表面筋電位を用いた認証システム実現のための個人識別手法の提案

黒木　聡舜 [a)]・山場　久昭 [b)]・油田　健太郎 [c)]・岡崎　直宣 [d)]

A Proposal of a User Identification Method for Realizing an Authentication System Using s-EMG

Tokiyoshi KUROGI, Hisaaki YAMABA, Kentaro ABURADA, Naonobu OKAZAKI

Abstract

At the present time, mobile devices such as tablet-type PCs and smart phones have widely penetrated into our daily lives. This movement caused a new threat that a stranger takes a peek at our authentication operations on our touch screens and steals our passwords and steals our important information and data in our mobile devices. This forced us to develop new authentication method that can prevent this sort of crime called a shoulder surfing attack. We have investigated a new user authentication method for mobile devices that uses surface electromyogram (s-EMG) signals, not screen touching. The s-EMG signals, which are generated by the electrical activity of muscle fibers during contraction, can be used to identify who generated the signals and which gesture he made. We introduced a pass-gesture, which is a list of hand signals, to realize the s-EMG based authentication method. In this paper, we propose two methods to compare two s-EMG signals and judge whether the two were made by the same gesture or not. One uses Support Vector Machines and the other uses Dynamic Time Warping method. We also introduced the appropriate method to select validate data to train SVMs using correlation coefficients and cross-correlation functions. A series of experiments was carried out to confirm the performance of the proposed methods. From the results of the experiment, we confirmed that the effectiveness of the two methods.

Keywords: user authentication, s-EMG, correlation coefficient, cross-corelation, SVM, dynamic time warping

1. はじめに

モバイル端末の既存のユーザ認証手法は覗き見耐性が十分であるとは言えない。スマートフォンやタブレットのようなモバイル端末の普及に伴い、覗き見によって認証に必要な情報が第三者に取得されてしまい、容易に認証を突破されてしまうという問題が起きてきている [1)]。通常、他人にモバイル端末を使用されてしまうことがないように画面ロックをかけ、その解除にあたっては個人認証が必要となるようにしている。特に、モバイル端末には電話帳やメールといった個人情報が格納されており、そのような情報の漏洩を防ぐためにも、個人認証を行うための認証情報の安全性の重要性は増してきている。しかし、既存の認証方式、例えばPINやAndroid端末に採用されているパターン認証などでは、覗き見により認証状が容易に取得されてしまう [2)]。

覗き見に対する耐性を与えるための接近法としては、指紋などの生体情報を用いた生体認証手法が注目されている [3)4)]。覗き見されても安全な認証を実現するには、覗き見されてもユーザ以外が認証を突破できないようにする、または、そもそも覗き見されない形で認証ができる手法が考えられる。生体認証手法を用いることにより、それらを実現とすることが期待できる。

筆者らはこれまで、このような生体情報の一つである表面筋電位に注目し、これを用いた認証が実現可能かどうかの検討を行ってきた [6) – 13)]。この手法では、手首から先の手の動き（以下、ジェスチャーと呼ぶ）に応じて、前腕部の筋電位が異なる波形を示す [6, 7)] ことを利用し、いくつかのジェスチャーの組み合わせをパスワードとして用いている [8, 9)]。すなわち、パスワードとして用いるジェスチャの筋電位の波形を登録しておき、それと同じ波形が入力されれば本人として認証する。

その実現には、得られた筋電位の波形同士を比較し、それらが類似しているか否かによって二つのジェスチャが同じものかどうかを計算機で自動判定することが必要である。以前の研究では、サポートベクターマシン（Support Vector Machine、以下SVM）を用いることにより、ユーザ毎に一つのジェスチャ判別器を用意して、ジェスチャを分類する手法について検討を行った [10, 11)]。しかし、精度の点で改善が必要であった。

そこで本研究では、新たにSVMを用いて、各ユーザのそれぞれのジェスチャ毎に判別器を用意する手法 [12)] と、動的時間伸縮法（Dynamic Time Warping、以下DTW）を用いて識別を行う手法 [13)] の2つを共に検討した。

以下、第2節ではモバイル端末の個人認証の課題、第3節

[a)]工学専攻機械・情報系コース大学院生
[b)]情報システム工学科助教
[c)]情報システム工学科准教授
[d)]情報システム工学科教授

では筋電位を用いた個人認証手法について説明する。第4節では筋電位の波形からジェスチャーをSVM、および、DTWを用いて識別する提案手法について述べ、第5節ではその性能評価実験の結果について述べる。

2. モバイル端末の個人認証の課題と対抗策

本節では、モバイル端末の従来の認証方式と、それへの脅威としての覗き見攻撃、及び、対策として期待される生体認証について、説明する。

2.1 従来の認証方式

現在、モバイル端末の個人認証としては、PIN認証やパターン認証等が広く用いられている。モバイル端末の普及以前より、数字やアルファベットの組み合わせ認証情報として用いるパスワード認証やPIN認証が用いられてきた。これらは、モバイル端末でも主要な認証方式の一つとして使用されている。その後、モバイル端末の普及に伴い、画面上の9つの点を結んだパターンを認証情報に用いるパターン認証が使われるようになってきている。ユーザは、画面上に表示された点と点の間を指でなぞることによって、登録したパターンを入力する。これは、Android端末に標準搭載されている認証方式である。

ただしこれらの認証方法は、第三者に覗き見られた場合に、認証情報が容易に盗まれてしまい、覗き見攻撃への耐性が十分であるとは言えない。

2.2 覗き見による認証情報の窃取

正規ユーザの認証行為を覗き見することによって、暗証番号やパスワードといった秘密情報を不正に取得する行為を、覗き見攻撃と呼ぶ。覗き見による攻撃方法は大きく2つに分けることができる。1つは「第三者が認証画面を直接覗き見することによる攻撃」(目視による攻撃)であり、もう1つは「ビデオカメラ等を利用した、認証画面の録画画像を用いた攻撃」(録画攻撃)である。

目視による攻撃の場合、特に機材を必要としないので、被攻撃者のそばによるだけで攻撃を実行できるため、端末の利用者は周りにその様な者がいないか、常に注意を払う必要がある。だだし、人間の記憶力や処理能力に限界があるため、認証手順を複雑にしたり、パスワードの桁数を増やすことで、攻撃者が認証情報をすべて記憶することを困難にすることができる。しかしながら、認証方法を複雑にしすぎると、正規のユーザにとっても使いにくいものになってしまうことに注意が必要である。

録画攻撃とは認証画面と認証操作の様子を撮影し、その後、録画した映像記録を解析して個人情報を取得するという方法である。目視による攻撃とは異なり、認証方法を複雑にしても対応が困難であり、録画攻撃への対策は容易ではない。[14, 15, 16, 17, 18]。録画攻撃への対策としては他人に覗き見られることのない環境で認証動作を行うという事が挙げられる。しかし、我々の生活環境にはいたる所に監視カメラが設けられており、意図的でなくとも認証動作が録画されてしまい、個人情報が漏洩される可能性が否めなくなっているため、どのような対策を用いるかが問題となっている[5]。

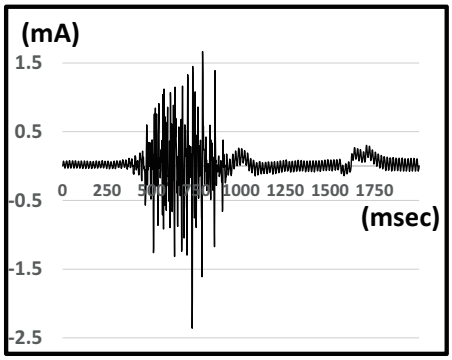

図1. 筋電図.

録画攻撃も含めた覗き見攻撃への対策手段としては、覗き見を困難にさせることばかりでなく、覗き見をされた場合にも安全性の確保ができるようにする対策が必要不可欠である。

2.3 生体認証

生体認証(バイオメトリクス認証)とは、人間の身体的特徴(生体器官)や行動的特徴(癖)を用いて本人認証を行う技術である。PIN認証やパターン認証などの現在の主流の認証手法と比較して、なりすましが困難であることから、より強固なセキュリティを有することが期待されている[3)19)20)]。生体認証への利用に適した生体情報の条件としては、全ての人が持つ特徴であること、同じ特徴を持つ人がいないこと、時間によって特徴が変化することないといった条件が挙げられる。具体的な認証情報としては、身体的特徴としては、指紋、掌形、虹彩等、行動的特徴として筆跡、リズム等があげられる。

3. 表面筋電位を用いた個人認証手法の提案

ここでは、生体情報の一つとして、筋電位を用いて個人認証を行う手法の基本的な考え方を説明する。

3.1 筋電位

筋電位とは脳から送られた信号が筋線維に伝達された際に生じるものであり、神経細胞が細胞内外の電位を変化させる事で測定する事が可能である。観測された電位の変化は図1のような筋電図として記録できる。皮膚表面で計測された筋電位を表面筋電位、またはs-EMG (surface electromyogram) signal という[21)]。

計測される筋電位は、どの筋肉をどのように動かすかによって異なる。この性質を利用して、筋電位を様々な機器への入力情報として活用する研究が、多方面で行われている。例えば田村等は、顔の皮膚表面から得られる筋電位を表面筋電計を用いて測定・解析して表情筋の動作を推定し、その動作を入力として用いることで車椅子を制御するハンズフリー車椅子の開発を行っている[23)]。また、指文字や手話といった医療研究でも表面筋電位は幅広く用いられている[24, 25, 26, 27, 28)]。

3.2 筋電位を用いた個人認証の基本的な考え方

筆者らが提案する手法では、計測される筋電位の波形がジェスチャー毎に異なる事、および、同じジェスチャーであっても、人によって波形が異なること利用する。すなわち、図2に示すような一連のジェスチャーをパスワード(認証情報)と

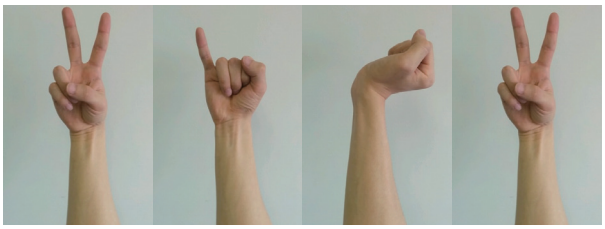

図 2. 登録をしたパスワード（ジェスチャー列）.

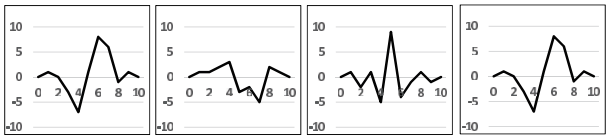

図 3. 対応する筋電図.

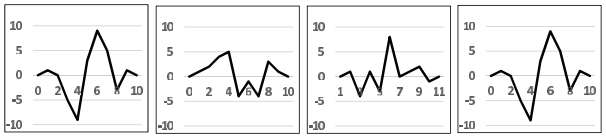

図 4. 所有者が入力した認証動作を測定した波形.

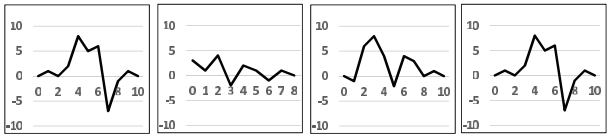

図 5. 攻撃者が入力した認証動作を測定した波形.

して用いる。

その基本的な考え方は次の様なものである。まず、それぞれのジェスチャーの波形（図 3）をモバイル端末上に登録しておく。所有者がそのモバイル端末を使用する時には、図 2 のジェスチャーを再現する。すると、図 4 に示すような、登録されている（一連のジェスチャーの）筋電位の波形と似た波形が測定されるはずであり、認証は成功する。一方、認証動作を覗き見した攻撃者が同じジェスチャーを行ったとしても、測定される筋電位の波形には個人差があるため（図 5）、認証を成功させる事ができない。すなわち、たとえ認証情報が攻撃者に知られてしまっていても、安全を確保できる手法となっている。

さらにこの手法では、ポケットの中のような人目にふれないといった環境でジェスチャを行うことができるため、パスワード認証や PIN 認証とは異なり、タッチパネルを目視して確認しながら認証動作を行う必要がない。すなわち、認証に筋電位を用いることには、覗き見されずに認証動作を行う事ができる利点もある。これを活かせば、覗き見攻撃に対する安全性を更に確保する事ができると考えられる。

3.3 提案手法の運用形態

提案する筋電位を用いた個人認証システムを実際に利用する局面は、

1. ユーザの皮膚に接触させた電極で感知した表面筋電位を、
2. その電極と接続されている筋電位計を用いて記録し、
3. その記録された表面筋電位のデータを携帯端末に転送し、
4. 事前に端末上に登録しておいたパスワード（ジェスチャー：筋電図の列）と比較、照合し、認証を行う、

というステップになる。

そのために必要なハードウェア構成としては、腕時計状のウェアラブルデバイスの表面筋電計の機能を搭載したもので携帯端末と通信させ、認証動作（ジェスチャー）を行い、個人認証を行う事が考えられる。実際に腕時計のバンドの裏に電極を搭載し、その電極から表面筋電位を測定し、測定結果は Bluetooth 等を用いて携帯端末に送信する、という形が考えられる [29, 30, 31]。

4. 筋電位の比較によるジェスチャの判別法

4.1 筋電位によるジェスチャの判別とその課題

筋電位計で測定して得られた波形を用いた個人認証システムを実現するには、筋電位の波形からジェスチャーの特徴を的確に捉えた特徴量の抽出することと、その特徴量同士を比較し、2 つの筋電波形が同一か否かの判定を行う適切な手法が必要である。既存の研究としては、高速フーリエ変換を用いて表面筋電位の特徴抽出を行い、抽出された特徴量同士の比較から、登録されている波形と新たな入力波形が類似しているか否か、すなわち同一のジェスチャーであるか否かの判定を行う方法などが報告されている。例えば Tamura 等は、波形が取る最大値と最小値との差を筋電位の特徴として用いる手法が、高い識別率を示すことを報告している [23]。

我々は以前の研究で、波形の最大値と最小値を筋電位の特徴として採用し、判別手法として SVM を用いる手法を報告している [12]。この時は、ユーザ毎にただ一つの判別器を用意し、複数のジェスチャのうち、入力された波形がどれであるのかをクラス分けするものであった。しかし、この方法での個人認証の精度は、十分なものではなかった。

そこで本研究では、ユーザ毎に、パスジェスチャを構成するジェスチャそれぞれの判別器を用意しておく方法を検討する。被験者ごとに、それぞれのジェスチャの筋電位を繰り返し計測し、それらを用いて SVM を訓練し、各ジェスチャ毎の判別器を生成する。そのような判別器を生成する方法として、SVM を用いた識別手法と、動的時間伸縮法を用いた識別手法をともに検討する。

また、それらの手法で必要となる学習用のデータの選択にも注意が必要であり、適切な選択方法についても合わせて検討を行う。実際に表面筋電位を計測する際には、波形に稀にノイズや波形の乱れが含まれてしまう事がある。判別器の生成にこのような波形データを採用してしまうと、得られる判別器の性能が不十分なものとなってしまうことが懸念される。そこで、適切な学習が行われる様に、学習に適したデータを選出する方法についても提案を行う。

4.2 提案手法の基本的な考え方

本研究では、ある被験者の判別器の生成には、その被験者のデータのみを用いることとする。この様な方法を取ったわけは、正規の所有者以外の人全てについての波形データを用意し、それらを負例として学習させることは原理的に不可能であること、また、この手法が実用化された場合においても、それぞれのユーザが自分のパスワードを登録する局面において、判別器の訓練に利用できるのは、本人のデータだけだか

らである。

ただし、この学習方法で得られた判別器群は、基本的には当該のジェスチャの特徴を捉えたものになっているはずであり、他人の筋電位の値を入力して与えた時に、それを拒否することが期待できる。しかし、他のユーザの筋電位の波形が入力された時、それを間違った入力であると判定する様には訓練されているわけではない。すなわち、他人を本人として受け入れてしまう割合（False Acceptance Rate）は、本人を誤って拒否してしまう割合（False Rejecting Rate）よりも大きくなると考えられる。

そこで、複数のジェスチャを組み合わせたパスジェスチャを用いて認証を行う際には、パスジェスチャを構成する全てのジェスチャが正しいと判定された時に認証が成功、一つでも間違っていると判定されたら、認証は失敗するという方針を採用することとした

また、この方針から、本手法では、図 2 のような一連のジェスチャー列（n 桁）を作成するにあたり、本人拒否率が最も低かったジェスチャー上位 n 個を選択するものとする。予備的実験の結果から、本人拒否率の良いジェスチャ、悪いジェスチャが存在し、それらは被験者によって異なることがわかっている。このことを受け、前述の判別器生成方針のもとでは、生成される判別器を用いた時の他人受入率の性能が予測困難であることをも合わせて考え、本人拒否率の良いジェスチャであることを優先して用いることとしたわけである。

4.3 学習用データの選択

4.3.1 標準波形の考え方と類似度の導入

既に述べた様に、表面筋電位を計測した際、波形に稀にノイズや波形の乱れが含まれてしまう事がある。この理由としては、計測時の電極の大幅なズレや筋痙攣、静電気など、様々なものが考えられる。判別器の生成にこのような波形データを採用してしまうと、得られる判別器の性能が不十分なものとなってしまうことが懸念される。

そこで本研究では、測定した波形データ数（n_0 個）の中から、判別器の訓練に適したデータだけを選出する方法として、標準波形と呼ぶものを利用する方法を採用する。具体的には、当該のジェスチャの特徴を最も反映されていると期待できるデータを標準波形として選んでおき、それと類似しているとみなせるものだけを学習用データとして採用する。

標準波形の選出には、相関係数を用いる。相互係数は -1 から 1 の値をとり、類似度を測る指標となる。0 に近いほど無相関であり、-1、1 に近いほど強い相関があると言うことができる。測定した波形データ群から 2 つを取り出した全ての組み合わせについて相関係数を求め、他との相関係数の平均が最も大きい波形のデータを標準波形とすることとした。その上で、この標準波形に類似しているデータを選んで、学習に用いる。その類似度の指標としても、相関係数を利用する。すなわち、標準波形との間の相関係数の値がより大きい波形のデータ群を学習に用いるわけである。例えば、後述する SVM の性能評価実験では、n_0 個のデータから、相関係数の値の大きい上位 n 個のデータで SVM を学習させるものとしている。

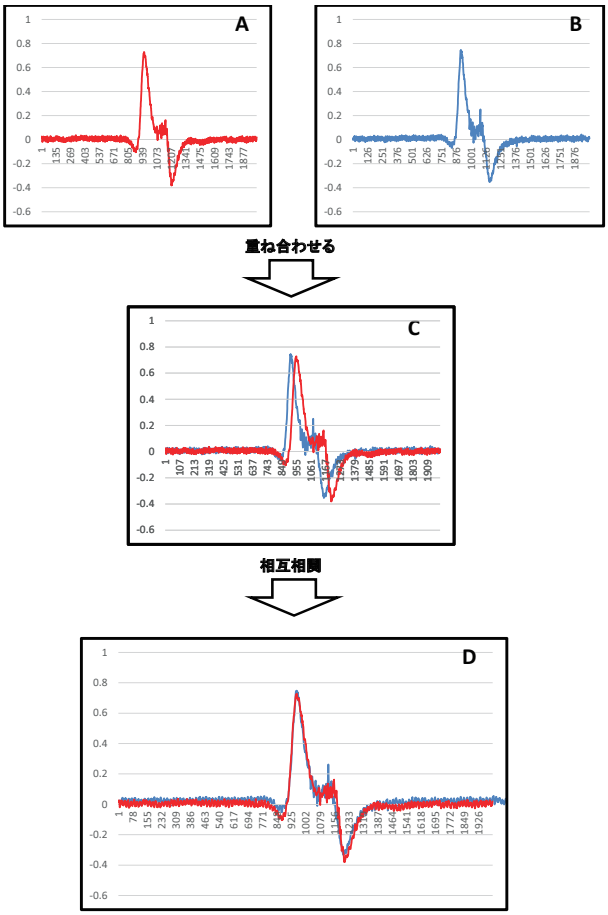

図 6. 相互相関関数を用いた例.

4.3.2 ジェスチャの開始タイミングの揺れへの対策

2 つの波形の相関係数を求めるに際して、それぞれのデータの中での、ジェスチャの開始時刻にズレがあると、得られた相関係数の値が不適切なものとなる恐れがある。例えば、図 6 の A と B のように、同じ被験者の同じジェスチャの筋電波形が 2 つあった時、それぞれの測定開始時刻を基準として 2 つの波形を重ね合わせると C のようになり、このまま相関係数を求めても、それほど高い相関はないという結果になってしまう。この例の場合、B を横軸の正方向にシフトして重ねると D の様になり、A と B はかなり一致した組み合わせであるという結果を得ることができる。測定開始時刻からジェスチャの開始時刻までの間隔が異なってることにより、このようなズレが生じてしまう。

そこでこの問題を改善するため、相互相関関数を利用することとした。相互相関関数は、2 つの信号・配列の類似性を確認するために用いられる手法の 1 つである。2 つの信号の畳み込みの式を以下に示す。

$$(f * g)(m) = \sum_{n} f(n)g(m-n) \tag{1}$$

この相互相関関数を最大とする m を求め、m だけずらした時の f と g の相関係数を 2 つの信号の類似度として採用するようにする。

4.4 SVM を用いる識別手法

4.4.1 Support Vector Machine

SVM とは教師あり学習を用いるパターン認識モデルの 1 つであり、分類や回帰等に適応が可能である。カーネルトリックと呼ばれる方法を用いて、非線形の識別関数を構成できるように拡張したサポートベクターマシンは、現在知られている多くの手法の中でも最も認識性能の優れた学習モデルの一つであり、線形入力素子を利用して 2 クラスのパターン識別器を構成する手法である。訓練サンプルから、各データ点との距離が最大となるマージン最大化超平面を求めるという基準（超平面分離定理）で線形入力素子のパラメータを学習する。SVM はデータの特徴の次元が膨大になっても識別の精度が高く、最適化するべきパラメータが少なく算出が容易であるという利点がある。

4.4.2 使用する特徴量

本研究では、SVM に学習させる特徴量として、総和、平均、標準偏差、平方和、歪度、尖度、5 数要約（最小値、下側ヒンジ、中央値、上側ヒンジ、最大値）の計 11 種類を導入した。ただし、波形全体からこれらの値を得ても不十分と考えられたので、図 7 に示す様に筋電波形を 10 分割し、その分割した部分それぞれからこれらの 11 種のデータを取り出すこととした。すなわち、1 回の計測データを、総計 110 個の値で表現することとした。

4.4.3 学習の手順

被験者 i のジェスチャ j の判別器をトレーニングする際には、被害者 i のジェスチャ j のデータを正例、被験者 i の j 以外のジェスチャを負例として SVM に与える。この時、被験者 i のジェスチャ j の計測データそれぞれから、前述の特徴量を算出する。それら 110 のデータを用いて、SVM を学習させる。

1. 被験者 i のジェスチャ j の計測データから、前述の方法で標準波形を選ぶ。
2. 標準波形を用いて、学習に利用するデータ（n 個）を選ぶ。具体的な選び方は、実験の節を参照。
3. 被験者 i のジェスチャ j の計測データそれぞれから、前述の特徴量を算出する。
4. 被験者 i のジェスチャ j の判別器 D_j^i は、被験者 i のジェスチャ j のデータを正例、被験者 i の j 以外のジェスチャのデータを負例として、SVM を訓練することによって生成する。

4.5 動的時間伸縮法を用いた識別手法

4.5.1 動的時間伸縮法

動的時間伸縮法（Dynamic Time Warping、以下 DTW）は、速度が異なる 2 つの時系列間の類似度を測定するための時系列解析アルゴリズムの 1 つである。2 つのシーケンス（例えば時系列）間の最適な一致を特定の制限で計算する。この手法の特徴は時間次元における特定の非線形変化とは無関係に類似性の尺度を決定することである。DTW では 2 つの時系列の各点の距離を総当りで比較した上で、系列同士の距離

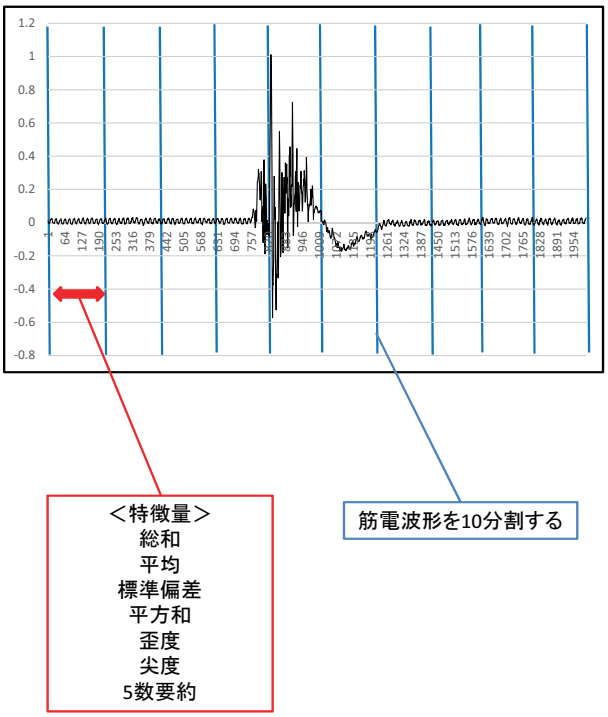

図 7. 選択した特徴量.

が最短となるパスを見つける。これが DTW 距離になる。そのため、2 つの系列の周期性 / 長さが違っても DTW 距離を定義することができる。DTW 距離の値が小さければ小さいほど類似度が高いことを意味する。

DTW は、データマイニングに加えて、ジェスチャ認識、ロボット、音声処理、製造で用いられている [32, 33, 34, 35, 36, 37]。

4.5.2 動的時間伸縮法による判別器

基本的には、SVM を用いる手法と同様、相関係数と相互相関関数を用いて標準波形を選出した上で、入力されてきた波形と、この標準波形との DTW 距離が、ある閾値よりも近い場合には同じジェスチャー、遠い場合は異なるジェスチャであると判定する。

閾値の決め方は、本人拒否率（false rejection rate）を小さくする方向を指向し、各ユーザの各ジェスチャ毎に、計測された n 個の波形データであれば、すべてが当該ジェスチャであると判定される様に決めることとする。すなわち、具体的には、標準波形以外の $n-1$ 個の波形と、標準波形との間の DTW 距離をそれぞれ算出し、最大の DTW 距離の値を閾値とする。

ただし、閾値を大きく取ることによって、他のユーザのジェスチャの波形を受け入れる可能性が高くなってしまう。そこで後述する実験では、この他人受け入れの割合を小さく抑えられる様、本人拒否の割合とのバランスで、閾値の値を調整する試みもあわせて行う。

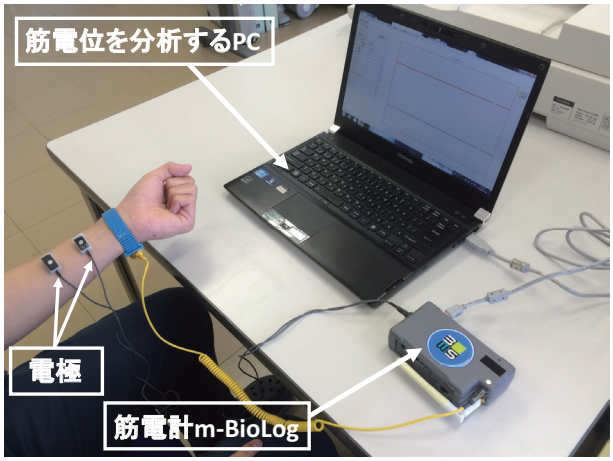

図 8. 筋電計 m-BioLog 計測の様子.

表 1. 識別実験のデータ取得に用いた機器とソフトウェア.

電極	筋電センサー（DL-141）
データロガー	バイオログ（DL-3100）
計測ソフトウェア	m-BioLog

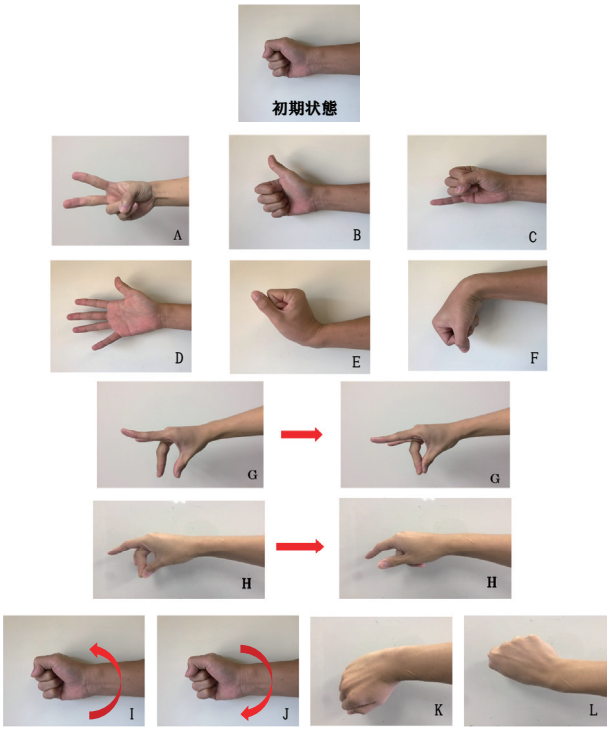

図 9. 予備実験で用いたジェスチャー候補.

5. 提案識別手法の性能評価実験

5.1 ジェスチャと筋電位の計測

5.1.1 使用した筋電位計

ジェスチャーの識別に使用する表面筋電位の測定は、以前の研究でも用いた S&ME 社の筋電位計（データロガー DL-2000 と筋電位センサ DL-141 の組み合わせ）で行なった [31]。測定の様子を図 8、機器情報を表 4.1 に示す。筋電位の測定は、筋電計を机の上に置き、計測者が椅子に座り、手のひらを上に向けた状態で行った。電極の貼り付け位置は、前腕部の手のひら側で、手首から肘に向かって数 cm の位置とした。詳細な位置は、どの位置に電極を装着すると波形が表れやすいのか、各被験者毎に予備実験に行い、その結果に基づいて決定した。また皮膚と電極間の接触抵抗を小さくするために、電極を貼る前に専用のクリームで皮膚の皮脂を除去し、アルコールを含まない綿でクリームをふき取ってから貼り付けた。

5.1.2 ジェスチャー候補とその計測

本研究で用いるジェスチャー候補として、図 9 に示す A〜L の 12 パターン（チョキ、親指、小指、パー、手の甲側に向けてひねる（伸展）、手の平側に向けてひねる（屈曲）、中指と薬指と親指を 2 回合わせる（ダブルタップ）、クラップ、前腕を下方向に 90 度回転させる（内外）、前腕を上方向に 90 度回転させる（回外）、手首を親指側に横に曲げる（橈屈）、手首を小指側に横に曲げる（尺屈））を用意した。

ジェスチャーの測定は拳を軽く握った状態を初期状態とし、そこからそれぞれのジェスチャーを行った。被験者が右手でこの動作を 10 回ずつ繰り返した時の筋電位を測定し、それを 1 セットとして、計 3 セット、30 個のデータを取得する（ただし、実験者の判断により、ノイズや波形の乱れがあると認められた波形は除外しておく）。

実際にここで得られた波形を人間が目視し、それがどのジェスチャーによるものかを識別できるかどうか予備的に実験を行ったところ、識別は可能であることを確認した。

5.2 実験の目的

提案手法の有効性を示すために、SVM または DTW を用いて作成したジェスチャの判別器のそれぞれについて、(1) 各判別器の性能評価と (2) 提案手法に基づくパスワードの安全性の評価を行なった。

まず、各判別器の性能評価は、各判別器の対象ジェスチャの波形データ（訓練には使われなかったデータ）が入力された時、それを正しく当該のジェスチャと判定できるかどうかを評価した（実験 1）。なお、以下では、「本人拒否率」という言葉を、当該のジェスチャであるにもかかわらず、誤った（当該のジェスチャではないという）判断を下した割合の意味で用いる。

一方、提案手法に基づくパスワードの安全性の評価は、前述した考え方に基づき、本人拒否率の小さいジェスチャを選んでパスワードを構成した時に、それらジェスチャの判別器に対して、別の被験者のジェスチャの波形を与え、それを当該の被験者でないと判定できるか否かで行う。つまり、当該の被験者以外の被験者を仮想攻撃者に見立てるわけである。なお認証が成功するのは、前述した様に、パスジェスチャを構成する全てのジェスチャが正しいと判定された場合である。

なお、パスジェスチャと同じジェスチャ列だけを与えた場合（実験 2）と、全てのジェスチャの組み合わせを与えた場合（実験 3）の 2 通りの評価を行う。前者はパスワードに対する他人受入率、後者は偶然突破確率に対応する。本来であればパスワードにどのジェスチャーが設定されてあるかわからないため、総当たり攻撃に対してどの程度の耐性を持つのかは、非常に重要である。

被験者毎に、それぞれのジェスチャの波形データを 30 ずつ

表 2. SVM を用いた場合の誤答数.

被験者	B	C	D	E	F	G	H	I	J
1	0	2	0	0	3	2	0	1	0
2	0	10	0	0	1	5	5	4	6
3	0	0	0	2	1	1	0	0	0
4	1	0	0	1	1	0	2	0	4
5	0	0	1	3	0	0	6	4	0
6	0	0	2	0	0	0	0	0	0

測定してあるので、それらの組み合わせで仮想的に攻撃としての入力を生成する。後述する実験では、パスワードを構成するジェスチャ数を 4 としているので、実験 2 で使用できる入力データは、仮想攻撃者一人あたり $30^4 = 810,000$ 通り作成できる（実験者の判断で、明らかな測定失敗やノイズを多く含むデータは取り除いているので、実際にはこの数よりもやや少なくなることがある）。実験 3 の場合、パスジェスチャとして使用できるジェスチャ候補数を n とすると、仮想攻撃者一人 ${}_nP_4 \times 30^4$ 通り作成できる。

以下、SVM で訓練した判別器に対する実験を実験 1A、実験 2A、実験 3A、DTW を用いて生成した判別器に対する実験を実験 1B、実験 2B、実験 3B とする。

5.3 SVM を用いた識別手法の性能評価実験

5.3.1 実験方法

ここでは予備実験の結果から、図 9 に示す 12 のジェスチャの内の、B〜J の 9 パターンを用いた。被験者は、健康な 20 代の学生（宮崎大学工学部所属）6 名であり、計測前に前腕を用いた激しい運動は行っていないことを確認して実験を行なった。

各被験者の筋電位 270 データ (30 データ× 9 ジェスチャー) の内、各ジェスチャーの標準波形を基準として相関係数が高い上位 20 データ（標準波形も含む）、計 180 データ（20 データ× 9 ジェスチャー）の特徴量を用いて SVM で機械学習を行い、各ジェスチャーの判別器を作成した（被験者 1 名あたりジェスチャー種分、9 つの判別器を作成した）。

5.3.2 実験 1A の結果

各被験者の各ジェスチャーの判別器に、それと同じジェスチャの波形データのうち、訓練に用いなかった残り 10 データを与え、正しく当該のジェスチャであると判定されるか否かを調べた。

その結果、当該のジェスチャーではないと間違った判定を行なってしまった回数を表 2 に示す。

この結果から、各被験者毎に識別率が高いジェスチャーとそうでないものがあることが確認できた。

5.3.3 実験 2A の結果

本手法では、前述した様に、本人拒否率が最も低かったジェスチャー上位 4 つを選択して、パスジェスチャを構成する。選択したジェスチャは、表 2 で下線を引いたものである。例えば被験者 1 であれば、B、D、H、J である。なお、今回の実験手法の元では、パスワードを構成するジェスチャの順序は、判定性能に影響しない。

表 3. 4 桁のパスワードに対する他人受入率.

被験者	平均 FAR
1	0%
2	0%
3	0%
4	0%
5	0%
6	0%

表 4. 4 桁のパスワードに対する偶然突破確率.

被験者	偶然突破確率
1	0.00000000%
2	0.00000102%
3	0.00000000%
4	0.00000174%
5	0.00003196%
6	0.00000007%

その選択された 4 つのジェスチャーを 4 桁のパスワードとして用いた際の他人受入率を調べた。この 4 桁のパスワードが全て一致した時のみ認証は成功する。4 桁のパスワードに対し、他の被験者 5 名の同じジェスチャー 30 データの組み合わせ（30 × 30 × 30 × 30 × 5）計 4,050,000 データを用いて識別を行った。その各被験者の識別結果を表 3 に示す。結果として、すべての被験者において、他人が受け入れられることは一度もないという良い結果となった。

5.3.4 実験 3A の結果

次に偶然突破確率を調べた。4 桁のパスワードに対し、自分以外の被験者 5 名のジェスチャー 30 データの組み合わせ

$$30^4 \times {}_9\mathrm{P}_4 \times 5$$

を用いて識別を行った。その各被験者の識別率を表 4 に示す。すべての被験者について、本人拒否率非常に小さく、良い結果となった。

5.4 動的時間伸縮法を用いた識別手法の性能評価実験

5.4.1 実験方法

筋電位の計測は、SVM を用いた手法の実験と基本的に同じであるが、実験で用いたジェスチャと被験者数が異なっている。この識別実験では、図 9 のジェスチャーの内、D〜H の 5 つのジェスチャを対象に行った。被験者は、健康な 20 代の学生（宮崎大学工学部所属）11 名である。

本実験では、まず以下の様な閾値の決定方法をとった。すなわち、まず各ジェスチャーにつき 30 回分の計測データの中から、相互相関関数と相関係数を用いて標準波形を選出したのち、残り 29 個の波形との DTW 距離を算出した。その比較の中で、DTW 距離の値が最も高かったものとの間の DTW 距離を閾値として採用した。ただし、計測した 30 回の中で、ノイズや波形の乱れがある波形は予め除外している。

表 5. 各識別器の閾値.

被験者	D	E	F	G	H
1	49.75	31.76	39.86	29.89	30.85
2	33.87	25.58	62.69	39.14	48.81
3	20.17	6.99	22.36	13.45	19.81
4	39.75	10.38	24.91	45.11	37.12
5	74.77	30.12	48.75	39.36	44.72
6	54.41	26.71	62.95	31.87	30.88
7	35.65	43.11	17.62	35.55	138.01
8	24.58	14.52	15.07	39.68	33.39
9	31.51	31.13	17.78	35.57	48.33
10	33.91	23.68	47.07	28.36	77.14
11	65.91	48.86	73.66	49.61	44.04

表 6. DTW を用いた手法での誤答数.

被験者	D	E	F	G	H
1	0	0	0	0	0
2	0	2	0	0	2
3	0	0	0	0	0
4	0	0	0	0	0
5	0	2	1	1	0
6	0	0	0	0	0
7	0	0	0	1	0
8	0	0	0	0	0
9	0	0	0	0	0
10	0	0	1	0	2
11	0	2	0	1	0

5.4.2 実験 1B の結果

本人識別を行った各被験者の各ジェスチャーの閾値を表 5 に、29 データの試行のうち、誤って同じジェスチャの入力を異なるジェスチャと判定した回数を表 6 に示す。当然のことながら、ノイズや波形の乱れのあったデータ以外は、全て正しく受け入れられているため、全体的に良い結果となっている。

5.4.3 実験 2B の結果

次に、DTW 距離の値が最も低かったジェスチャー上位 4 つを選択した。選択したジェスチャは、表 6 で下線を引いたものである。例えば被験者 1 であれば、E、F、G、H である。

その上で、選択された 4 つのジェスチャーを 4 桁のパスワードとして用いた際の他人受入率を調べた。4 桁のパスワードに対し、他の被験者 10 名の同じジェスチャー 30 データの組み合わせ（30 × 30 × 30 × 30 × 10）計 8,100,000 データを用いて識別を行った。その各被験者の識別結果を表 7 に示す。被験者 #9 を除き、良い結果となっている。

被験者#9 の平均他人受入率は 3.634%と他より悪くなっているが、被験者#8 に対しての受入率がが 33.77%、被験者#3 に対しての受入率が 2.57%であり、残りの 8 人の被験者は 0%であった。

5.4.4 実験 3B の結果

次に、偶然突破確率を調べた。4 桁のパスワードに対し、他の被験者 10 名の異なるジェスチャー 30 データの組み合わせ

$$30^4 \times {}_5\mathrm{P}_4 \times 10$$

を用いて識別を行った。その各被験者の識別率を表 8 に示す。結果、すべての被験者においてよい結果となった。

セキュリティの観点からは、他人受入率を低く抑えることが好ましい。そこで各被験者のジェスチャそれぞれについて、他人受入率が 0%になるように閾値の値を調整した。その場合の本人拒否率と他人受入率を表 9 に示す。

なお今回の実験は、被験者が 11 名と少人数であり、またジェスチャー種も 5 種と少ない条件で行なっている。今後、より多くの被験者、及びジェスチャー種で実験を行うことが必要である。

6. 考察

SVM を用いた手法については、全体の結果としてはすべての被験者に対して良好な結果となった。しかし、今回対象となった被験者 6 名という少人数であったので、今後はより多くの被験者を対象に実験を重ねることが必要である。また、今回の実験で用いた 11 個の特徴量よりもさらに性能の良い特徴量を探索し、認識手法の性能改善を行うことが考えられる。

DTW を用いた手法でも、識別可能という結果が得られた。しかし、適した閾値の設定が必要不可欠である。また今回は、5 種のジェスチャー中から 4 種のジェスチャーを選んで 4 桁のパスワードを構成した。ジェスチャー候補の種類を増やすことでパスワードの選択の幅が広がり、精度向上につながることが期待できる。

7. 終わりに

本研究では、表面筋電位を用いた認証システムの実現のための個人識別手法として、筋電位の波形から抽出したいくつかの特徴量を用いて SVM を訓練する手法と、筋電位の値を直接比較して判定に用いる手法の 2 つの検討を行った。

実験の結果、どちらの手法も有望なものであることがわかった。しかし、どちらの手法でも精度の向上のためにさらなる検討が必要である。

将来的には、本研究で行った手法を用いてシステムを構築し、ポケットから携帯端末を取り出す動作の間に認証が完了し、すぐさま携帯端末を使用できるようにすることも視野に入れた上で検討を行っていきたい。

参考文献

1) “インターネットの普及状況,” http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc253110.html, (accessed 2018-1-24).

2) 西坂健太郎、寺田真敏、土居範久: “携帯電話を対象とした PIN 認証向け日本語パスワードの提案,” 情報処理学会研究報告 IPSJ マルチメディア通信と分散処理研究会報告, pp.1-8, 2010.

表 7. 4 桁のパスワードに対する他人受入率.

被験者	1	2	3	4	5	6	7	8	9	10	11	平均 FAR
1		0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
2	0%		0%	0%	0%	0%	0%	0%	0%	0%	0.82%	0.082%
3	0%	0%		0%	0%	0%	0%	0%	0%	0%	0%	0%
4	0%	0%	0%		0%	0%	0%	0%	0%	0%	0%	0%
5	0%	0%	0%	0%		0%	0%	0%	2.36%	0%	0%	0.236%
6	0%	0%	0%	0%	0%		0%	0%	0%	0%	0%	0%
7	0%	0%	0%	0%	0%	0%		0%	0%	0%	0%	0%
8	0%	0%	0%	0%	0%	0%	0%		0%	0%	0%	0%
9	0%	0%	2.57%	0%	0%	0%	0%	33.77%		0%	0%	3.634%
10	0%	0%	0%	0%	0%	0%	0%	0%	0%		0%	0%
11	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%		0%

表 8. 4 桁のパスワードに対する偶然突破確率.

被験者	偶然突破確率
1	0.49%
2	0.606%
3	0%
4	0.001%
5	0.708%
6	0%
7	0.215%
8	0.002%
9	0.217%
10	0%
11	0.207%

表 9. 適した閾値にした際の本人拒否率と他人受入率.

被験者	FRR	FAR
1	0%	0%
2	10.71%	0%
3	0%	0%
4	0%	0%
5	10.34%	0%
6	0%	0%
7	0%	0%
8	0%	0%
9	10.1%	0%
10	0%	0%
11	3.44%	0%

3) 妹尾尚一郎、厚井裕司、貞包哲男、中谷直司、馬場義昌、鹿間敏弘: “生体認証によるネットワーク個人認証システム,” 情報処理学会論文誌, pp.1111-1120, 2003.

4) 辻 敏夫、福田 修: “生体信号解析の新展開,” 日本 AEM 学会誌, vol.13, No.3, 2005.

5) Hiroki Tamura, Takafumi Gotoh, Dai Okumura, Hisashi Tanaka, Koichi Tanno: “A Study of the s-EMG Pattern Recognition Using Neural Network,” International Journal of Innovative Computing, Information and Control, pp.4877-4884, 2009.

6) Hisaaki Yamaba, So Nagatomo, Kentaro Aburada, Shinichiro Kubota, Tetsuro Katayama, Mirang Park, Naonobu Okazaki: “An Authentication Method for Mobile Devices that is Independent of Tap-Operation on a Touchscreen,” Journal of Robottics, Networking and Artifcial Life. Vol.1, pp.60-63, 2015.

7) 山場久昭、長友　想、油田健太郎、久保田真一郎、片山徹郎、朴　美娘、岡崎直宣: “表面筋電位を用いた個人認証手法の実現に向けた基礎研究,” 情報処理学会研究報告, Vol.2015-CSEC-69、No.32、pp.1-6、2015.

8) 黒木聡舜、山場久昭、久保田真一郎、片山徹郎、朴美娘、岡崎 直宣: “表面筋電位を用いた個人認証システムの実現に向けた検討.” 情報処理学会研究報告、Vol.2015-SPT-15、No.5、pp.1-6、2015.

9) H. Yamaba, T. Kurogi, S. Kubota, et al.: “Evaluation of feature values of surface electromyograms for user authentication on mobile devices,” Artificial Life and Robotics, Vol.22, pp.108-112, 2017.

10) H. Yamaba, T. Kurogi, T. Aburada, et al.: “On applying support vector machines to a user authentication method using surface electromyogram signals,” Artificial Life and Robotics, Vol.23, pp.87-93, 2018.

11) 黒木聡舜、山場久昭、油田健太郎、朴　美娘、岡崎直宣: “表面筋電位を用いた個人認証システム実現の相互相関係数を用いた個人識別手法の検討,” 情報処理学会研究報告, Vol.2017-SPT-24, No.12, pp.1-6, 2017.

12) Tokiyoshi Kurogi, Hisaaki Yamaba, Kentaro Aburada, Shinichiro Kubota, Tetsuro Katayama, Mirang Park, Naonobu Okazaki: “A study on user identification method using cross-correlation and SVM to realize an authentication system by s-EMG,” Proceedings of 23th International Symposium on Artificial Life and Robotics, pp.462-467, 2018.

13) Tokiyoshi Kurogi, Hisaaki Yamaba, Kentaro Aburada, Tetsuro Katayama, Mirang Park, Naonobu Okazaki:

"A study on a user identification method using dynamic time warping to realize an authentication system by s-EMG," Lecture Notes on Data Engineering and Communications Technologies, Springer, Vol.17, pp.889-900, 2018.

14) TETSUJI TAKADA: "fakePointer: A User Authentication Scheme that Makes Peeping Attack with a Video Camera Hard," Information Processing Society of Japan, 2008.

15) 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," 情報処理学会 Computer Security, Symposium 2014, pp.1023-1028, 2014.

16) 和斉 薫: "モバイル端末向け個人認証方式における柔軟な安全性強度の実現手法に関する研究," 宮崎大学大学院修士論文, 2015.

17) 日隈光基: "録画画像を用いた攻撃に耐性を持つパズル型認証方式の提案," 宮崎大学卒業論文, 2016.

18) Mohamed Khamis, Regina Hasholzner, Andreas Bulling, Florian: "Two-factor Authentication on Public Displays Using Gaze-Touch passwords and Personal Mobile Devices," ISBN 978-1-4503-5045-7/17/06, 2017.

19) Anil K. Jain, Karthik Nandakumar, Arun Ross, "50years of biometric research: Accomplishments, challenges, and opportunities," Pattern Recognition Letters 79, pp.80-105, 2016.

20) Blair C.Armstrong, MariaV.Ruiz-Blondet, "Brainprint : Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics," Neurocomputing166, pp.59-67, 2015.

21) "筋電図の種類と役割," http://www.sakaimed.co.jp/special/kinden/kinden02.html, (accessed 2018-1-24).

22) "神経細胞と静止膜電位," http://noucobi.com/neuro/neurophysiology/S1.html, (accessed 2018-1-24).

23) 田村宏樹、奥村 大、淡野公一: "表面筋電位を FFT 処理しないで動作識別する方法の検討," 電子情報通信学会論文誌 D, Vol.J90-D, No.9, pp.2652-2655, 2007.

24) 石川圭佑、戸田真志、櫻沢 繁: "表面筋電信号を用いた実時間指運動認識インタフェースとその応用," 情報処理学会シンポジウム論文集 3 号, pp.871-874, 2011.

25) Nobutaka TSUJIUCHI, Takayuki KOIZUMI: "Technique for Discriminatio bnetween Seven Motions Using Real-Time EMG Signals," The Japan Society of Mechanical Engineer, ISSN Vol.12, pp.2424-3000, 2014.

26) 井部鮎子、郷古 学、伊藤宏司: "表面筋電位を用いた前腕義手の複合動作識別," 計測自動制御学会論文集 Vol.45, No.12, pp.717 - 723, 2009.

27) JieLiu: "Adaptive myoelectric pattern recognition toward improved multifunctional prosthesis control," Medical Engineering and Physics, Vol.37, pp.424-430, 2015.

28) Marie Chan, Daniel Esteve, Jean-Yves Fourniols, Eric Campo: "Smart wearable systems: Current status and future challenges," Artificial Intelligence in Medicine, Vol.56, pp.137-156, 2012.

29) 斎藤良介、吉村博幸: "ECG 心伯波形の特徴量抽出と認証精度について," ISSN 2432-6380, pp.21-26, 2016.

30) Thalmic Labs Inc.: https://www.myo.com/, (accessed 2018-1-24).

31) "筋電計 S&M Biolog," http://www.sandme.co.jp/supportbl.html#dl4000, (accessed 2018-1-24).

32) Eamonn J.Keogh, Michael J.Pazzani: "Scaling up dynamic time warping for datamining applications," 6th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp.285-289, 2000.

33) Byoung-Kee Yi, H.V.Jagadish, Christos Faloutsos: "Efficient retrieval of similar time sequences under time warping," International Conference of Data Engineering, Vol.14, pp.201-208, 1998.

34) Donald J.Bemdt, James Clifford: "Using dynamic time warping to find patterns in time series," AAAI-94 Workshop on Knowledge Discovery in Databases (KDD-94), pp.359-370, 1994.

35) D.M.Gavrila, L.S.Davis: "Towards 3-d model-based tracking and recognition of human movement: a multi-view approach. International Workshop on Automatic Face and Gesture-Recognition," IEEE Computer Society, 1995.

36) Matthew D.Schmill, Tim Oates, Paul R.Cohen: "Learned models for continuous planning," The Seventh International Workshop on Artificial Intelligence and Statistics, 1999.

37) Klaus Gollmer, Clemens Posten: "Detection of distorted pattern using dynamic time warping algorithm and application for supervision of bioprocesses," On-Line Fault Detection and Supervision in the Chemical Process Industries, pp.101-106, 1995.