。また、自然な把持動作以外の把持ジェスチャを行った場合には評価していない。携帯端末に搭載された圧力センサを用いて、通常の端末操作時の把持力を測定し、個人認証を行うシステム [7] では、特別な操作を必要とせず、通常の端末操作時のユーザの把持力特徴から個人認証が可能であるが、認証が終了するまで数十秒かかってしまう。本研究では、このシステムで用いたデバイスを利用して、パスワードを入力する要領で携帯端末を握るジェスチャを行い、その把持ジェスチャを事前に本人が登録した正解データと比較することで、スムーズで高精度な携帯端末の個人認証が可能なシステムの構築を目指す。

3. 提案システム

本章では圧力センサを用いて把持ジェスチャの圧力分布を取得することで個人認証を行うシステムについて述べる。

3.1 想定環境

本研究では図1に示すように、圧力センサアレイを携帯電話の左右両側面と背面の左右両端に搭載した携帯電話端

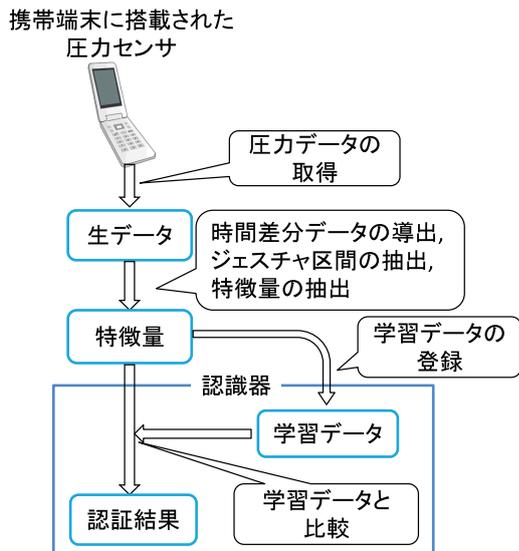


図 3 提案システムの構成

末を用いる [7]. 使用する圧力センサアレイは図 2 に示す $2.5 \times 2.5(\text{mm})$ の小さなタイル状のものであり、高い空間分解能をもつ。センサ数は合計 226 個で、全てのセンサはゴムで覆われている。センサの測定レンジは $0 \sim 100(\text{kPa})$ 、分解能は $0.024(\text{kPa})$ 、サンプリングレートは $10(\text{Hz})$ であり、各センサの圧力値は携帯端末本体の記憶領域に保存される。本携帯端末の仕様上、リアルタイムに直接外部にセンサデータを出力できないため、本研究では一旦端末に保存されたデータを PC に取り込んでから認証処理を行う。

また本研究では、携帯端末を手にとって、通常のロック解除作業を行うタイミングで把持ジェスチャを行って認証する環境を想定しているため、認証用のジェスチャは数秒程度の片手で行えるものとする。

3.2 個人認証処理

図 3 に提案システムの構成を示す。提案システムの処理は以下に示す 5 段階から成り、本節ではそれぞれの処理方法について述べる。

- (1) 圧力データの取得
- (2) 時間差分データの導出
- (3) ジェスチャ区間の抽出
- (4) 特徴量の抽出とデータ間距離の算出
- (5) 認証判定

3.2.1 圧力データの取得

端末に搭載された圧力センサアレイを用いてユーザの把持ジェスチャ中の圧力を計測する。圧力センサアレイから得られるデータをグレースケールで表したものを図 4 に示す。図 4 は、人差し指から小指までの 4 本の指で人差し指側から順番に握る把持ジェスチャを行った時の圧力値であり、縦軸がサンプリング番号 (サンプリング時刻)、横軸がセンサ番号を表しており、握って圧力が加わっている部分が白くなっている。このように、226 次元の圧力値を 1 サ

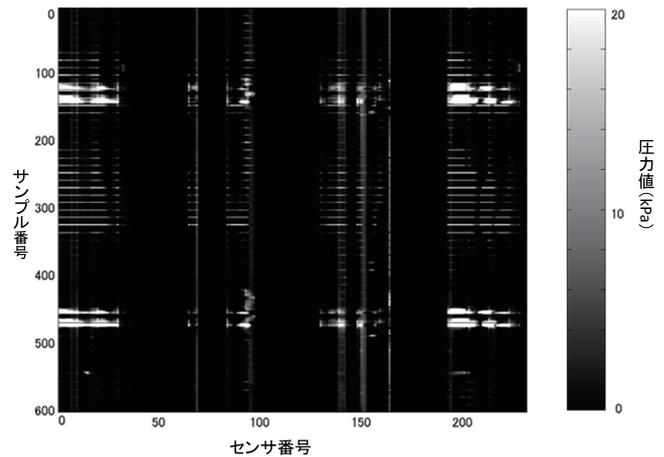


図 4 圧力センサアレイから得られるデータ

ンプルとしたデータが取得できる。

3.2.2 時間差分データの導出

本研究で用いている圧力センサは柔らかく、センサに歪みが生じて、握っていない時も圧力値が出力されるなど、加えられた把持圧力に対する出力値が一定でないことがあるため、生の圧力値ではなく時間差分値を用いる。時間差分値を用いることでセンサの歪みによる影響を緩和している。 N 個の圧力センサから時刻 t に取得した生の圧力値を $\mathbf{F}(t) = (f_1(t), f_2(t), \dots, f_N(t))^T$ とする。ただし、 $f_i(t)$ ($1 \leq i \leq N$) は i 番目の圧力センサの値であり、 $(\bullet)^T$ は (\bullet) の転置行列である。時間差分値 $\mathbf{G}(t) = (g_1(t), g_2(t), \dots, g_N(t))^T$ を以下の手順に従って導出する。

$$\mathbf{G}(t) = \mathbf{F}(t) - \mathbf{F}(t-1) \quad (1)$$

3.2.3 ジェスチャ区間の抽出

取得した圧力データにはユーザが把持していない部分や力を入れていない部分のデータが含まれているため、ユーザが把持ジェスチャを行っている区間のデータを抽出する必要がある。提案手法では、ある値以上の圧力値を示しているセンサ数が設定した閾値を超えた場合、ジェスチャが開始されたと判断する。また、ジェスチャ開始後一定時間が経過したのち、ある値以上の圧力値を示しているセンサ数が設定した閾値を下回った場合、ジェスチャが終了したと判断する。具体的なアルゴリズムを以下に示す。

まず、 N 個の圧力センサから時刻 t に取得した圧力値の時間差分値 $\mathbf{G}(t) = (g_1(t), g_2(t), \dots, g_N(t))^T$ のうち、 $|g_i(t)| > g_{Th}$ ($1 \leq i \leq N$) を満たすセンサの個数 N' を求める。ただし、 $g_i(t)$ は時刻 t におけるセンサ番号 i の圧力値の時間差分値、 g_{Th} はあらかじめ設定した圧力値の時間差分値の閾値であり、 $g_{Th} = 10(\text{kPa})$ である。この値は予備実験より決定した。また、 N は圧力センサの数で本研究では $N = 226$ である。 N' はサンプリングのたびに導出され、次のようにジェスチャ区間の抽出の開始と終了を判断する。

(1) データ抽出開始条件

N' と閾値 N_{Th} を比較し、 $N' \geq N_{Th}$ の場合、データの抽出を開始する。このとき、抽出開始時刻 $t = t_a$ を記録する。

(2) データ抽出終了条件

N' と閾値 N_{Th} を比較し、 $N' < N_{Th}$ の場合、 N' が $N' \geq N_{Th}$ から $N' < N_{Th}$ となった時刻を $t = t_b$ とする。抽出したデータの長さ（サンプル数） $A = t - t_a$ と、終了までの待機時間 $B = t - t_b + 1$ を計測する。 $N' < N_{Th}$ が満たされ続け、 $A > A_{Th}$ かつ $B > B_{Th}$ の場合、データの抽出を終了し、抽出したデータをデータセット $\mathbf{G} = (\mathbf{G}(t_a), \dots, \mathbf{G}(t))$ とする。 $N' \geq N_{Th}$ の場合、 t_b をリセットする。

A_{Th} および B_{Th} は、あらかじめ設定した A および B の閾値である。 A_{Th} は誤って端末を握ってしまった時に、極端に短い長さのデータセットを抽出してしまうことを防ぐために設定している。これによって十分な長さ A_{Th} 以上のデータを抽出できる。また、待機時間 B_{Th} はジェスチャ中に把持力が加わらなかった瞬間にデータの抽出が誤って終了してしまうことを防ぐために設定している。本研究では 10(Hz) でサンプリングを行っており、 $A_{Th}=10$ サンプル、 $B_{Th}=5$ サンプルとした。また、 N_{Th} は抽出の開始および終了のためのセンサ数の閾値であり、本研究では $N_{Th}=10$ とする。これらの値は予備実験により決定した。

3.2.4 特徴量の抽出とデータ間距離の算出

入力されたジェスチャデータ \mathbf{G} と本人の正解ジェスチャデータとの距離を算出するための特徴量を抽出する。本研究では把持ジェスチャを構成する要素として握る位置、握り方の時間変化（タイミング）、握る力の3種類があると考え、それらの組合せとして以下の4種類の特徴量を抽出した。特徴量の要素の組合せとして、「位置+タイミング」のように、「力」の要素を含まないものがない理由は、「力」の要素を含まなかった場合、圧力センサが触れているかどうかのみを識別するタッチパネルのように作用し、加わっている圧力値を取得できるという圧力センサの特性を活かせないと考えたためである。

- (a) 位置+タイミング+力
- (b) タイミング+力
- (c) 位置+力
- (d) 力

本節では各特徴量の説明および抽出方法とデータ間距離の計算方法を述べる。

(a) 位置+タイミング+力

本特徴量は抽出したデータセット \mathbf{G} をそのままデータ間距離の算出に用いる。したがって、端末を把持する位置、タイミングおよび加えられた把持力が類似しているジェスチャ間の距離が小さくなる。特徴量 \mathbf{Y} は $\mathbf{Y}(t) = \mathbf{G}(t)$ であり、

$$\begin{aligned} \mathbf{Y} &= (\mathbf{Y}(1), \mathbf{Y}(2), \dots, \mathbf{Y}(l)) \\ \mathbf{Y}(t) &= (g_1(t), g_2(t), \dots, g_N(t))^T \end{aligned} \quad (2)$$

となる。初期設定時に登録したジェスチャデータ（正解データ）Aの特徴量を $\mathbf{Y}_A = (\mathbf{Y}_A(1), \dots, \mathbf{Y}_A(l))$ 、認証時に行うジェスチャデータ（テストデータ）Bの特徴量を $\mathbf{Y}_B = (\mathbf{Y}_B(1), \dots, \mathbf{Y}_B(l))$ として、次式より \mathbf{Y}_A と \mathbf{Y}_B の距離 $d(\mathbf{Y}_A, \mathbf{Y}_B)$ を得る。

$$d(\mathbf{Y}_A, \mathbf{Y}_B) = \sum_{i=1}^l \|\mathbf{Y}_A(i) - \mathbf{Y}_B(i)\| \quad (3)$$

ただし、 l はジェスチャデータ A とジェスチャデータ B の長さを比較し、小さい方の値を用いる。 $\|\bullet\|$ はベクトル \bullet のユークリッドノルムである。

(b) タイミング+力

本特徴量は長さ l のジェスチャ区間における各時刻での N 個のセンサの圧力値のヒストグラム列を用いる。したがって、端末を把持するタイミングと加えられた把持力が類似しているジェスチャ間の距離が小さくなる。ヒストグラムの範囲を R 、階級数 K とすると、特徴量 \mathbf{Y} は

$$\begin{aligned} \mathbf{Y} &= (\mathbf{Y}(1), \mathbf{Y}(2), \dots, \mathbf{Y}(l)) \\ \mathbf{Y}(t) &= (y_1(t), y_2(t), \dots, y_K(t))^T \end{aligned} \quad (4)$$

となる。ただし、 $\mathbf{Y}(t)$ は時刻 t におけるヒストグラムであり、 $y_j(t)$ は階級 j の度数、階級の幅 H は $H = R/k$ である。正解データ A の特徴量を $\mathbf{Y}_A = (\mathbf{Y}_A(1), \dots, \mathbf{Y}_A(l))$ 、テストデータ B の特徴量を $\mathbf{Y}_B = (\mathbf{Y}_B(1), \dots, \mathbf{Y}_B(l))$ として、次式より \mathbf{Y}_A と \mathbf{Y}_B の距離 $d(\mathbf{Y}_A, \mathbf{Y}_B)$ を得る。

$$d(\mathbf{Y}_A, \mathbf{Y}_B) = \sum_{i=1}^l \|\mathbf{Y}_A(i) - \mathbf{Y}_B(i)\| \quad (5)$$

ただし、 l はジェスチャデータ A とジェスチャデータ B の長さを比較し、小さい方の値を用いる。

(c) 位置+力

本特徴量は N 個のセンサそれぞれにおけるジェスチャ区間の圧力値のヒストグラム列を用いる。したがって端末を把持する位置と加えられた把持力が類似しているジェスチャ間の距離が小さくなる。ヒストグラムの範囲を R 、階級数 K とすると、特徴量 \mathbf{Y} は

$$\begin{aligned} \mathbf{Y} &= (\mathbf{Y}(1), \mathbf{Y}(2), \dots, \mathbf{Y}(N)) \\ \mathbf{Y}(i) &= (y_1(i), y_2(i), \dots, y_K(i))^T \end{aligned} \quad (6)$$

となる。ただし、 $\mathbf{Y}(i)$ はセンサ i におけるヒストグラムであり、 $y_j(i)$ は階級 j の度数、階級の幅 H は $H = R/k$ である。正解データ A の特徴量を $\mathbf{Y}_A = (\mathbf{Y}_A(1), \dots, \mathbf{Y}_A(N))$ 、テストデータ B の特徴量を $\mathbf{Y}_B = (\mathbf{Y}_B(1), \dots, \mathbf{Y}_B(N))$ として、次式により \mathbf{Y}_A と \mathbf{Y}_B の距離 $d(\mathbf{Y}_A, \mathbf{Y}_B)$ を得る。

$$d(\mathbf{Y}_A, \mathbf{Y}_B) = \sum_{i=1}^N \|\mathbf{Y}_A(i) - \mathbf{Y}_B(i)\| \quad (7)$$

表 1 把持ジェスチャ

ジェスチャ名	動作
握る	人差し指から小指までの 4 本の指で 1 秒握る。
3 回握る	人差し指から小指までの 4 本の指で素早く 3 回握る。
波打ち (上, 抜)	人差し指から小指までの 4 本の指で人差し指側から順番に握る。次の指に力を入れる時、前の指の力は抜く。
波打ち (上, 入)	人差し指から小指までの 4 本の指で人差し指側から順番に握る。次の指に力を入れる時、前の指の力は入れたままにする。
波打ち (下, 抜)	人差し指から小指までの 4 本の指で小指側から順番に握る。次の指に力を入れる時、前の指の力は抜く。
波打ち (下, 入)	人差し指から小指までの 4 本の指で小指側から順番に握る。次の指に力を入れる時、前の指の力は入れたままにする。
上 2 本で握る	人差し指と中指で 1 秒握る。
下 2 本で握る	薬指と小指で 1 秒握る。
端 2 本で握る	人差し指と小指で 1 秒握る。
中 2 本で握る	中指と薬指で 1 秒握る。

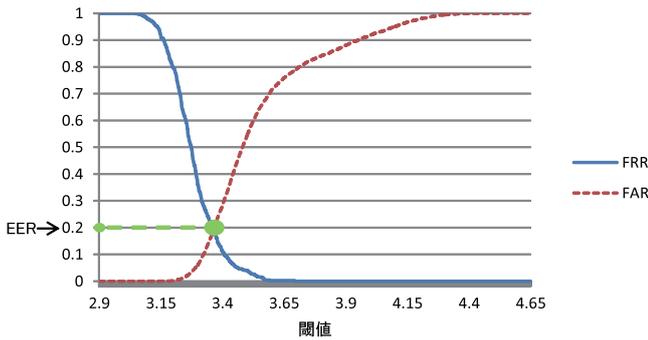


図 5 FRR-FAR 曲線と EER

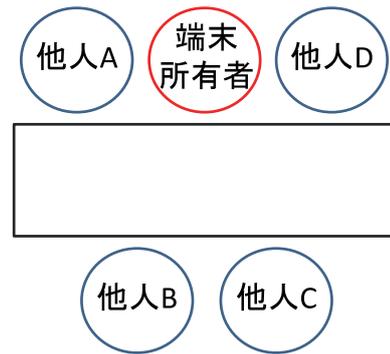


図 6 各被験者の位置関係

(d) 力

本特徴量は N 個のセンサのジェスチャ区間の値を足し合わせた値を用いる。したがって、ジェスチャ中に端末に加えられた全ての把持力が類似しているジェスチャ間の距離が小さくなる。特徴量を Y とおくと、

$$Y = \sum_{i=1}^L \sum_{j=1}^N |g_j(i)| \quad (8)$$

となる。ただし、 $g_j(i)$ は時刻 i におけるセンサ j の圧力値である。正解データ A の特徴量を Y_A 、テストデータ B の特徴量を Y_B として、次式より Y_A と Y_B の距離 $d(Y_A, Y_B)$ を得る

$$d(Y_A, Y_B) = |Y_A - Y_B| \quad (9)$$

3.2.5 認証判定

各特徴量から求められたデータ間距離 d と設定した閾値 d_{Th} を比較し、 $d < d_{Th}$ であれば受入、 $d \geq d_{Th}$ であれば拒否とする認証判定を行う。 d_{Th} を大きく設定すれば認証されやすくなるため、本人が正しく認証されるようになるが、同時に他人も認証されやすくなる。一方 d_{Th} を小さく設定すれば認証されにくくなるため、他人の認証を拒否しやすくなるが、本人の認証も拒否されやすくなる。このように d_{Th} の値によって認証性能を制御できる。

4. 評価実験

提案する個人認証手法の性能を評価するために実験を

行った。実験は認証ジェスチャを自由に設定する場合を想定して行った。

本人は自分で設定したジェスチャで認証を行い、他人は認証動作を見て、それを真似することで認証を試みる環境でシステムの評価を行う。

4.1 実験の手続き

図 6 に示すように 20 代の男性 5 名が机の周りに並んだ椅子に座り、そのうち 1 名が端末の所有者としてあらかじめ自由に設定した把持ジェスチャで認証動作を 5 回行った。他の 4 名は認証の様子を見て、本人のジェスチャを真似した把持ジェスチャを 5 回を行い、認証を試みた。これを 1 セットとして、1 セットごとに各被験者の座る位置を時計まわりにずらし、端末の所有者役を交代しながら 5 セット分のデータを取得した。それぞれの被験者には、実験開始前に自分で後から再現のできる 2~3 秒程度の短いジェスチャという条件で自由にジェスチャを設定してもらい、5 回分のジェスチャデータを学習データとして取得している。各被験者が設定したジェスチャを表 2 に示す。データの取得は机に置いてある携帯端末を右手で手に取り、ジェスチャを行ってもらい、再び机に置くという手順で行い、試行ごとに 10 数秒の時間を空けた。データの取得後、閾値を変化させながら認証処理を行い、ジェスチャおよび特徴量について特性を調査した。

表 2 各被験者が設定した把持ジェスチャ

ジェスチャ名	動作
ジェスチャ 1	人差し指, 小指, 人差し指, 小指, 中指と薬指の順に握る.
ジェスチャ 2	人差し指, 薬指, 中指, 小指の順に握る.
ジェスチャ 3	薬指と小指, 人差し指と中指, 人差し指と小指の順に握る.
ジェスチャ 4	中指, 薬指, 小指, 人差し指の順に握る.
ジェスチャ 5	人差し指, 小指, 薬指, 中指の順に握る.

表 3 各ジェスチャの EER と FAR

学習データ数	指標	特徴量	平均	ジェスチャ				
				1	2	3	4	5
1 個	EER	位置+タイミング+力	0.17	0.36	0.20	0.04	0	0.24
		タイミング+力	0.40	0.25	0.56	0.42	0.18	0.56
		位置+力	0.04	0.18	0.01	0	0	0.03
		力	0.21	0.44	0.20	0.08	0	0.36
	FRR (FAR=0.05)	位置+タイミング+力	0.34	0.60	0.56	0.04	0	0.52
		タイミング+力	0.61	0.76	0.68	0.84	0.40	0.36
		位置+力	0.06	0.32	0	0	0	0
		力	0.58	0.88	0.88	0.16	0	0.96
2 個	EER	位置+タイミング+力	0.13	0.28	0.13	0.02	0	0.24
		タイミング+力	0.25	0.26	0.36	0.28	0.14	0.22
		位置+力	0.02	0.08	0.02	0	0	0.02
		力	0.21	0.41	0.20	0.07	0	0.38
	FRR (FAR=0.05)	位置+タイミング+力	0.22	0.42	0.32	0.02	0	0.32
		タイミング+力	0.50	0.54	0.56	0.86	0.18	0.32
		位置+力	0.06	0.28	0	0	0	0
		力	0.60	1.00	0.92	0.12	0	0.92
3 個	EER	位置+タイミング+力	0.10	0.15	0.12	0.03	0	0.16
		タイミング+力	0.20	0.22	0.28	0.28	0.08	0.12
		位置+力	0.02	0.09	0	0	0	0
		力	0.20	0.40	0.24	0.06	0	0.32
	FRR (FAR=0.05)	位置+タイミング+力	0.20	0.52	0.16	0	0	0.30
		タイミング+力	0.38	0.46	0.40	0.82	0.08	0.14
		位置+力	0.04	0.22	0	0	0	0
		力	0.58	1.00	0.88	0.12	0	0.88
4 個	EER	位置+タイミング+力	0.05	0.08	0.04	0.04	0	0.08
		タイミング+力	0.16	0.16	0.20	0.35	0.04	0.04
		位置+力	0.02	0.12	0	0	0	0
		力	0.22	0.46	0.32	0.04	0	0.30
	FRR (FAR=0.05)	位置+タイミング+力	0.12	0.36	0.04	0	0	0.24
		タイミング+力	0.30	0.32	0.28	0.80	0.04	0.04
		位置+力	0.04	0.20	0	0	0	0
		力	0.54	1.00	0.84	0.04	0	0.84
5 個	EER	位置+タイミング+力	0.05	0.10	0.05	0	0	0.10
		タイミング+力	0.14	0.10	0.20	0.40	0	0
		位置+力	0.03	0.15	0	0	0	0
		力	0.22	0.40	0.40	0	0	0.30
	FRR (FAR=0.05)	位置+タイミング+力	0.08	0.20	0	0	0	0.20
		タイミング+力	0.24	0.20	0.20	0.80	0	0
		位置+力	0.04	0.20	0	0	0	0
		力	0.52	1.00	0.80	0	0	0.80

4.2 評価結果および考察

学習データの個数を変化させた時の各ジェスチャの EER と FAR=0.05 の時の FRR を表 3 に示す. まず, 学習デー

タが 1 個の場合で各実験ごとの結果を比較する. 「位置+力」の特徴量を用いることで, 全てのジェスチャにおいて EER と FAR=0.05 の時の FRR の平均がそれぞれ 0.04,

表 4 各ジェスチャの本人間距離の平均と分散

特徴量		ジェスチャ				
		1	2	3	4	5
位置+タイミング+力	平均	16.50	3.65	2.92	0.84	3.68
	分散	683.11	1.16	0.44	0.041	0.61
タイミング+力	平均	0.53	0.61	0.53	0.45	0.58
	分散	0.016	0.020	0.0045	0.0066	0.013
位置+力	平均	3.41	3.25	3.26	3.39	3.30
	分散	0.021	0.0016	0.0051	0.0030	0.0093
力	平均	0.19	0.0096	0.0067	0.0024	0.017
	分散	0.13	0.000025	0.000016	0.0000033	0.00010

0.06 となり、他人はジェスチャをほとんど真似できないことが分かった。特徴量ごとの EER の平均についてみると、「位置+力」の特徴量は学習データが 1 個の場合でも 0.04 と低い値を示しており、学習データが 4 個の場合は 0.02 まで低下している。したがって、「位置+力」の特徴量は最も性能が良い特徴量であるといえる。また、「位置+タイミング+力」、「タイミング+力」の特徴量は学習データを増やすことで EER をそれぞれ 0.05, 0.14 まで改善できている。「力」の特徴量については、学習データを増やしても EER に改善が見られず、現時点では有効な特徴量でないことが分かった。今後さらに学習データを増やした場合の評価を行い、各特徴量の性能を調査する必要がある。

ジェスチャについて見ると、「ジェスチャ 3」、「ジェスチャ 4」のジェスチャは学習データを 1 個、「ジェスチャ 2」、「ジェスチャ 5」のジェスチャは学習データを 3 個用いた場合でそれぞれ EER が 0 になっている。一方、「ジェスチャ 1」のジェスチャは学習データを 5 個用いた場合でも EER が 0.15 であった。この点について、被験者が行ったジェスチャの再現性を見るために、各ジェスチャを本人が行った 5 回のデータの距離を計測した。5 回分のデータから得られる 2 組データの距離 10 通りの平均値および分散値を結果を表 4 に示す。結果より、「ジェスチャ 1」のジェスチャは分散が他のジェスチャと比較して大きいことから、EER が高くなった理由は「ジェスチャ 1」のジェスチャは他のジェスチャと比較して指の動きが複雑であり、ジェスチャの再現度が低かったことが原因であると考えられる。したがって、ジェスチャ登録の際に学習データ間距離の分散が大きいジェスチャを登録できないようにすれば、システムの性能は向上すると考えられる。

最後に、学習データの個数を変化させた時の被験者の座席位置ごとの EER の特徴について述べる。ジェスチャ動作は全て右手で行ったため、指先の動きが見えやすい端末所有者の右側の位置ではジェスチャが見破られ、EER の値が高くなると予想していたが、結果からはそのような傾向はみられなかった。その他の傾向もみられなかったため、ジェスチャ自由に設定される場合、他人が指先の動きを覗き見できたとしても、ジェスチャを再現することは難しい

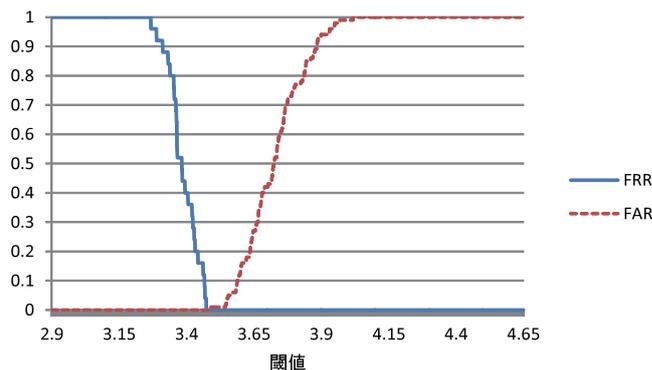


図 7 「ジェスチャ 4」のジェスチャの FRR-FAR 曲線 (EER=0)

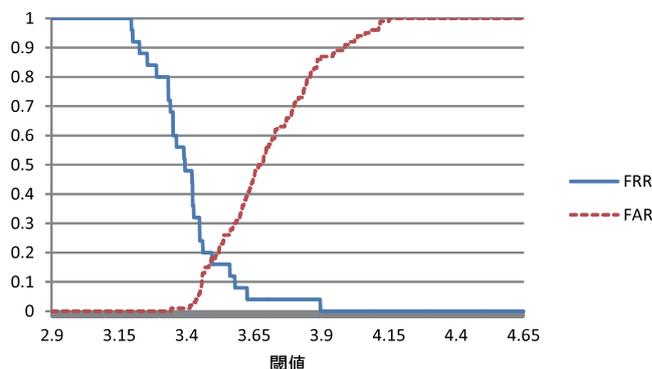


図 8 「ジェスチャ 1」のジェスチャの FRR-FAR 曲線 (EER=0.18)

ことが分かった。

現時点で認証に適していると考えられるジェスチャの例として「ジェスチャ 4」のジェスチャを、認証に適していないと考えられるジェスチャの例として「ジェスチャ 1」のジェスチャを挙げ、「位置+力」の特徴量と 1 個の学習データを用いた時のそれぞれの FAR-FRR 曲線を図 7 と図 8 に示す。図 7 に示す「ジェスチャ 4」のジェスチャは EER が 0 であり、性能が高いことが分かる。図 8 に示す「ジェスチャ 1」のジェスチャは EER が 0.18 と他の自由に設定したジェスチャと比べると高い値になっている。このため、ユーザがジェスチャ設定時にジェスチャを評価して、ジェスチャの変更を提案する機構が必要であると考えている。

5. まとめ

本研究では、携帯端末の側面に搭載した圧力センサを用いて、ユーザが端末を握って把持ジェスチャを行った際の把持力の分布から個人認証を行うシステムを構築した。把持ジェスチャは携帯端末の操作中に自然に行えるジェスチャであるため、提案システムにより、煩雑な操作を必要とせず個人認証が行える。提案システムの評価実験の結果、本人が自由に設定したジェスチャで認証を行い、他人がそれを真似することで認証を試みる環境では、EERの平均の最小値が0.02であり、自由に設定した5つのジェスチャのうち4つでEERの最小値が0になった。これは、本人が正しく認証され、他人が認証されない精度がほぼ100%であることを意味しており、自由に認証ジェスチャを設定する環境で、認証手法として有効であることを確認した。

今後の課題として、認証処理における抽出する特徴量の検討やデータ間距離の導出方法およびジェスチャ区間の抽出手法の改善によるシステムの性能の向上や、性能の良いジェスチャの種類の傾向の調査、ジェスチャの経年変化による認証精度の変化の調査などが挙げられる。

謝辞 本研究の一部は、科学技術振興機構戦略的創造研究推進事業（さきがけ）の支援によるものである。ここに記して謝意を表す。

参考文献

- [1] 崎田隆行, 鹿島雅之, 佐藤公則, 渡邊 睦: 指先トラッキングとその軌跡抽出を用いた個人認証に関する研究, 電子情報通信学会技術研究報告. PRMU, パターン認識・メディア理解, Vol. 107, No. 384, pp. 59-64 (2007).
- [2] 太田雅敏, 行方エリキ, 石原 進, 水野忠則: 端末自体の動きを用いた携帯端末向け個人認証, 情報処理学会論文誌, Vol. 46, No. 12, pp. 2997-3007 (2005).
- [3] K.Kim and et al: Hand grip pattern recognition for mobile user interfaces, *Proc. of the Conference on Innovative Applications of Artificial Intelligence*, Vol. 2, pp. 1789-1794 (2006).
- [4] W. Chang, K.E. Kim, and H. Lee: Recognition of Grip-Patterns by Using Capacitive Touch Sensors, *Proc. of IEEE International Symposium on Industrial Electronics*, pp. 2936-2941 (2006).
- [5] 佐藤勝規, 佐藤 究, 小笠原直人, 布川博士: 握るという動作を用いた個人認証システムの実装, 情報処理学会研究報告 (コンピューターセキュリティ研究会), Vol. 129, No. 384, pp. 7-12 (2006).
- [6] 梶原祐輔, 大島圭祐, 中村宗広, 南保英孝, 木村春彦: リモコン型操作デバイスと圧力分布センサを用いたPCの認証システム, 電気学会論文誌 C, Vol. 133, No. 5, pp. 1041-1046 (2013).
- [7] T. Iso and T. Horikoshi: Statistical Approaches for Personal Feature Extraction from Pressure Array Sensors, *Proc. of The Fifth IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing*, pp.129-133 (2013)