加速度センサを用いたスマートフォンの筆跡認証の性能向上

西郷里 拓[1]　川本 淳平[1]　櫻井 幸一[1]

概要：スマートフォン本体の加速度センサを利用して，不安定な入力環境における署名認証の精度を向上させる手法を提案する．スマートフォンの普及により個人情報や業務関連情報など機密情報を携帯する人が増えている．多くのスマートフォンでは，紛失や盗難時に，これらの機密情報を保護するために簡易なパスワード認証が用意されているが十分とは言い難い．より安全性を増した認証方法も提案されており，その一つに署名認証がある．しかし署名入力時に本体の揺れが影響し意図しない入力となることがある．我々の提案手法では，スマートフォンに搭載された加速度センサの情報を取得してデータを補正する．その結果，他人受入率を上げることなく本人拒否率を最も良い場合で 56.3 %から 43.8 %に減らすことができた．

Precision Improvement by the Acceleration Information in the Signature Verification of the Smartphone

Taku Nishigori[1]　Junpei Kawamoto[1]　Kouichi Sakurai[1]

Abstract: In this paper, we proposed a method which improves precision of the signature verification in smartphones by acceleration sensors while the smartphones are in unstable environments. People carry confidential information into smartphones. However, we have a risk that leakage of such information with loss of smartphones. Although many smartphones have verification with the password, these verifications are not secure enough. Hence, some more secure verification methods than the password are proposed. The signature verification is one of them. It has tolerance for shoulder hacking. Unfortunately, input data for such verification is distorted with a swing of smartphones caused by unstable environment (e.g. during walking). We correct data with an acceleration sensor put on the smartphone. As a result, we reduced the false rejection rate of verification to 43.8% from 56.3% without gaining false acceptance rate.

1. はじめに

近年，情報通信技術は日々進化しておりその中でも携帯電話の普及率は高まっている．特に，スマートフォンの普及率も増加している．スマートフォンに大量のデータを入れて持ち運ぶ人も増えてきている．データの中には電話番号などの個人情報だけでなく業務上の機密データが含まれている場合もありスマートフォンのセキュリティは重要な課題となっている．スマートフォンにおけるセキュリティとしては，コンピュータウイルス対策やより安全な OS の研究などがある．しかし，それらのセキュリティが頑強なものであってもスマートフォン本体の盗難や紛失時に他人が自由に端末を利用できてしまっては無意味である．第三者による不当な端末の使用を防ぐために認証技術は重要である．現在のスマートフォンにおける個人認証はパスワードやパターン入力が主流である（図 1）．しかし，これらの認証は覗き見されると簡単に覚えられてしまいセキュリティとして安全とはいいがたい．

スマートフォンにおける覗き見耐性のある個人認証方式の研究も数多く行われている．一般的に，認証の種類には三つの主な形態，記憶による認証，物による認証，生体認証がある．記憶による認証とは主にパスワードの入力である．入力を複雑化することで覗き見耐性を得る手法 [6] が提案されているが入力時間が従来より増加し記憶への負荷も大きい．物による認証とは，ワンタイムパスワードを生成するためのトークンや IC カードでの認証である．これらは記憶への負担は少ないがスマートフォンと同じく盗難

[1] 九州大学, 福岡県福岡市西区元岡 744 番地
Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, JAPAN

図 1　スマートフォンの個人認証画面

時に他人の認証を防ぐすべはない．生体認証は本人の証明のために何かを持ち歩く，何かを記憶する必要がほぼ存在せず利便性と安全性を兼ね備えた認証として知られている．

指紋認証は生体認証の中でも有名な手法の一つである．指紋は音声や顔に比べて経年変化が少なく他人との類似性も少ないため長期間に渡って安定した識別精度を維持できる．1970 年代には犯罪捜査用の指紋照合の研究もおこなわれており近年多くのスマートフォンにも指紋認証のためのセンサが取り付けられている．指紋認証の欠点としては指の表面の乾燥や手荒れ，汚れの付着などで認証の精度が落ちてしまうという問題があり，センサと認証アルゴリズムの両面での性能向上が課題となっている．実際にスマートフォンに搭載されている指紋認証としては，iPhone5S 以降の iPhone に搭載されている指紋認証機能の「Touch ID」や，Samsung の GALAXY S5 の指紋認証センサ，ARROWS の裏面にあるセンサーによる指紋認証が有名である．

顔認証は生体認証の中でも指紋や目の虹彩や静脈による認証と比べると経年変化が大きく精度に問題があると考えられているのが一般的である．しかし，認証情報をクラウド上に保存することを考えると，指紋や静脈の情報に比べ，顔というのは公に知られている情報であるという点で勝っている．Android では顔認証が実際に実装されているがこれは顔写真で突破が可能であるという問題があった．それに対して Disrupt SF 2014 で「IsItYou」という顔認証の新しいテクノロジーが発表されたがこれは顔写真だけでなく３ D プリントされたお面でも認証されずに済むという利点がある．しかし経年変化が大きいという問題がある．

その生体認証の一種に署名認証がある．署名文化のある欧米では盛んに研究が行われている [2][3]．署名認証には次のような特徴がある．

- 従来より社会的に用いられている署名という手法であり利用者の受容性が高い．
- 行動特徴による認証であり本人の意思確認を伴う．
- 情報漏えいが発生した場合，登録データを柔軟に変更できる．
- 全く同じ署名の再現は困難であり過去に使われた署名データの棄却により署名情報の盗難防止になる．
- 電子文書への貼り付けが可能である．

このような特徴を持つことから，署名認証は生体認証の中でも重要な技術の一つである [9]．署名認証は，オンライン方式とオフライン方式の二つに分けることができる．オフライン方式とは紙などに書かれた文字や文章をスキャナーで細かいメッシュ状の濃度値として認証システムに入力する方式である．これに対してオンライン方式というのは文字が書かれた状況（書き順，圧力，速度）を認証の際の情報として用いる方式である．認証に利用できる情報もオフライン方式と比べて多種にわたるので，オンライン署名認証では本人であっても入力するデータが毎回少しずつ異なっているという問題がある．この問題を解決するために Dynamic Time Warping(DTW) を用いた手法 [2] や Hidden Markov Model(HMM) を用いた手法 [3] が提案されている．本稿では DTW を利用する．

署名認証の問題点は複数あるが，重要な課題の一つに入力する状況に認証精度が左右されるという問題がある．現在の署名認証の想定している入力時の状況は座った状態などの安定した環境での入力である．しかし，実際の生活でスマートフォンを使うことを考えると歩きながらの認証や，電車や車などの突発的な揺れが生じうる状況での認証も行われている．そのような状況においての安定した認証技術は必要なものであるといえる．署名認証についての既存研究としては，新たな個人性抽出手法 [5] の提案や，署名時のペンの傾きに着目したもの [4] などがあるが，これらは入力時の条件が安定した環境での入力である．本研究は多くのスマートフォンに搭載されている加速度センサを用いて入力時の移動状態におけるノイズを補正し，署名認証の精度を向上させる．本研究では，署名時のタッチ情報と加速度センサの値の時系列データから本体の揺れを検知しデータの一部を取り除く．提案手法の評価実験において本人拒否率を 66.7 %から 58.3 %に下げることができた．また，他人入力のデータを同様に補正したとき補正前と等価エラー率は変わらなかった．よってこの手法により，他人が認証に成功しやすくなることはない．

2. 関連研究

前節でも述べたように生体認証の中でも署名認証の重要性は高い．本節では署名認証の関連研究について紹介する．署名認証の関連研究は主に照合時のアルゴリズムを改良したもの，照合時に使用するパラメータを変更したもの，入力方法を変えるものがある．

2.1 DWT と適応信号処理を用いたオンライン署名照合

オンライン署名照合にて筆順や筆圧などのデータを直接照合に用いるのではなく離散ウェーブレット変換（Discrete

wavelet transform,DWT) によるサブバンド分解を用いて多重レベルに分解した信号により照合を行う方法が提案されている [8]．DWT とは時間-周波数の同時分解が可能な圧縮，解析手法である．サブバンド分解をすることで得られた高周波成分では個人の差がより顕著になる．また，筆順（位置情報）だけを用いて照合を行うときに Dynamic Programming(DP) マッチング法を導入することでストローク数の変動を考慮に入れた柔軟な照合が行える．

この手法による実験の結果本人には自筆署名の参照を許さず，詐称者には本人署名をなぞらせる環境下でも識別率約 95 %を達成している．

2.2 ペンの傾きに着目したオンライン署名照合

通常照合に使うパラメータの XY 座標と筆圧に加えて入力時に使用するペンとタブレットの間の角度，ペンの方向にも個人差は見られるという観点で実験を行い，照合率 98.2 %を達成できた [4].

XY 座標，筆圧，ペンの角度，方向を比較する際同一人物の署名であっても時間的な長さはその都度変わるので DP マッチングによって比較する二つの特徴ベクトルを比べた．リファレンスデータの作成方法は 5 回の署名データを DP マッチングで時間正規化を行いそれらの相加平均をとったものとした．ここではペンの傾き，ペン先の位置（XY 座標)，筆圧の 3 つのパラメータを統合して照合を行った．その結果 3 つのパラメータを別々に照合したときと比べてより良い照合率が得られた．

2.3 タッチ情報を利用した手書きサイン認証システム

スマートフォンでは筆圧の時系列データの取得が困難であるとして，サインを書くときの筆記時間，座標情報を積極的に利用する [10]．認証方法は前提として入力は漢字であると仮定し，まず総画数が一致しているか，次にタッチ時間のテンプレートとの差は閾値以内であるか，最後に一画ごとに 10 分割にしてサインの角度の移り変わりを調べた．閾値の決定法は登録するサインの標準偏差の 3 倍を平均値に足したものであった．本論文はこの閾値決定法を参考にしている．

2.4 Kinwrite

Jing らによって Kinect を使った手書き文字認証システム「KinWrite」が提案されている．認証方法は Kinect というジェスチャー・音声認識によって操作できるデバイスの前で指で文字を描き，その 3 D 情報を Dinamic Time Warping(DTW) によってテンプレートと比較し認証するというものである．本論文ではこの論文のテンプレート決定法と閾値設定方法を参考にしている．

DTW を使うためには本人が入力した比較対象となるテンプレートが必要である．本人が入力した複数の情報をすべてそれぞれ DTW によって比較し DTW の距離がほかのどの組み合わせよりも小さくなるものをテンプレートとする．

認証のためには本人と他人を区別するための境界線が必要である．閾値の設定の仕方としては本人拒否率と他人受入れ率をどちらも低くなるように設定しなければならないがこの 2 つはトレードオフの関係にある．この手法では特に他人受入れ率をできるだけ低くしようとしており，具体的にはテンプレートと本人が入力したいくつかの情報，本人以外が入力した偽の情報の DTW 距離をすべて算出し，その中の偽の情報で一番 DTW 距離が小さかったものを DTW 距離の閾値と設定している．

2.5 DTW（Dynamic Time Warping : 動的時間伸縮法)

ここでは本論文でもデータの類似度算出にも用いている Dynamic Time Warping(DTW) について説明する．[7]

二つの時系列データを比較する際，それぞれのデーとタの同時刻における計測値の差の絶対値の和を取ったものはユークリッド距離と呼ばれ，二つのデータの類似度を簡単に計算することができる方法の一つであるが，これは計測値数が同じ時系列データにしか適用できない上，人間の直観に反する結果が出てしまう場合がある．

DTW は片方の時系列データにおける一点をもう片方の時系列データの複数の点に対応づけることで時間方向の非線形な伸縮が可能となる．よって DTW は計測値数の異なる二つの時系列データの類似度をより人間の直観に合うように算出することができる．また，DTW は DP マッチングとも呼ばれる．

これら以外にも署名認証の関連研究は多く見受けられるが，どれも署名入力時には安定した状態での入力が前提である．よって，入力時の周りからの影響を考慮した署名認証は必要であると考えられる．

3. 予備実験

3.1 実験環境の作成

署名認証の研究を行うにあたり，署名データを収集するための実験環境を作成した．実験に使用した機器は Sony の XPERIA（SO-03D) である．タッチしたとき，タッチした位置の座標と本体の加速度，ジャイロスコープの値，回転ベクトルセンサの値を取得するアプリを作成した．また，取得したデータを保存するためには既存のアプリ「Catlog」を用いた．このプログラムを使った予備実験として，署名認証において入力情報と認証精度の関係と，端末本体が静止していない状態で入力すると認証に支障が出るのかどうかという実験を行った．

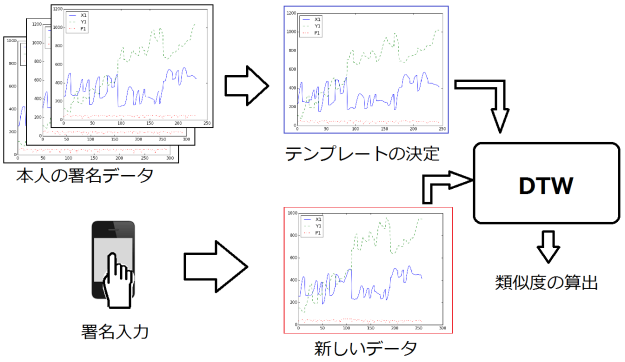

図 2　類似度算出のフローチャート

3.2　DTW による類似度計算

今回収集したデータの類似度を算出するために 2.5 節で紹介した DTW を使う．テンプレートの決定と新しいデータを比較するまでのフローチャートを図 2 に示す．本人の署名データから Kinwrite の手法 [1] と同様にテンプレートを決定する．新たに入力した署名データとテンプレートの類似度を DTW によって計算する．

Python 上で 2 つの時系列データを比較するためにプログラムを作成した．そのうちの DTW の部分については dtw 1.0 というモジュールを使用した [11]．実験の結果である類似度とはこのプログラムで算出される DTW 距離のことをいい，小さいほど二つのデータが似ていることを表している．

3.3　入力する情報量の違いによる認証の精度の違い

例えば，漢字の「一」という字を誰が書いても個人の特徴は出にくいことは容易に想像できる．そこで，署名認証の安全性にはどれくらいの情報量が必要になるのか調べるための実験を行った．

実験のために収集したデータは，3 画，7 画，11 画，15 画，19 画の漢字．（それぞれ「上」，「山内」，「毛利」，「岡村」，「長野」）これらを第一著者が書いたデータと，研究室のメンバーなどの協力者に書いてもらったデータを集め，前述のプログラムを用いて本人拒否率 (False Rejection Rate:FRR) と他人受入率 (False Acceptance Rate:FAR) の等価エラー率を求めた．本人拒否率は本人が入力した署名データとテンプレートとの DTW 距離が閾値以上のものの割合．他人受入率は本人以外が入力した署名データとテンプレートとの DTW 距離が閾値よりも小さいものの割合である．閾値を変化させて本人拒否率と他人受入率が等しくなる時のエラー率を等価エラー率（Equal Error Rate:ERR) と呼び入力する漢字の画数による認証精度の評価を行った．

結果は図 3 が示すように，画数が多いほど等価エラー率が低く認証精度が高いことが分かる．よって今後の実験で用いる漢字入力を「長野」という 19 画の漢字にする．

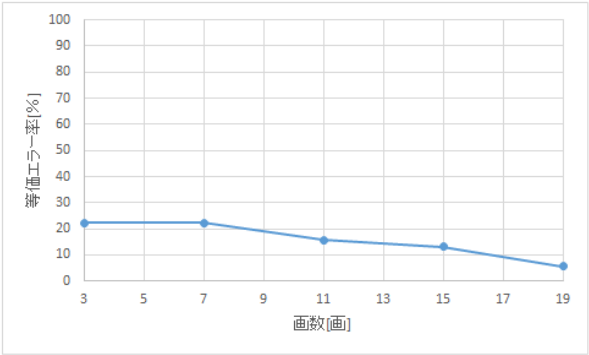

図 3　画数別の等価エラー率

また，丸を書いた場合と「長野」と書いた場合の F 値を測った．F 値とは適合率（precision）と再現率（recall）の調和平均であり，正確性と網羅性の総合的な評価の指標となるものである．閾値は田中らの手法 [10] を用いた．丸を書いたときの F 値は 0.806 であった．「長野」と書いたときの F 値は 0.9286 であった．このことからも，署名登録の際はある程度の情報量が必要であることが分かる．

3.4　本体の動きが認証に影響するか

署名認証の持つ問題点として，環境の影響により認証精度が低下するという問題がある．この問題の影響を実際に調べるための実験を行った．この実験での入力は「長野」という漢字にて行った．また入力時の環境の影響として座った状態での入力，歩きながらの入力，走りながらの入力の 3 つの条件で実験を行った．

座った状態で入力したものから田中らの手法 [10] と同様に閾値を決定した．実験の結果，座った状態で入力したデータの本人拒否率は 0 %であった．歩きながら入力したデータの本人拒否率は 31.3 %であった．走って入力したときの本人拒否率は 81.8 %であった．これより，入力時に本体が動いていると認証精度が低下することが分かる．

4.　提案手法

予備実験から，署名認証において本体の揺れは認証に大きな影響を及ぼすことが確認できた．

スマートフォンは日常的に使われるものであり歩きながら電車のなか，車の中で使用することもある．このように日常生活の中ではスマートフォンの操作中に本体が揺れてしまうことは少なくない．

現在，スマートフォンには様々なセンサが搭載されている．周囲の温度を検出する温度センサ，端末の回転を検知するジャイロセンサ，重力センサ，地磁気センサなどがある．そのなかでもスマートフォン本体の加速度を検出する加速度センサを使うことで本体が揺れた時を検出できるのではないかと考えた．

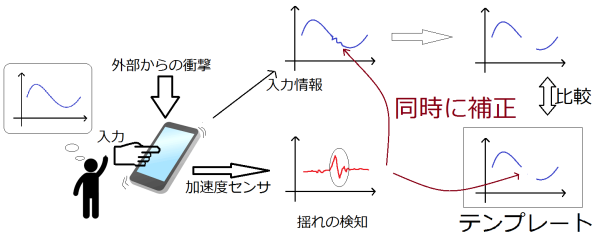

図 4　提案手法のイメージ

4.1　加速度センサの原理

今回使用する機種には 3 軸加速度センサという XYZ 軸の 3 方向の加速度を一度に検出できる MEMS センサの一種が搭載されている．MEMS センサとは半導体式のセンサで従来のものより小型化できるので携帯機器への採用が多い．3 軸加速度センサにはピエゾ抵抗型，静電容量型，圧電型の 3 種類がある．ピエゾ抵抗型は圧力がかかると電気抵抗が変化する半導体を利用したものである．静電容量型は加速度による静電容量の変化を検知するもの．圧電型は圧電効果による電流を検知する方式である．

4.2　提案手法

入力時の本体の揺れという問題に対して，本論文では現在多くのスマートフォンに搭載されている加速度センサを用いて本体の揺れを感知し，その揺れから予想される入力のブレを補正するという手法を提案する．提案手法のイメージを図 4 に示す．

4.2.1　テンプレートと閾値の設定

収集したデータの中から筆者が座った状態で書いたもののデータをそれぞれ類似度計算プログラムにかけて DTW 距離を算出し，Kinwrite の手法と同様にテンプレートを決定する．

閾値の設定法は 2 種類の決め方がある．一つは，田中らの手法 [10] を参考にしたもので，決定したテンプレートと本人のその他の署名データそれぞれとの DTW 距離を算出し，その標準偏差を 3 倍したものと平均値を足したものを閾値とする方法．もう一つは，Kinwrite の手法 [1] と同様に他者の入力とテンプレートを比較した結果で一番 DTW 距離が小さいものを閾値とする方法．二つを比べると後者はその時点で得られているデータの中では他人受入率を 0 %にする方法であり，他人受入率を考える時などには前者を使う．

4.2.2　加速度データの利用

今回は署名の入力中に本体が一度だけ揺れるという状況を仮定して実験を行う．

本論文で提案する加速度データを用いたデータの補正方法を説明する．まず，取得した署名の時系列データを S とする．時刻 t におけるタッチセンサの情報を $\mathbf{s}(t)$ とする．また，x(t),y(t),p(t) をそれぞれ時刻 t における x 座標，y 座標，タッチの圧力とする．

$$S = \Big(\mathbf{s}(1), \mathbf{s}(2), \ldots, \mathbf{s}(T)\Big) \tag{1}$$

$$\mathbf{s}(t) = \Big(x(t), y(t), p(t)\Big) \tag{2}$$

同時に取得した x,y,z 方向の加速度センサの時系列データを，それぞれ A_x, A_y, A_z とする．また，時刻 t における x,y,z 方向の加速度センサの値を $a_x(t), a_y(t), a_z(t)$ とする．

$$A_x = \Big(a_x(1), a_x(2), \ldots, a_x(T)\Big) \tag{3}$$

$$A_y = \Big(a_y(1), a_y(2), \ldots, a_y(T)\Big) \tag{4}$$

$$A_z = \Big(a_z(1), a_z(2), \ldots, _z(T)\Big) \tag{5}$$

署名入力時に一度だけ本体が揺れるという前提のもと，最も加速度センサの値が大きくなった時間を t_{max} とする．t_{max} はそのデータ中の x,y,z 方向の加速度センサの値すべての中で最も大きい値を取ったものを記録した時間 t とする．

ここで得られた t_{max} をもとにデータの一部を取り除いた時系列データを $\hat{S}$ とする．データを取り除く際にデータを取り除く範囲を決める定数を δ とする．

時刻 t での要素とその時刻の前後 δ 個の要素の集合を $S_t(\delta)$ とする．$\hat{S}$ は以下のように求まる．

$$S_t(\delta) := \{\mathbf{s}(t \pm i) | 0 \leq i \leq \delta\} \tag{6}$$

$$\hat{S} = S - S_{t_{max}}(\delta) \tag{7}$$

比較対象となるテンプレートの時系列データを S_{temp} とし，S_{temp} と S の間の DTW 距離を $DTW(S_{temp}, S)$ とする．

S から一部のデータを取り除いたのでそれに対応するデータをテンプレートからも取り除かなければならない．そこで今回は一部を取り除いたテンプレートを $\hat{S}_{temp}(n)$ とする．ここでの n は $-\phi$ から ϕ までの値を取る．

$$\hat{S}_{temp}(n) = S_{temp} - S_{t_{max}+n} \tag{8}$$

そして，最終的に補正したデータと補正したテンプレートを比較した結果得られる DTW 距離を D とする．

$$D = \min_{-\phi \leq n \leq \phi} DTW(\hat{S}_{temp}(n), \hat{S}) \tag{9}$$

ここで δ と ϕ の意味について述べる．

まず δ は加速度センサの値のピークの前後をどの程度取り除くかという数値である．これが小さいと取り除くべきところが取り除けず，本人拒否率の削減が難しい．しかし，削減範囲を広くとってしまうと，3.3 節で議論したように認証に用いる情報量が減ってしまい，他人受入率が上昇してしまう．よって，適切な δ を選ぶ必要がある．今回は経

験的に求めた $\delta = 25$ を用いることにする．

次に ϕ はテンプレートのデータを取り除く際に中心となる点をどの範囲までずらして調べるかという値である．これが無限大に大きいとテンプレートの時系列データの中から隣り合った $2\delta + 1$ 個のデータを取り除く全ての場合について考えることになる．この場合，目的のデータを取り除ける可能性は高くなるが計算量が多くなってしまう．今回は 100 に設定している．

4.3 予想される提案手法の問題点

今回の提案手法は本人が署名データを入力した際の意図しない入力を補正するためのものであるが，この手法を本人以外が署名をまねて入力した時や，間違った入力をした際に補正されてしまわないかという問題が考えられる．

5. 評価実験

5.1 データ収集

データを収集するにあたって単純な形の署名を用いる場合と，複雑な形の署名を用いる場合の二種類用意した．各データはそれぞれ 3 種類の署名データを収集した．また，署名が単純な場合と複雑な場合のそれぞれについて入力者が椅子に座った状態で書いたもの，動きながら書いたもの，第三者が書いたものを集めた．

入力者以外が書いたデータに関しては，9 人の被験者に入力の様子を見てもらったあとで入力を真似て書いてもらうという方法でデータを収集した．

今回単純なデータは縦に一本棒を書いたもの，横に一本棒を書いたもの，丸を一つ書いたものの 3 種類．複雑なデータとしては 19 画の漢字「長野」と書いたもの 1 種類を実験に用いた．

署名を動きながら入力する方法であるが，今回は座った状態で入力しながら途中で本体を少し振ることで入力にブレが発生するようにしてデータを収集した．このデータの現実的なシチュエーションとしては満員電車などで肩がぶつかったとき，車で段差を乗り越える時といった状況を想定している．

5.2 データまとめ

単純な入力をまとめたものを見ると第三者が入力したデータでも真似をすることがたやすいからか DTW 距離が小さくなっている．Kinwrite の手法と同様に第三者のデータで最も DTW 距離が小さいものを閾値とすると本人の書いたデータでも認証されにくくなってしまうことが分かる．縦棒を書いたときの本人拒否率は約３５％。横棒を書いたときは約５８％．一つの丸を書いた場合は 50 %であった．複雑な入力に関して，19 画の漢字「長野」と書いた場合，本人拒否率は約 5.56 %であった．

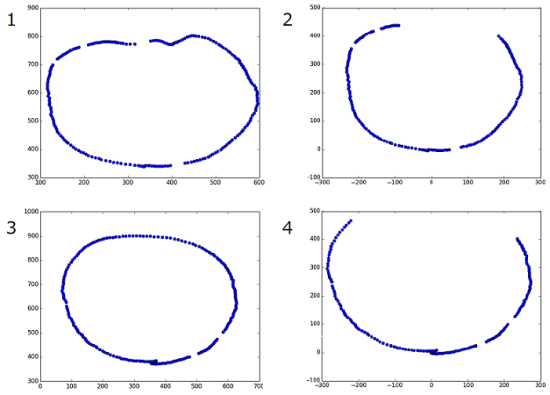

図 5 実際の補正（1:揺れ有補正前，2:揺れ有補正後，3:テンプレート補正前，4:テンプレート補正後）

また，丸を書いた場合と「長野」と書いた場合の閾値を変えたときの本人拒否率と他人受入率から，丸を書いたときの等価エラー率（本人拒否率と他人受入率が交わる点）は約 28 %，「長野」と書いたときは約 5.56 %となった．この結果から実際の署名認証では入力情報が多いほうがより良い結果が得られることが分かる．今回は簡単な入力の中で丸を一つ書いたときと難しい入力（「長野」と書いたとき）で提案手法の補正効果を評価する．

5.3 実験と結果

本論文での提案手法は，加速度センサの値が大きいとき，周辺の座標データを取り除くことで DTW 距離を小さくするものである．丸を一つ書くときにおいて，揺れのあったデータとそれを補正したものをプロットしたものを図 5 に示す．今回は歪みの見られる丸の上部の一部分を取り払っている．

5.3.1 単純なデータ

まず丸を一つ書いたときの実験について結果をまとめる．今回揺れのあるデータ 11 個収集した．図 6 に結果をまとめる．11 個のデータの内，元々の値がテンプレートその他の本人署名データの DTW 距離の平均値である 10.59 より低いもの，ほぼ同じ（10.69）であるものが 4 個あった．それ以外の 7 つのデータに補正をかけるとそのうちの 6 個の DTW 距離が小さくなった．その下がり幅が一番大きかったものは 5.35 低下し，平均値は約 2.6 となった．田中らの手法 [10] と同様に閾値を設定すると閾値は 23.31 になり本人拒否率が 18.2 %となった．これを補正用のプログラムを用いて補正すると本人拒否率は 0 %になった．閾値を設定したものの 91.9 %つまり 21.41 に減らすと補正後の結果が 0 %より大きくなった．

補正前後のデータと第三者入力データをそれぞれ補正プログラムにかけた場合の F 値の変化も算出した．補正前は F 値が 0.563 だったものが，補正後は 0.759 となった．

また，この補正プログラムが揺れがあったところをきちんと補正しているのか確認するための実験を行った．実

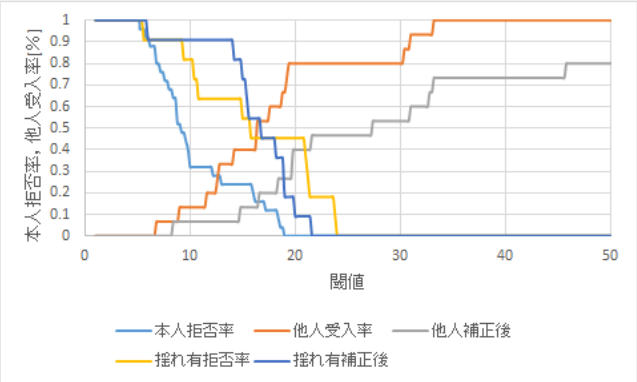

図 6　実験データまとめ（丸）

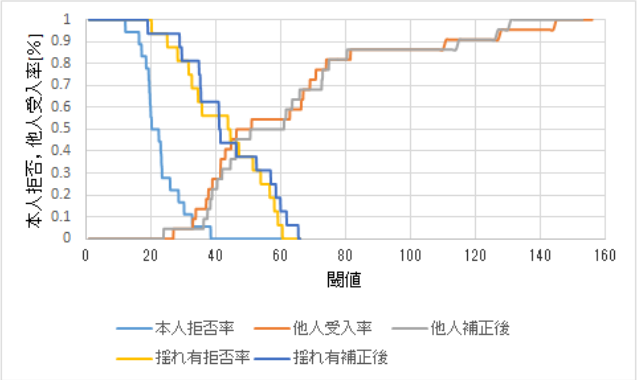

図 7　実験データまとめ（長野）

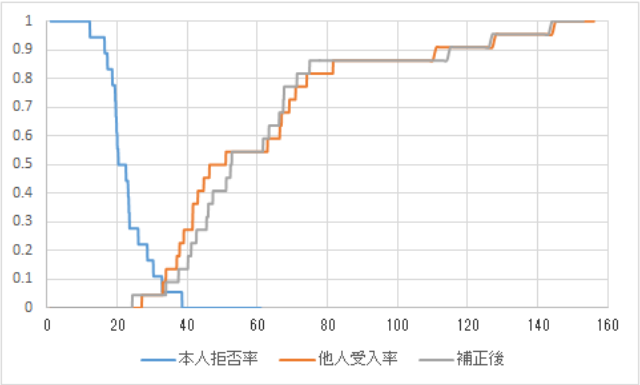

図 8　他人の入力を補正したとき（長野）

験方法は，座った状態で本体を揺らさないように一部が変形した丸を入力する．補正後に DTW 距離が縮んでしまっているものがあったが，それらの補正のされ方を確認すると偶然にもそれらはすべて丸にブレがあるところが補正されていたことが分かった．

5.3.2　複雑なデータ

次に「長野」という文字を書いたときのデータについて，結果を図 7 にまとめる．揺れのあるデータ 16 個収集した．閾値を 41.48 に設定すると，本人拒否率が 56.3 %だったものが，補正後は 43.8 %まで減った．補正前後のデータと他人入力のデータをそれぞれ補正プログラムにかけた場合の F 値の変化も算出した．補正前は F 値が 0.368 だったものが，補正後は 0.439 となった．

揺れ補正プログラムを他人の入力データに使うとどうなるかという実験の結果を図 8 に示す．補正した他人受入率の曲線が補正前より左にシフトされたならば，他人の入力を間違えて補正してしまったということになる．としかし，今回の図 8 を見ると，この補正の結果は補正前より明らかに左にシフトしているとは言えない．また，本人拒否率の曲線との交点も補正前と同じなので等価エラー率も変わらない．

表 1　実験結果まとめ

	本人拒否率		F 値	
	補正前	補正後	補正前	補正後
簡単な入力	18.2	0	0.563	0.759
難しい入力	56.3	43.8	0.368	0.439

各データについての本人拒否率と F 値の補正前後の変化を表 1 にまとめる．

5.4　考察

本研究の目的は，本体の揺れを加速度センサで読み取り，データを補正して本人拒否率を下げるというものであった．

まず，単純な入力データについて考察する．今回の実験では提案手法のプログラムを使用することで，本人拒否率が 18.2 %だったものが補正後は 0 %になった．複雑な入力では本人拒否率が大きくなったことを見ると，単純な入力であるのでこのように本人拒否率が 0 %という結果になったのだと考えられる．閾値を下げると他人受入率が下がり，認証の精度が向上するが，今回のように入力データが単純なものの場合，閾値を下げるという選択肢も出てくるだろう．

一部が変形した丸を書いた実験では，揺れが起きたところを偶然補正したとき以外は DTW 距離が小さくなることはなかった．よってプログラムは揺れがあれば補正し，なければ補正しないプログラムであるといえる．加速度センサが取った最大の値がある値を超えない場合は補正をしないように閾値を設定することで問題を解決することができると考えられる．閾値の設定については揺れのある状況でとったデータの中でもっとも小さかった値が 2.5 であり，揺れのない状態でとったデータで最も大きい値が 1.8 だったため今回は 2.0 に設定するとうまくいった．この閾値設定は今回実験に使用した実験機器の機種が一種類だったということもあり普遍性は保証できない．よってほかの機種や状況での実験が課題として残っている．

次に，複雑な入力データについて考察する．今回の実験では本人拒否率が 56.3 %だったものを 43.6 %にまで減らすことができた．本人拒否率は下がっているが補正前の本人拒否率が元々高かったことに加えて，補正後も劇的に改善されたとは言い難い．単純なデータでの補正ができているのでプログラムの改良により難しいデータの補正も可能であると考えられる．

第三者が入力したデータをプログラムにかける実験の結果，本人拒否率と他人受入率との交点である等価エラー率は変わらなかった．この場合も入力時には本体には揺れはない．よって，加速度センサの結果に閾値を設けることで偶然補正される確率を減らすことができると考えられる．他人入力時のデータを補正プログラムにかけたときの結果を見ると，単純な入力，複雑な入力ともに補正後のグラフが左にシフトしているとは言えない．よってこのプログラムで第三者の入力を誤って補正してしまうことはないと考えられる．

また，補正前後のデータと他人入力データの F 値の変化を記す．単純な入力では，0.563 から 0.759 に変化した．複雑な入力では，0.368 から 0.439 に変化した．どちらの F 値も大きくなったことから，このプログラムによって認証精度が上昇したと言える．

6. まとめと今後の課題

スマートフォンの普及率増加に伴い個人情報などの重要なデータを持ち運ぶ人は増えている．しかし，現状のスマートフォンのセキュリティは覗き見攻撃への耐性が十分とは言えない．

覗き見攻撃に耐性のある認証法の一つとして署名認証がある．署名認証の抱えている問題点の一つに入力時の環境の変化が照合の精度を下げる可能性があるというものがある．日常的に署名認証を用いるには，電車や車などのスマートフォンが揺れて入力がぶれてしまうような環境の変化しうる場所での安定した照合も求められている．

本論文では実際に単純な署名認証システムを作り様々な条件での実験を試みた．まず予備実験として動きながらの入力を行うと本人拒否率が増加し，ここに改良すべき点があることが判明した．そして実際にデータの入力時に座標の時系列データと同時に取得した本体の加速度センサの値の変化から座標データに修正を加えるという実験を行った．単純な入力（丸を一つ）の場合，補正前は本人拒否率が 18.2 %あったものを補正後は 0 %にすることができたが補正後の本人拒否率が 0 %となっているのは現実的に見て信用できるデータとは言えない．複雑な入力（「長野」という二文字）の場合，補正前の本人拒否率は 66.7 %だったが補正後は 58.3 %になった．これはあまり良い結果とは言えないので改良が必要であると感じた．また，同時に行った実験で，第三者の入力を誤って補正しないことも分かった．

現在 XY 座標，圧力の 3 つのパラメータを一つのリストに入れて類似度計算をし，加速度センサから補正をかける時もまとめて補正している．この現在の手法に対して次のような新たな手法による実験も必要である．それぞれ座標データと圧力データを別々に類似度計算をしてその相加平均や相乗平均をとる，また，加速度センサは XYZ の 3 軸でとっているのでそれぞれを別々に使うという手法の実験．揺れが見られたところとその前後の 3 つのエリアに分け，揺れが起こったところの類似度には少し補正（たとえば 0.5 倍）をして 3 つの値を出してその平均を取るという手法の実験．加速度データがどれくらいの値を取れば補正をするのかという閾値を設定するためにほかのスマートフォンの機種での実験も必要である．

今後はこれらの二つの新しい手法の実験を進めるとともに，DTW 以外の類似度計算アルゴリズムを使用した際の結果との比較，今回はデータ入力中の揺れを 1 回に限定していたが複数回の揺れに対する補正ができる手法を考える．

7. 謝辞

本研究を進めるにあたり，ご多忙にもかかわらず熱心にご指導頂きました，櫻井幸一教授，川本淳平助教，松本晋一様，穴田啓晃様に心から感謝致します．また，実験に協力頂きました櫻井研究室の皆様に心から感謝致します．

参考文献

[1] Tian, J., Qu, C., Xu, W., & Wang, S. (2013, February).“KinWrite: Handwriting-Based Authentication Using Kinect.” In NDSS.

[2] Plamondon, Rejean, and Guy Lorette. “Automatic signature verification and writer identification—the state of the art.” Pattern recognition 22.2 (1989): pp.107-131.

[3] Fierrez-Aguilar, Julian, et al.“An on-line signature verification system based on fusion of local and global information.” Audio-and video-based biometric person authentication. Springer Berlin Heidelberg, 2005. pp.523-532

[4] 山中晋爾, 浜本隆之, and 半谷精一郎. “ペンの傾きを利用した署名照合方式の改良.” 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ 100.77 (2000): pp.65-72.

[5] 山崎恭, and 小松尚久. “カテゴリー化された筆跡情報に基づく個人性抽出手法.” 電子情報通信学会論文誌 D 79.8 (1996): pp.1335-1346.

[6] 東山侑真, 岡村真吾, 矢内直人, 藤原融. “タッチパネル端末の特性を利用した覗き見攻撃耐性をもつ個人認証手法”Computer Security Symposium 2014 October2014 pp.1023-1028

[7] 内田誠一.“DP マッチング概説: 基本と様々な拡張 (テーマセッション (2), パターン認識・メディア理解のための学習理論とその応用).” 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 106.428 (2006): pp.31-36.

[8] 中西功, et al. “DWT によるサブバンド分解と適応信号処理を用いたオンライン署名照合.” 電子情報通信学会論文誌 A 87.6 (2004):pp.805-815.

[9] 中村善一. “日本語筆跡に現れる個人性の抽出とオンライン筆者照合に関する研究.” 奈良先端科学技術大学院大学博士論文 (2008).

[10] 田中優輝, 吉田孝博, 半谷精一郎. “スマートフォン上で得られるタッチ情報を利用した手書きサイン認証システムに関する研究” Symposium on Cryptography and Information Security January2015,20-23

[11] python; Package Index; dtw; 1.0 `https://pypi.python.org/pypi/dtw/1.0` (accessed 2015-2-10)