2003－HI－105　(4)
2003／9／26

加速度センサ搭載腕時計型端末を用いた腕の動きによる個人認証

行方　エリキ[†]　太田　雅敏[†]
石原　　進[††]　水野　忠則[†††]

筆者らは，これまで携帯端末の動きによる個人認証を提案し，検討してきた．筆者らのこれまでの検討では，加速度センサを用いて，加速度の大きさの差分を認証判定の基準にしていた．今回の論文では，これまでの認証手法とは異なる視点で考え，ピーク出現の間隔を認証の指標としている．これによって，センサ間における測定値の大小の違いや，姿勢，使用者の状態（歩行中，乗車中など）によって加わる外乱の影響を受けにくい認証が可能になると推測する．腕時計型の端末を使って実際に提案手法を評価したところ，加速度の大きさの差分が少ないサンプルの割合を認証基準にしたときと，静止時においてはほぼ同等の結果が得られた．今回の提案手法と加速度の大きさを補助的に使うことで，より精度の高く，加速度測定条件に対する影響の少ない認証が実現できると推測する．

An Individual Authentication Method With Arm Movements Using a Wrist Watch Loaded With an Accelerator Sensor

ERIC NAMIKATA,[†] MASATOSHI OHTA,[†] SUSUMU ISHIHARA[††]
and TADANORI MIZUNO[†††]

So far,we have proposed and examined a method of authentication with arm movements using a portable device.We used an accelerator sensor , and used the difference of acceleration samples between the registered data and the subject data as factor of authentication.In this paper, we investigate a new authentication method that uses the interval of peaks of acceleration.The difference of measured acceleration value among sensor devices user's posture user's state(walking,riding a car and so on)will not affect the result of the authentication if the new method is used. We evaluated the proposed method with a wrist watch type device,we confirmed that the authentication result is almost equal to the method using difference of acceleration value when the users try the authentication movement under the same situation when the registration data are recorded.

1. はじめに

近年，情報技術の急速進展により，ノート PC や PDA，インターネットアクセス機能を備えた携帯電話が爆発的に普及し，極めて多くの人々が電子化された個人情報を持ち歩くようになった[3)]．これらの携帯情報機器は，個人情報の宝庫といえ，電話番号リストだけでなく，電子メールやスケジュール，各種サービスのための認証情報など，重要な個人情報が含まれている．また今後，小型情報端末や腕時計型をはじめとする多種のウェアラブル情報機器が普及すると見られている．これらの小型情報端末は小型・軽量化が進んでおり，持ち運びが非常に容易になっている．その反面，端末をテーブルや新幹線，ホテルなどどこかに置き忘れたり，紛失したりするケースが増えてきている．個人情報が多く含まれていることから携帯情報端末を盗むことによって，その個人情報を悪用するといったケースも考えられ，携帯情報端末における認証は非常に重要であるとわかる．また，今後ネットワークを経由した電子商取引 EC（Electronic Commerce）が普及すると見られ，その重要性はさらに増すことになるだろう．

筆者らのグループでは，これまで加速度の大きさの差分をベースとしたアルゴリズムで認証手法を検討してきた． 1) では，加速度の時系列データで腕が認証のために動作している区間のみを抽出ししきい値以内のサンプル数がサンプル全体に占める割合のしきい値以上であれば認証成功としていた． 2) では，DP マッチングを用いることで時間軸上の少量のずれを共用しつつ， 1) と，同じように加速度の大きさの差分を求

† 静岡大学大学院情報学研究科
Graduate School of Information,Shizuoka University
†† 静岡大学工学部
Faculty of Engineering,Shizuoka University
††† 静岡大学情報学部
Faculty of Information,Shizuoka University

める認証手法を提案している．

本論文では，これまでの加速度の大きさの差分を用いた認証手法ではなく加速度のピークの出現間隔による認証手法について検討する．ピークはセンサから出力された加速度の厳密な大小を問題としないため，センサ間における測定値の大きさの違いや，姿勢，使用者の状態（歩行中，乗車中など）によって加わる外乱の影響を受けにくい認証が可能になると考える．以下，本論文の構成について述べる．

第 2 章では，従来の認証方式の種類と特徴について述べる．続く，第 3 章では腕の動きによる個人認証システムについて概観し，使用用途をいくつか紹介する．第 4 章では前半に認証処理について概観し，後半にその詳細なアルゴリズムを示す．第 5 章では，提案手法の有効性を実験によって評価し，検討課題を述べる．最後に，第 6 章で提案する認証手法のまとめを記す．

2. 従来の認証方式

従来の認証方式は大きく 3 種類に分けられる．以下にそれらの特徴を述べる．

2.1 知識による認証

パスワードや ID をペンやボタンで入力する最も古い認証方式である．本方式は，ほとんどの人が使っており，心理的抵抗は少なく，パスワード管理コストのみ必要という利点を持っている．しかし，パスワードは簡単なものにすると悪者によって推定されたり，また複雑なものに設定すると本人がパスワードを忘れてしまうといった問題点がある．

2.2 所有物による認証

IC カードや磁気カードなどに代表されるような物理的キーによる認証方式である．ユーザ数が多い場合でも導入コストが安く，容易に導入できることが利点として挙げられる．しかし，物理的キーの紛失や盗難，破損，偽造などの危険性がある．このような場合，絶えずメンテナンスが必要になり，コストが時間とともにかさむ．

2.3 バイオメトリクスによる認証

身体的あるいは行動的な特徴を使って個人を識別する認証方式である．身体的特徴としては，指紋，掌形，顔，静脈パターン，虹彩などがあり，行動的特徴としては声紋や動的署名がある．これらのバイオメトリクスによる認証は従来のパスワードや所有物による認証手法に比べ，他人に不正利用される可能性が低い．しかし，認証の際に特別な認証装置が必要であるといった問題や，特徴を登録する際に心理的抵抗があるといった問題がある．

2.4 携帯端末における認証の要求事項

前述したことからわかるように，従来の認証方法はそれぞれ一長一短があるため，厳密にどの認証方法がよいのかを決めることはできない．しかし，携帯端末を用いて携帯端末自体の利用者認証，あるいは携帯端末を通じてそのほかのシステムの認証を行うことを考えた場合，以下の要求を満たしていることが望ましい．

- 手軽に認証ができること
- 認証の際に外乱の影響を受けないこと
- 携帯端末に負荷をかけないように計算量が少ないこと

3. 腕の動きによる個人認証

3.1 研究全体の概要

これまで，ユーザの動きの検出に画像処理による方法[4) 5)]がいくつか提案されている．しかし，検出の精度を上げるにつれカメラなどの画像入力デバイスも大きくなり，携帯端末に不向きであった．そこで，本研究ではこのような画像入力デバイスなどに比べ，小型かつ比較的安価であり，他の装置を使用せずに手軽に動きが検出できるなどの理由から加速度センサを用いることとした．現在，加速度センサを用いて動きを検出し，それを元に認証を行っている製品として CAVEO 社[6)]の Anti-theft がある．Anti-theft は PC カードに加速度センサを搭載し，前後左右の傾きを検出し，その組み合わせをパスワードとして利用するノート PC 用の防犯グッズである．Anti-theft がパスワードを入力した人物の違いを考慮しないのに対し，本システムはピークの出現間隔を用いた認証手法により，なりすましを防ぐことが期待できる．しかし，Anti-theft で登録できるのは人間の動作の特徴とは関係ない限られた移動パターンの組み合わせに過ぎず，他人が容易に認証用動作を覚えることができてしまう．

本研究では，加速度センサ搭載の端末を用いて，腕の動きを検出し認証を行うことを検討している．特に腕時計型の端末として，シチズン時計 (株）と IBM 社が共同開発した WatchPad ™ ☆を用いている．**表 1** に WatchPad ™ の簡単な仕様を示す.（詳細については [7)] を参照）

認証時には，**図 1** のように腕時計を装着して認証を行う．

3.2 使 用 用 途

本研究で提案している携帯端末の動きを用いた認証方式は，認証対象の端末以外の機器を使用しないこと，

☆ WatchPad は IBM Corporation の商標です.

表 1　WatchPad ™ 仕様

本体	
サイズ	65mm × 46mm × 16mm
重さ	43g
通信機能	Bluetooth(V1.1), 赤外線（irDA V1.2）
加速度センサ	
メーカー・型番	Analog Devices 社製 ADXL202E
分解能	60Hz 帯域幅で 2mG
軸	XY 軸
加速度検出範囲	－2 G～＋2 G

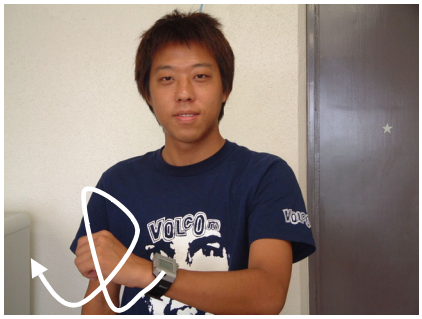

図 1　動きによる認証

端末自体を動かす以外の動作が不要であるため，手軽に認証ができることがその最大の利点として挙げられる．特に，腕時計型の端末では，端末自体が常に身につけられた状態にあるために，手軽さが極めて高くなる．また，現在，腕時計はわれわれにとって最も身近なウェアラブルデバイスであり，今後も高い機能がこれらに搭載され，ウェアラブルデバイスの中心として発達することが期待できる．以下に，腕の動きを用いた個人認証方式の利用例を挙げる．

■携帯端末自体の個人認証

腕時計だけでなく，携帯電話や PDA など小型携帯端末の高機能化に伴い，アドレス帳に加え，スケジュールや各種サービスのためのパスワードなどが個人情報として携帯端末に入っている場合が多くなっている．このような個人情報を保護するためにも携帯端末における個人認証は必須であると言える．

■他のシステムを利用する時の個人認証

認証装置を腕時計と考えた場合，装着してから 1 回の認証でアクティベート状態にすれば他システムを利用するたびに認証を行う必要がなくなる．アクティベート状態を切るには単に腕時計を外せばよい．アクティベート状態のとき，例えば，次のような利用方法が考えられる．

- 近くにあるドアの鍵が開く（鍵のような物理的なキーの代わりとなる）
- 腕時計とレジのＰＯＳ端末間の代金決済，割引クーポン券，ポイントサービス，電子レシートのデータの授受
- 自動販売機での物品購入
- 腕時計に対する電子チケットの発券や，決済，入場管理
- 腕時計に定期券や，プリペイドカードの機能を付加したチケットレスの改札

4. 認 証 処 理

本章では，今回提案する携帯端末の加速度のピーク値出現間隔を使用した個人認証手法について説明する．

4.1 認 証 指 標

これまで検討してきた加速度の大きさの差分を用いた認証手法では，次の 2 つの懸念すべき点があった．

(1)　ユーザの姿勢（腕の初期位置や向きなど）や行動（歩く，走る，運転するなど）による外乱の影響を受けやすい

(2)　個々のセンサデバイスの測定誤差の影響を受けやすい

(1) では，例えば，止まっている時と走りながら測定した加速度データは異なり，同じ動作をしているつもりでも認証判定に影響を与えてしまう．(2) では，センサデバイス間において測定された値が異なる場合，認証データをデバイス間で共用することができなくなるという問題が生じる．そこで，筆者らは加速度の大きさに影響を受けにくい指標として，加速度波形のピークに着目した．これまでの一連の実験により，同一人物におけるマスタデータと認証判定対象加速度データの波形のピークはほぼ同じタイミングで出現することが観測されている．そこで，加速度波形のピーク出現間隔を認証指標として有用であると考えた．提案手法では，加速度センサの測定値は差分を用いた手法のように厳密である必要がなく，ピークの出現時刻を検出できればよい．また，波形のピーク出現間隔はセンサデバイスの違いによる測定値の違いに関係なく同じ認証用登録データを使うことができるので，同じ登録データを複数の端末で共用するような環境にも適用が容易である．

4.2 ピーク検出手法

音声認識や画像処理の分野では，波形のピーク検出は大きな課題の一つとなっている．人間の動作の認識や識別に用いられる波形のピーク検出の例としては，8) のように筆圧データにおけるピークを検出している例や 9) のように加速度データのピークを検出している例がある．本論文では， 4) で手話画像の圧縮化を

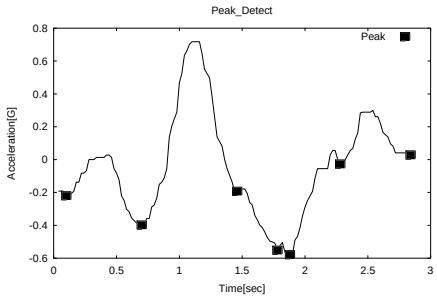

図 2　ピークの検出例

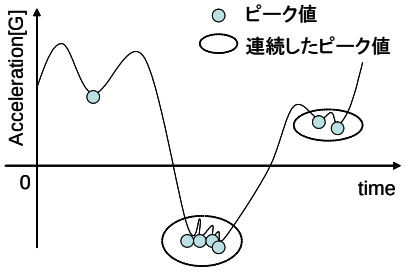

図 3　連続してピーク値が検出された波形の例

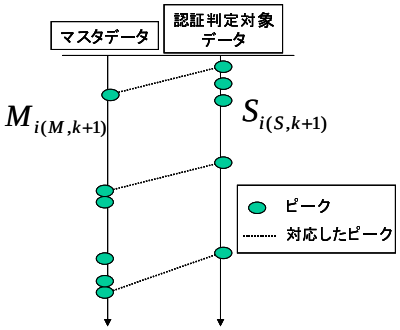

図 4　検出されたピーク値のみのグラフ

行うためにビデオ画像を用いたフレーム間の差分からピーク検出を行っている方法に習って加速度データの谷のみを検出し，これらの出現間隔により認証を行うこととした．

以下に谷の検出アルゴリズムを示す．

時刻 t における加速度を a_{t}，最後に検出したピークから現在参照している加速度までの時間を T とする．元の加速度データではノイズがあるため，適切な選択処理を行わない限りピーク値がいくつも検出されてしまう．そのため，ピーク値検出の際には，元データに対しメディアンフィルタをかけ，ノイズを低減している．今回実装のメディアンフィルタでは対象とするデータの前後 4 個分（0.16 秒分）のデータを対象としてメディアンを計算している．メディアンフィルタをかけた後，**式 (1)** を満たしていればピークとみなす．実際の動作データ（サンプリングレート 50Hz）に対し，ピークが検出された波形の例を**図 2** に示す．

$$\begin{aligned} &a_{\mathrm{t}} < min(a_{\mathrm{t}-1}, a_{\mathrm{t}+1}) \text{ and} \\ &a_{\mathrm{t}}/(T+4) < max(a_{\mathrm{t}-1}-a_{\mathrm{t}}, a_{\mathrm{t}+1}-a_{\mathrm{t}}) \text{ and} \\ &a_{\mathrm{t}}/4/(T+4) < min(a_{\mathrm{t}-1}-a_{\mathrm{t}}, a_{\mathrm{t}+1}-a_{\mathrm{t}}) \end{aligned} \quad (1)$$

4.3　ピークの出現間隔による認証手法

マスタデータと認証判定対象データのピーク出現の間隔を照合することによって認証を行う．ただし，**図 3** ように短い間隔でピーク値が出現する場合は，正しいピーク出現間隔を測定できないため，これらの存在を無視して照合を行うのが適当である．本手法では，ピーク値の出現間隔ができるだけ等しくなっていると見なせるように，間隔が短いピークを無視することとし，無視したピークの個数を認証定時に不利に働く指標として扱う方法を用いた．(**図 4** 参照．**図 4** は，縦軸に時間軸をおいてマスタデータと認証判定対象データのピークのみをプロットした時のグラフの例である．)

ピークの出現間隔による認証アルゴリズムの詳細を以下に示す．

1. マスタデータ，認証判定対象データの検出されたピーク数を求める

それぞれ P_{M}，P_{S} とする．マスタデータと認証判定対象データの検出されたピーク数のしきい値を P_{d} として，$P_{\mathrm{S}} \leq P_{\mathrm{d}}$ の場合，認証判定対象データは無効と見なす．なお，マスターデータに関しては，データ登録時に $P_{\mathrm{M}} > P_d$ が満たされているとする．ピーク数が少ない，または，ピークがないデータに対しては本稿で提案しているピーク間隔の系列に基づく認証を有効に作用させることはできないので，このようなデータは扱わない．今回は，P_d の値を 3 とした．

2. マスタデータと認証判定対象データのピーク出現間隔の対応付けをする

マスタデータ，認証判定対象データにおける i 番目のピーク出現間隔をそれぞれ M_i，S_i とする．両者ピーク出現間隔の系列の中でピーク出現間隔ができるだけ同じになるように，一致判定をしている時刻におけるピーク出現間隔が短い方の系列で出現したピークを無視していく．ここで k をそれまでにマスタデータと認証判定対照の間で一致させたピークの数とする．

$i(\mathrm{M},k)$，$i(\mathrm{S},k)$ をそれぞれ k 個までの一致判定を終

えたマスタデータと認証判定対象データのピーク間隔のインデックスとする．以下の式で得られる I_{k+1} が最小になるような，$i(\mathrm{S},k+1)$，$i(\mathrm{M},k+1)$ を求める．

$$\begin{aligned}&\text{if}\quad M_{i(\mathrm{M},k)+1} < S_{i(\mathrm{S},k)+1}\\ &\quad i(\mathrm{S},k+1) = i(\mathrm{S},k)+1\\ &\quad I_{k+1} = \left| S_{i(\mathrm{S},k+1)} - \sum_{i=i(\mathrm{M},k)+1}^{i(\mathrm{M},k+1)-1} M_i \right|\end{aligned} \tag{2}$$

$$\begin{aligned}&\text{if}\quad S_{i(\mathrm{S},k)+1} < M_{i(\mathrm{M},k)+1}\\ &\quad i(\mathrm{M},k+1) = i(\mathrm{M},k)+1\\ &\quad I_{k+1} = \left| M_{i(\mathrm{M},k+1)} - \sum_{i=i(\mathrm{S},k)+1}^{i(\mathrm{S},k+1)-1} S_i \right|\end{aligned} \tag{3}$$

$$\begin{aligned}&\text{if}\quad S_{i(\mathrm{S},k)+1} = M_{i(\mathrm{M},k)+1}\\ &\quad i(\mathrm{M},k+1) = i(\mathrm{M},k)+1\\ &\quad i(\mathrm{S},k+1) = i(\mathrm{S},k)+1\end{aligned} \tag{4}$$

この処理を $i(\mathrm{M},k) \le P_{\mathrm{M}}$ かつ $i(\mathrm{S},k) \le P_{\mathrm{S}}$ を満たす間行う．この処理によって行うことのできたピーク値の一致回数を $k_{\max}$ とする．

3. 認証判定を行う

距離を D とする．D は全ての対応付けしたピーク出現間隔の距離の和と対応付けしたピーク値の数で求められる．(**式** (5))

$$D_x + D_y \le d \tag{5}$$

加速度を 2 軸以上で測定可能な場合，各軸に対して同様の処理を行い，各軸の D の和に対してしきい値 d によって認証の成否を判定する．例えば 2 軸を用いる場合，x 軸,y 軸上の加速度に対する D として D_x，D_y を求め，以下の式が満たされていれば認証成功と判定する．

$$D_x + D_Y \le d$$

今回は，d の値を 2.00 とした．

5. 評価実験

4 章で述べたアルゴリズムを WatchPad ™ 上で試作し，ピークの出現間隔による認証手法の有効性について調べるために実験を行った．

5.1 実験方法

被験者の左腕に WatchPad ™ を装着し，サンプリングレート 50Hz で 3 秒間加速度データを取得した．被験者は静止状態で立ったまま認証動作を行った．端末の構造上，端末を腕に装着したときぶれが起きるため，結果に影響を及ぼす可能性がある．そこで，時計がぶれるのを防ぐために被験者全員にリストバンドの上から端末を装着してもらった．

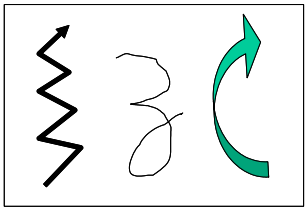

図 5 被験者が登録した動作パターンの例

まず，本人拒否率を調べるために，被験者に自分のオリジナルの動きを一人一パターンずつ端末に登録してもらい，その後，複数回同じ動作を行ってもらった．登録されたパターンのいくつかを **図 5** に示す．**図 5** の左の例は，ひじを直角に曲げ手を横にブルブル振動させる動作である．同図中央は筆記体で小文字の z を描いたもの，右側の例はパンチで左フックをしたときの動作である．被験者全員の登録した動作パターンはみな似ているところがなかった．被験者数は 12 人で，各人 3 回ずつ本人拒否率のために認証動作を行ってもらった．

次に，他人受け入れ率を調べるために，被験者の前で他の利用者が小文字の d を筆記体で書くという動作を登録し，被験者にそれを模倣してもらった．ただし，成りすましが容易にできるように被験者には登録した動作があらかじめ小文字の d であると口頭で伝えた．被験者数は 10 人であり，各人 3 回ずつ認証動作を行ってもらった．

5.2 実験結果・考察

本人拒否率，他人受け入れ率をそれぞれ ”認証失敗回数 / 試行回数”, ”認証成功回数 / 試行回数” で求めたとき，被験者全体で 10/36，10/30 という結果を得た．この結果は， 1) で提案した加速度の大きさを用いた手法とほぼ同じとなった．

図 6 は，同一人物の登録マスタデータと認証判定対照データのグラフの例である．**図 6** からわかるように，二つの波形はほぼ同じであるため認証は成功としていると見なしてよいだろう．しかし両者の同開始から同一時間後の加速度サンプル値は加速度の大きさが最大で 0.3〜0.4G 異なっている．実験条件より被験者は静止状態で立ったまま認証動作を行っているので，被験者の姿勢，使用状況はほぼ一定であるといえる．

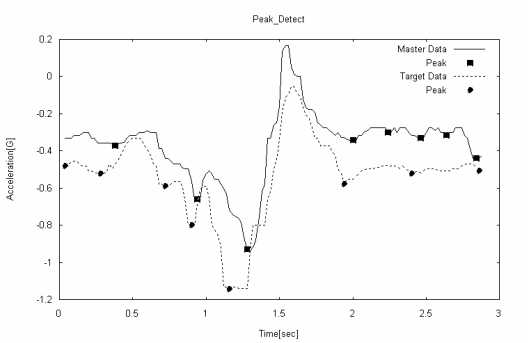

図 6 加速度の大きさの違いを吸収した例

このような誤差が生じる他の可能性として，認証動作登録時と認証を行ったときの端末の装着のずれによるものや，被験者が単にあまり力を入れないで認証動作を行っただけかもしれない．前者で誤差が生じる理由として，WatchPad TM 搭載の加速度センサは静止加速度も測定されるため，わずかな，x 軸，y 軸に沿った端末のずれが測定値に影響を及ぼすためと考える．それゆえに，二つの波形はほぼ同じであるにもかかわらず，各軸の加速度の大きさの差分が少ないサンプルの割合を認証基準にしたときでは認証失敗という結果になってしまう．

これに対し，本稿での提案手法ではピークが加速度の大きさに依存することなく正しく検出されていて，認証成功と判定された．このように，ピークの出現間隔による認証手法では，波形は似ているがユーザの姿勢，使用状況などにより誤差が生じた場合でも有効であると考える．

5.3 検 討 課 題

今回提案した認証手法では，マスタデータ，認証判定対照データの両ピーク系列の中で検出したピークを無視することによってピーク出現間隔をできるだけ同じになるようにしている．このため，本手法はピーク数が多い波形に対しては非常に弱く改善が必要である．解決策として，無視したピーク数に応じて認証が難しくなるようにするペナルティを大きく与える方法，一致したピーク出現間隔の距離を測るときに加速度の大きさを考慮する方法，ピークの出現回数が少なすぎる登録動作を許さないなどの方法が考えられる．また，提案手法では加速度のピークが認証指標となっているので，適切なピーク検出が最重要課題である．今回は 4) のピーク検出法を習いピーク検出を行ったが，今の実験を行った範囲ではピークが極端に多く取れたり，まったく取れなかったりというような事例がいくつか見られた．これらにより，実験全体としての本人否認率，他人受け入れ率の測定結果が従来方法と同程度にとどまってしまっており，現在のピーク検出のアルゴリズムを改良，または，新たなアルゴリズムを考える必要がある．

6. ま と め

本論文では，動きによる認証方式の認証手法としてピークの出現間隔を使った手法を提案し，検討した．提案手法は，使用者の姿勢や使用状況，端末の装着のずれなどによって起きる加速度の測定値の違いを吸収できることが確認できた．また，加速度の大きさの差分が少ないサンプルの割合を認証基準にしたときとほぼ同じ本人拒否率・他人受け入れ率であった．今後の課題は，本人拒否率・他人受け入れ率を下げるために，提案手法に加速度の大きさを補助的な指標として考慮し，低い本人否認率，他人受け入れ率を得られるように改良を行うことである．

参 考 文 献

1) 行方, 坂根, 石原, 水野: ”加速度センサ搭載腕時計を用いた動きによる認証方式の提案” 情報処理学会第 65 回全国大会, 1W-2 (2003).
2) 太田, 行方, 石原, 水野: ”加速度センサを用いた手の動きによる個人認証に関する検討” マルチメディア，分散，協調とモバイル（DICOMO2003）シンポジウム論文集, 情報処理学会シンポジウムシリーズ, Vol.2003, No.9, pp.261–264 (2003).
3) 電気通信事業者協会, ”http://www.tca.or.jp/japan/database/daisu/index.html”
4) 宮尾淳一:”手話における意味的特徴点と手話動画圧縮への応用” 電子情報通信学会論文誌 D- ,Vol.J84-D-I,No.11,pp.1577-1580 （2001）
5) 大橋, 中程, 吉田, 江島:”「棒」入力システムのためのジェスチャ認識の実現” 情報処理学会論文誌, Vol40 No.2 1999 年 2 月
6) Caveo,”http://www.caveo.com/”
7) IBM, ”http://www.trl.ibm.com/projects/ngm/”
8) 菊池, 赤松,: ”高速筆記者のための高感度筆圧ペンの試作と筆者認証実験” 電子情報通信学会論文誌 D- ,Vol.J83-D- ,No.8 pp.1763-1772 （2000）
9) 宇佐, 持田: ”HMM とファジィを使った指揮認識システム” 情報処理学会研究報告, MUS, 音楽情報科学, Vol. 97,Num. 67,pp.37-44 （1997）