

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特性評価

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

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、特定の個人のみに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、煩雑な操作が不要で安全性の高い手法として、携帯端末の側面に搭載した圧力センサを用いて、把持ジェスチャの圧力分布から個人認証を行う手法を提案する。携帯端末を操作しようとする際に、多くのユーザは端末を取り出して把持する。把持ジェスチャはその時に端末を握る動作であり、端末を使用しようとする一連の動作の中で自然に行え、持ち方を変えたり、もう片方の手で操作するなどの煩雑な操作を必要としない。また、把持ジェスチャのユーザの手は端末から離れず指の力の入れ具合の変化のみであるため、ジェスチャ動作が他人から分かりづらく、仮にジェスチャ動画が見られても、その動作を再現することは難しいため、安全性も高い。評価では、把持ジェスチャによる個人認証の精度を測定し、ジェスチャごとの特性を調査した。

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方法として、文字列パスワードによる個人認証が一般的に用いられている。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。単純なパスワードや、生年月日、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など、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。さらに、身体的特徴はユーザ固有であり、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。

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

¹ 神戸大学大学院工学研究科
Graduate School of Engineering, Kobe University

² 科学技術振興機構 さきがけ
PRESTO, Japan Science and Technology Agency

³ NTT ドコモ 先進技術研究所
Research Laboratories, NTT DOCOMO

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

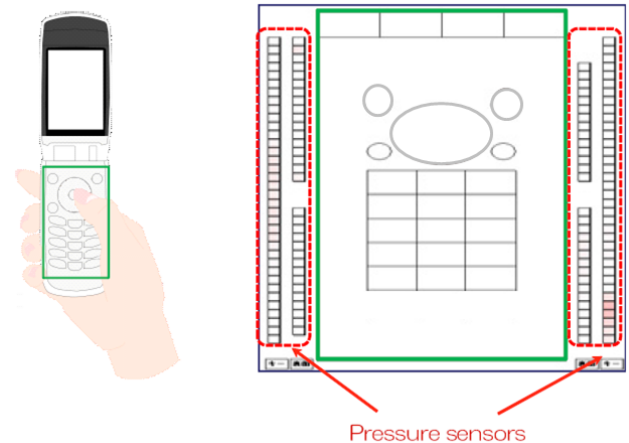


図 1 圧力センサを搭載した携帯端末



図 2 圧力センサアレイ

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ついては評価していない。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両側面と背面の両端側に搭載した携帯電話端末を用いる [7]。使用する圧力センサアレイは図 2 に示す 2.5mm × 2.5mm の小さなタイル状のものであり、高い空間分解能を持つ。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 0~100kPa、サンプリングレートは 100Hz 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。本研究では評価実験のために、端末に保存されたデータを PC に取り込み、認証

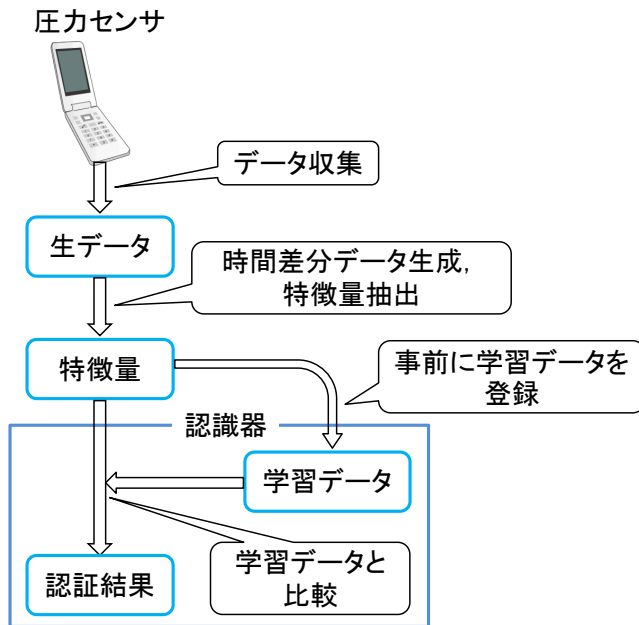


図 3 提案システムの構成

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により認証を行うことを想定している。したがって、認証用のジェスチャは数秒程度の片手で行えるジェスチャを想定している。

3.2 個人認証処理

図 3 に提案システムの構成を示す。大まかにはセンサから得られた生データの圧力値を特徴量変換し、事前に登録した本人の学習データと比較して、高い類似度であれば認証を許可するという流れである。具体的な処理手順は以下に示す 5 つの段階から成り、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によってユーザの把持ジェスチャ中の圧力データを計測する。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ものであり、握って圧力が加わっている部分が白くなっており、226 次元の圧力値を 1 サ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

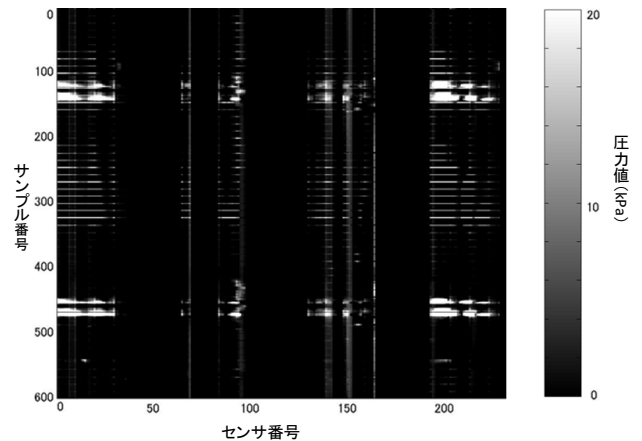


図 4 圧力センサアレイから得られるデータ

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、 $f_i(t)$ 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。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示す。

- (1) 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、 N は圧力センサの数で本研究では $N = 226$ である。
- (2) N' が閾値 N_{Th} を超えているか判定する。
 - (a) データ抽出開始前
 - (i) $N' < N_{Th}$ の場合
 $t = t + 1$ とし、(1) に戻る。
 - (ii) $N' \geq N_{Th}$ の場合
データを抽出と、抽出したデータの長さ（サンプル数） $IntervalA = t - t_a + 1$ の計測を

開始する。ただし、 t_a はデータの抽出を開始した時刻である。 $t = t + 1$ とし、(1)に戻る。

(b) データ抽出開始後

(i) $N' < N_{Th}$ の場合

N' が $N' \geq N_{Th}$ から $N' < N_{Th}$ となった時刻を、 t_b とする。データを抽出し、抽出したデータの長さ (サンプル数) $IntervalB = t - t_b + 1$ を計測する。 $IntervalA > IntervalA_{Th}$ かつ $IntervalB > IntervalB_{Th}$ 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。そうでない場合、 $t = t + 1$ とし、(1)に戻る。

(ii) $N' \geq N_{Th}$ の場合

データを抽出と、抽出したデータの長さ (サンプル数) $IntervalA = t - t_a + 1$ を計測する。 $t = t + 1$ とし、(1)に戻る。

ただし、 $IntervalA_{Th}$ および $IntervalB_{Th}$ は、あらかじめ設定した $IntervalA$ および $IntervalB$ の閾値である。 $IntervalA$ 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 $IntervalA$ 以上のデータを抽出できる。また、 $IntervalB$ 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。

3.2.4 特徴量の抽出とデータ間距離の算出

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「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、圧力センサがタッチパネルのように作用するためセンサの特性を生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まとめて述べる。

(a) 位置+タイミング+力

この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。そのため、端末を把持する位置とタイミング、加えられた把持力の全てにおいて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 $\mathbf{Y} = (\mathbf{Y}(1), \dots, \mathbf{Y}(l))$, $\mathbf{Y}(t) = (y_1(t), y_2(t), \dots, y_N(t))^T$ とおくと、 $\mathbf{Y}(t) = \mathbf{G}(t)$ となる。すなわち、

$$\begin{aligned}\mathbf{Y} &= (\mathbf{Y}(1), \mathbf{Y}(2), \dots, \mathbf{Y}(l)) \\ &= (\mathbf{G}(1), \mathbf{G}(2), \dots, \mathbf{G}(l))\end{aligned}\quad (2)$$

となる。

式 (2) より、初期設定時に登録したジェスチャデータ (正解データ) $\mathbf{A}$ 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) $\mathbf{B}$ の特徴量を $\mathbf{Y}_B = (\mathbf{Y}_B(1), \dots, \mathbf{Y}_B(l))$ とする。ただし、 l はジェスチャデータ $\mathbf{A}$ とジェスチャデータ $\mathbf{B}$ の長さを比較し、小さい方の値を用いる。この時、 $\mathbf{Y}_A$ と $\mathbf{Y}_B$ の距離 $d(\mathbf{Y}_A, \mathbf{Y}_B)$ は

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

のように求められる。ただし、 $\|\bullet\|$ 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

この特徴量では、ジェスチャ区間 (長さ l) 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特徴量とする。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、特徴量は

$$\mathbf{Y} = (\mathbf{Y}(1), \mathbf{Y}(2), \dots, \mathbf{Y}(l))\quad (3)$$

となり、時刻 t におけるヒストグラムは $\mathbf{Y}(t) = (y_1(t), y_2(t), \dots, y_K(t))^T$ となる。ただし、 $y_j(t)$ は階級 j の度数であり、階級の幅 H は $H = \frac{R}{K}$ である。

式 (3) より、初期設定時に登録したジェスチャデータ (正解データ) $\mathbf{A}$ 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) $\mathbf{B}$ の特徴量を $\mathbf{Y}_B = (\mathbf{Y}_B(1), \dots, \mathbf{Y}_B(l))$ とする。ただし、 l はジェスチャデータ $\mathbf{A}$ とジェスチャデータ $\mathbf{B}$ の長さを比較し、小さい方の値を用いる。この時、 $\mathbf{Y}_A$ と $\mathbf{Y}_B$ の距離 $d(\mathbf{Y}_A, \mathbf{Y}_B)$ は

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

のように求められる。

(c) 位置+力

この特徴量では、 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特徴量とする。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、特徴量は

$$\mathbf{Y} = (\mathbf{Y}(1), \mathbf{Y}(2), \dots, \mathbf{Y}(N))\quad (4)$$

となり、センサ i のヒストグラムは $\mathbf{Y}(i) = (y_1(i), y_2(i), \dots, y_K(i))^T$ となる。ただし、 $y_j(i)$ は階級 j の度数であり、階級の幅 H は $H = \frac{R}{K}$ である。

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。

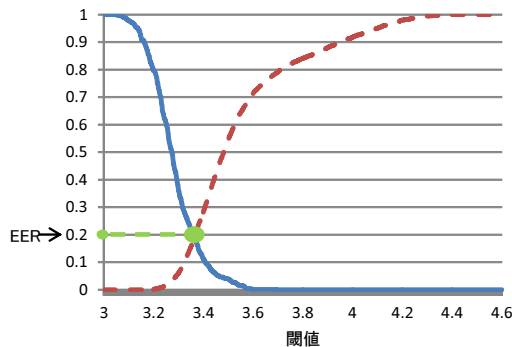


図 5 FRR-FAR 曲線と EER

式 (4) より、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 $\mathbf{Y}_A = (\mathbf{Y}_A(1), \dots, \mathbf{Y}_A(N))$, 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 $\mathbf{Y}_B = (\mathbf{Y}_B(1), \dots, \mathbf{Y}_B(N))$ とする。この時、 $\mathbf{Y}_A$ と $\mathbf{Y}_B$ の距離 $d(\mathbf{Y}_A, \mathbf{Y}_B)$ は

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

のように求められる。

(d) 力

この特徴量では、 N 個のセンサの全ジェスチャ区間 (長さ l) の値を全て足し合わせた値を特徴量とする。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、

$$Y = \sum_{k=1}^l \sum_{m=1}^N |g_m(k)| \quad (5)$$

となる。ただし、 $g_m(k)$ は時刻 k におけるセンサ m の圧力値である。

式 (5) より、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 Y_A , 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 Y_B とする。この時、 Y_A と Y_B の距離 $d(Y_A, Y_B)$ は

$$d(Y_A, Y_B) = |Y_A - Y_B|$$

のように求められる。

3.2.5 認証判定

以上のように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。

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評価実験を行った。認証時に行うジェスチャを他人が知っている場合と、覗き見によってジェスチャの種類を推測する場合の 2 つの場面を想定して実験を行った。

4.1 認証ジェスチャが既知の場合

まずはじめに、あるユーザの認証に必要なジェスチャが既知である場合を考える。他人が 10 種類のジェスチャのうち認証に用いられているジェスチャを知っている状態で提案システムの評価を行う。

4.1.1 実験の手続き

20 代の男性 10 名が 10 種類の把持ジェスチャをそれぞれ 10 回ずつ行い、1 人当たり 100 サンプルのデータセットを取得した。10 種類の把持ジェスチャを表 1 に示す。10 種類の把持ジェスチャはいずれも人差し指から小指までの 4 本の指の力の入れ方を指定しており、親指の力の入れ方は特に指定しないものである。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、実際の認証動作に近い動作をユーザーに行ってもらった。また、試行ごとに 10 数秒の時間を空け、センサの歪みの影響を極力緩和するようにした。データ取得後、得られたデータを PC に取り込み、各ジェスチャごとのデータセットから 3.2 節で述べた 4 種類の特徴量を抽出した後、閾値を変化させながら認証処理を行い、図 5 に示すような FRR(False Rejection Rate: 本人拒否率) と FAR(False Acceptance Rate: 他人許容率) の変化を調べ、FRR と FAR が等しくなる EER(Equal Error Rate: 等誤り率) を取り出しこれを評価の指標とすることで各ジェスチャの認識性能と用いる特徴量の特性を調査した。

4.1.2 評価結果および考察

各ジェスチャの EER と FAR=0.05 の時の FRR を表 2

表 2 認証ジェスチャが既知の場合の各ジェスチャの EER と FAR

	特徴量	ジェスチャ									
		握る	3 回握る	波打ち (上, 抜)	波打ち (上, 入)	波打ち (下, 抜)	波打ち (下, 入)	上 2 本	下 2 本	端 2 本	中 2 本
EER	位置+タイミング+力	0.34	0.36	0.45	0.42	0.42	0.42	0.34	0.41	0.39	0.38
	タイミング+力	0.32	0.28	0.40	0.36	0.29	0.29	0.28	0.40	0.34	0.28
	位置+力	0.26	0.22	0.38	0.20	0.20	0.20	0.19	0.44	0.20	0.26
	力	0.32	0.32	0.43	0.32	0.36	0.36	0.31	0.44	0.30	0.24
FAR=0.05 の時の FRR	位置+タイミング+力	0.75	0.62	0.90	0.78	0.82	0.76	0.78	0.99	0.98	0.71
	タイミング+力	0.76	0.62	0.83	0.77	0.75	0.68	0.64	0.83	0.82	0.75
	位置+力	0.56	0.52	0.86	0.47	0.78	0.42	0.40	0.77	0.45	0.62
	力	0.87	0.85	0.87	0.86	0.86	0.84	0.84	0.92	0.78	0.78



図 6 ジェスチャ秘匿率調査実験において認証用ジェスチャを行う被験者の様子

に示す. 特徴量については, 「位置+力」の特徴量が 4 つの特徴量の中で平均的に低い EER を示しており, 最も性能の高い特徴量といえる. 把持ジェスチャに注目すると, 「波打ち (上, 抜く)」と「下 2 本」のジェスチャの EER が高く, 認証用ジェスチャとして適切でないと考えられる. EER が高くなった原因を今後調査し, 認証用に適切ではないジェスチャにどのような傾向があるのか調査する必要がある. 対して, 「3 回握る」, 「波打ち (上, 入)」, 「波打ち (下, 抜)」, 「波打ち (下, 入)」, 「上 2 本」, 「端 2 本」のジェスチャは 0.19~0.22 と比較的低い EER を示しており, 現時点では認証に適したジェスチャだと考えられる. しかし, 5 回に 1 回は本人が正しく認証されず, また他人が誤って認証されることとなるため, 認証用として実用可能なほど高い EER とは言えない. また, FAR=0.5 の時の FRR を見ると, 「波打ち (下, 抜)」のジェスチャが 0.78 と EER に比べて高い FRR を示しており, このジェスチャは FAR を上げてセキュリティレベルを上げた時, 認証用ジェスチャとして適切でないと考えられる. 対して, 「3 回握る」, 「波打ち (上, 入)」, 「波打ち (下, 抜)」, 「波打ち (下, 入)」, 「上 2 本」, 「端 2 本」のジェスチャは 0.40~0.52 と比較的低い FAR を示しているが, 2 回に 1 回は本人が正しく認証されないこととなるため, セキュリティレベルを上げた場合, 認証用として実用可能とは言えない. このように EER や FAR が実用可能な値を示さなかったことは, 実際は認証用のジェスチャを他人に知られているという前

表 3 各ジェスチャの秘匿率

ジェスチャ名	秘匿率
握る	0.45
3 回握る	0.14
波打ち (上, 抜)	0.48
波打ち (上, 入)	0.42
波打ち (下, 抜)	0.44
波打ち (下, 入)	0.46
上 2 本で握る	0.46
下 2 本で握る	0.52
端 2 本で握る	0.52
中 2 本で握る	0.52

提で評価を行っていることが原因だと考えられる.

4.2 認証ジェスチャを覗き見る場合

実際の認証システムの利用を想定した場合, あるユーザの認証に必要なジェスチャは未知である. そのような状況で他人が認証を試みる場合, 本人が認証している様子を覗き見 (ショルダーハッキング) することが考えられる. そこで, 他人が認証ジェスチャを知らない状態で, 覗き見により認証ジェスチャを推測して認証する場合で提案システムの評価を行う.

4.2.1 各ジェスチャの秘匿率調査実験

はじめに, 他人が認証ジェスチャを覗き見した場合, 各ジェスチャが 10 種類のうちのどのジェスチャに見えるかのアンケートを取り, 各ジェスチャの秘匿率を調査した. 被験者は 4.1 節の実験と同じ 10 名である. 1 名が 10 種類の認証用ジェスチャをランダムに決められた順番で行い, 残り 9 名はそのジェスチャを見てどのジェスチャであると思ったかを回答した. この手順を, 認証用ジェスチャを行う被験者を交代させながら, 10 名全員の認証用ジェスチャに対して繰り返した. 認証用ジェスチャを行っている被験者の様子を図 6 に示す. 図 6 のように, アンケートに答える被験者には, 人差し指から小指の 4 本の指が動きが最も見えやすい角度で認証動作を見てもらった. また, 被験者には 10 種類の把持ジェスチャの詳細について事前に説明し, 理解してもらった上で実験を行った. 実験後, アンケートの結果から各ジェスチャの秘匿率 *ConcealedRate* を,

$$ConcealedRate = \frac{ANSWER_{all} - ANSWER_{correct}}{ANSWER_{all}}$$

として算出した. ただし, $ANSWER_{all}$ を各ジェスチャに

表 4 認証ジェスチャを覗き見る場合の各ジェスチャの EER と FAR

	特徴量	ジェスチャ									
		握る	3 回握る	波打ち (上, 抜)	波打ち (上, 入)	波打ち (下, 抜)	波打ち (下, 入)	上 2 本	下 2 本	端 2 本	中 2 本
EER	位置+タイミング+力	0.32	0.36	0.44	0.42	0.42	0.35	0.28	0.39	0.38	0.38
	タイミング+力	0.32	0.27	0.38	0.32	0.20	0.32	0.26	0.33	0.29	0.24
	位置+力	0.19	0.21	0.38	0.19	0.14	0.14	0.14	0.39	0.14	0.18
	力	0.30	0.32	0.43	0.32	0.36	0.27	0.28	0.41	0.30	0.22
FAR=0.05 の時の FRR	位置+タイミング+力	0.71	0.62	0.88	0.78	0.82	0.75	0.64	0.85	0.78	0.74
	タイミング+力	0.70	0.60	0.83	0.72	0.64	0.65	0.60	0.80	0.75	0.66
	位置+力	0.46	0.52	0.78	0.46	0.66	0.32	0.32	0.72	0.33	0.46
	力	0.87	0.85	0.87	0.86	0.86	0.83	0.83	0.92	0.78	0.74

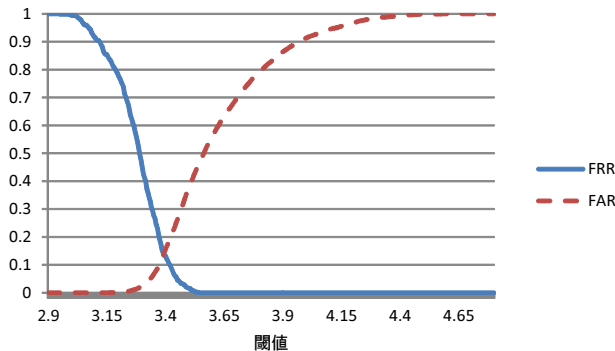


図 7 「波打ち (下, 入)」のジェスチャの FRR-FAR 曲線

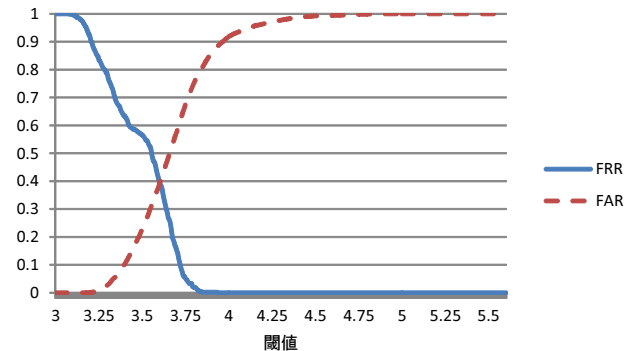


図 8 「下 2 本」のジェスチャの FRR-FAR 曲線

対する総回答数, $ANSWER_{correct}$ を正解回答数とする. 各ジェスチャの秘匿率を表 3 に示す. 「3 回握る」ジェスチャを除き, いずれのジェスチャも 0.50 前後の秘匿率となった. 0.50 とは 2 人に 1 人はジェスチャ動作が見破れたことを意味しており, このように秘匿率が低い原因として, 図 6 のように指が動きが最も見えやすい角度で認証動作を見てもらったことが原因であると考えられる. 実際の利用環境では, 実験を行った時より認証動作が見えづらくなるため, 秘匿率は高くなると考えられる. 「3 回握る」ジェスチャの秘匿率が低かったのは, ジェスチャにおける指の動きが他のジェスチャより大きかったことが原因であると考えられる.

4.2.2 実験の手続き

4.1 節の実験で得られたデータセットと, 4.2.1 節で得られたアンケート結果を用いて, 覗き見により認証ジェスチャを推測した場合のシステムの評価を行う. 4.1 節の実験では, 他人が認証に必要なジェスチャを知っている想定であったため, 認証データとして登録ジェスチャと同じジェスチャのデータセットを用いていた. しかし, 本評価では 4.2.1 節で得られたアンケート結果から, 被験者が回答したジェスチャのデータセットを用いて認証処理を行い, 4.1 節の実験と同様にジェスチャおよび特徴量について特性を調査した.

4.2.3 評価結果および考察

各ジェスチャの EER と FAR=0.05 の時の FRR を表 4 に示す. 特徴量について見ると, FAR を導出する際に, 他人の認証ジェスチャが正しくない場合もあったにもかかわらず, 「位置+力+タイミング」, 「タイミング+力」, 「力」

の特徴量で EER の改善は見られず, これらの特徴量は現時点では有効な特徴量ではないことが分かった. 全体として, 「位置+力」の特徴量を用いた場合が, FAR を導出する際に異なるジェスチャ同士の距離を用いることで, EER を低くすることができており, 現時点では最も有効な特徴量だと言える. 把持ジェスチャについて見ると, 「波打ち (下, 入)」, 「上 2 本」, 「端 2 本」のジェスチャについては, EER が 0.14 に, FAR=0.05 の時の FRR が 0.32~0.33 に低下しており, 現時点では認証用ジェスチャとして適したジェスチャであると言える. これらのジェスチャの EER や FAR が低くなった原因として, 被験者ごとに把持する箇所が大きく異なっていたことが原因だと考えられる. 今後, このように, 個人の再現性が高く, かつ個人差が大きいジェスチャおよび特徴量を調査していく必要がある. 参考として, 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「波打ち (下, 入)」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「下 2 本」のジェスチャを挙げ, 「位置+力」の特徴量を用いた時のそれぞれの FAR-FRR 曲線を図 7 と図 8 に示す.

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, ユーザが端末を特定の握り方で握る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, 把持ジェスチャによる個人認証の特性を評価した. 評価の結果, 他人が認証ジェスチャを覗き見て認証する場合, EER の最小値が 0.14 であった. しかし, 認証として十分小さな値とは言えないため, 認証システムの改善を行

う必要があることが分かった。

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、ジェスチャの種類の検討、実際に悪意ある第三者がセキュリティロックの解除を試みた場合の認証拒否率の調査などが挙げられる。

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)