

脳波を用いた複数特徴量の組み合わせによる生体認証

石川由羽[†] 西畑かおり[†] 高田雅美[†] 鴨浩靖[†] 城和貴[†]

概要: 脳と機械を直結する Brain Machine Interface 技術の研究が盛んに行われている。我々は BMI で使用される認証技術として、脳波を用いた個人認証の提案を行う。脳波個人認証の研究は、多方面から進められている。本稿では、従来研究で提案されている複数特徴量を組み合わせることで、より精度の良い脳波認証を目指す。特徴量の組み合わせにはアンサンブル学習の1つである AdaBoost を使用する。特徴量と使用電極の組み合わせパターンを考慮することで、より適切な識別器の生成を行う。また、AdaBoost を用いた認証手法を提案する。

キーワード: 生体認証, 脳波, 特徴抽出, AdaBoost

Biometric Authentication based on Multi-feature Combination using EEG

Yu Ishikawa[†], Kaori Nishibata[†], Masami Takata[†], Hiroyasu Kamo[†], Kazuki Joe[†]

1. はじめに

脳と機械を直結する Brain Machine Interface (BMI) 技術が注目されている。健常者が安全かつ容易に利用できる BMI として、脳波を用いた非侵襲 BMI の開発が盛んに行われている。現在では、脳波で操作する義手・義足や、脳波を読み取り自律移動する車いす制御システム、人から人への脳波の直接通信の研究等、様々な分野で進められている。また、人の感情を察知して動くデバイス「necomimi」や、Google Glass を脳波で操作するアプリケーション「MindRDR」等、すでに市販されている BMI 技術もある。このように、BMI 技術が日常に浸透するにつれて、認証技術の向上も求められる。従来の認証技術では、主に ID とパスワードを用いた個人認証が利用されている。しかし、盗用や、総当たり方式で認証試行された場合には容易に詐称される恐れがある。そのため、従来の手法では、安全性の面から必ずしも確実な手段とはいえず、近年ではバイオメトリック認証が利用されている。

バイオメトリック認証とは、生体情報を用いた個人認証のことである。現在では、指紋や虹彩、顔、声紋等の生体認証が研究・開発されており、従来のパスワード認証に比べて盗用が困難である。特に、指紋や虹彩は認証性能も高く、実用化も行われているが、それらを用いた認証システムが詐称されたとの報告もある。原因の1つとして、情報が常にさらされている点が挙げられる。

そこで、脳波を用いた生体認証が考えられている。脳波を使用する場合、内部情報かつ専用の計測器が必要であるため、盗用が困難であるといえる。また、BMI で利用することを考えると、脳波をそのまま使用できるため、別の

生体認証を用いるよりも効率が良い。脳波を用いた生体認証の研究は、すでに多方面から進められている。例えば、40名の被験者の開眼時・閉眼時の脳波を使用することで、80%の精度で個人認証を実現した報告[1]や、閉眼時の4名の被験者の脳波リズムを解析し、90%以上の精度を実現した報告[2]がある。また、視覚誘発電位を用いて個人認証を行った報告[3]や運動想起電位や言語想起課題により個人認証を行った報告[4]もある。上記のような従来研究では、研究によって様々な特徴量、学習手法が提案されている。本稿では、これらの特徴量を組み合わせることで、より高精度な認証手法の提案を目指す。

本稿では、SVM を使用して分類を行う。通常 SVM は分類として使用されるが、認証として使用する場合には分類結果から承認要請の受理・拒否判定を行う必要がある。従来研究[5]の手法では、複数回データを計測して、それぞれのデータを SVM で分類することで、分類されたデータ回数を認証に使用する。正しく分類されたデータ回数が閾値以上の場合には受理、閾値未満の場合には拒否とする。以上の手法により、認証として利用することが可能となる。しかし、閾値設定のために、分類時と比較して長時間のデータ計測が必要となる。そこで、本稿では、1回分のデータで認証を行うため、AdaBoost を使用した認証を提案する。

2. 特徴抽出

2.1 データ計測と前処理

本稿では多チャンネル脳波計として BioSemi を用いて計測を行う。基準電極の導出には双極誘導法を使用する。脳波計のサンプリング周波数は最大 2048Hz、搭載可能な電極数は最大 256 チャンネルである。今回はサンプリング周波

[†] 奈良女子大学
Nara Women's University

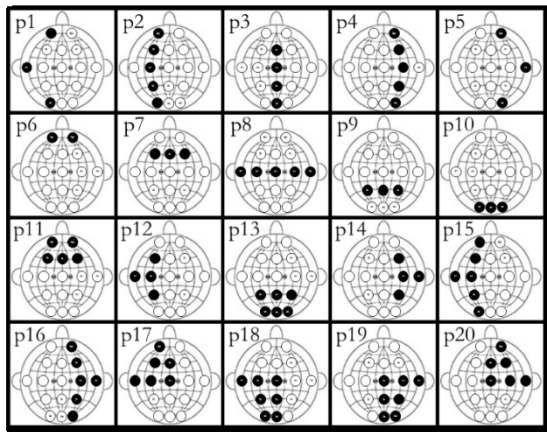


Figure 1 電極の組み合わせパターン

数 2048Hz, 電極数 16 チャンネルで計測を行う。

計測データには前処理を施し、特徴量抽出に適したデータに補正する。まず、バンドパスフィルタを用いて、計測データから 4–40Hz の脳波周波数帯域のみを抽出する。一般的に 1–3Hz は δ 波と定義されているが、脳波以外の筋電位や眼球運動、心拍等の生体現象によるアーチファクトを多く含むため、本稿では除外する。また、60Hz に現れる交流障害等の環境に起因するアーチファクトもバンドパスフィルタにより取り除くことができる。次に、一時的に現れるパルスノイズ等を補正するため、バンドパスフィルタ後のデータの標準偏差を求め、 3σ を超えるデータを 3σ に補正する。最後に、ノイズ補正後のデータを 0–1 に正規化する。これらの処理により、バイアス等を取り除き、より認証に適したデータに再構築する。

2.2 特徴量

脳波の解析で最も一般的な手法である周波数解析として、高速フーリエ変換 (FFT) を用いたパワースペクトル (PS) を使用する。FFT を行う際に、データ長は 2 のべき乗とする。パワースペクトルはチャンネルごとに求める。得られたパワースペクトルを θ 波 (4–8Hz), α 波 (8–14Hz), β 波 (14–26Hz), γ 波 (26–40Hz) の周波数帯域ごとに平均含有率を算出し、4 つの特徴量とする。データ長を 4 分割して、各データの含有率を求める。使用する全電極を特徴量とする。

2 電極間の周波数解析を行うため、クロススペクトル (CS) を利用する。パワースペクトルと同様に FFT を使用する。得られたクロススペクトルをパワースペクトル同様に 4 つの周波数帯域ごとに平均含有率を算出し、特徴量とする。データ長の分割は行わない。使用する全電極の組み合わせを特徴量として与える。

相互相関係数 (CC) を使用して、2 電極間の類似性を特徴量とする。係数が 1 の場合は正の相関あり、0 の場合は相関なし、 -1 の場合は負の相関ありといえる。データ長を 8 分割して、各データの係数を求める。使用する全電極

の組み合わせを特徴量とする。

2 電極間の相互依存を利用するため、相互情報量 (MI) を使用する。前処理としてデータの離散化が必要である。データ長の分割は行わない。使用する全電極の組み合わせを特徴量として与える。

また、個人認証に適した電極を確認するため、電極の組み合わせパターンを考慮する。Figure 1 に電極の組み合わせパターンの一覧を示す。一覧の 20 パターンに加えて、全 16 チャンネルを使用したパターンの計 21 パターンを使用する。

3. 認証手法

脳波を用いて個人分類を行うために、AdaBoost を使用する。AdaBoost とは、Boosting によって複数の弱識別器を組み合わせたアンサンブル学習の 1 種であり、学習データの重みを適応的に更新する手法である。最終的な識別器は弱識別器の重み付き多数決により決定する。特徴量には 2.2 節で説明した特徴量 4 種類と電極の組み合わせパターン 21 種類の組み合わせ 84 種類を用意する。これらの特徴量に SVM を適用して、84 パターンの弱識別器候補を生成する。カーネルには RBF を使用する。本稿では学習回数を 50 回とする。生成された強識別器が個人認証の学習モデルとなる。

AdaBoost により個人分類した結果を利用して、認証を行う。システムは登録フェーズと認証フェーズで構成される。登録フェーズでは、2 章で説明した通り、まず、脳波計測を行い、得られた計測データに前処理を施し、複数の特徴抽出を行う。これら得られた特徴から、AdaBoost を用いて学習モデルを生成する。認証フェーズでは、登録フェーズ同様に計測データから特徴量を抽出する。登録フェーズで生成した学習モデルを用いて、認証データを最も信頼度の高い登録者に分類する。判定には AdaBoost 時に算出される信頼度を利用する。信頼度が閾値以上であれば、本人であるとみなし受理する。閾値未満であれば、他人であるとみなし拒否する。認証性能は等価エラー率 (EER : Equal Error Rate) と認証率で評価する。

4. 実験

4.1 実験手法

被験者は健康な 20 代女性 26 名である。計測時は座位、安静状態で行う。1 回当たり 10 秒の計測を 1 人当たり 5 回行う。これを 10 回繰り返す。全データ数は 26 人 \times 50 個の計 1300 個である。データ数は 2 のべき乗とする必要があるため、初めの 8 秒間 (2048Hz \times 8 秒) のデータを使用する。

本稿では、2 種類の実験を行う。まず、実験 1 として分類精度の確認を行う。使用データは 26 人の計 1300 個全てである。10 交差検定を行い、分類精度を検証する。まず、SVM を用いて、特徴量として使用した 4 種類 (PS, CS,

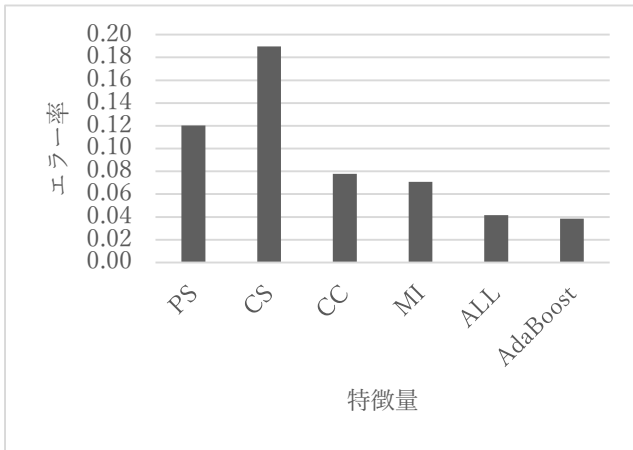


Figure 2 実験 1 各特徴量の分類率

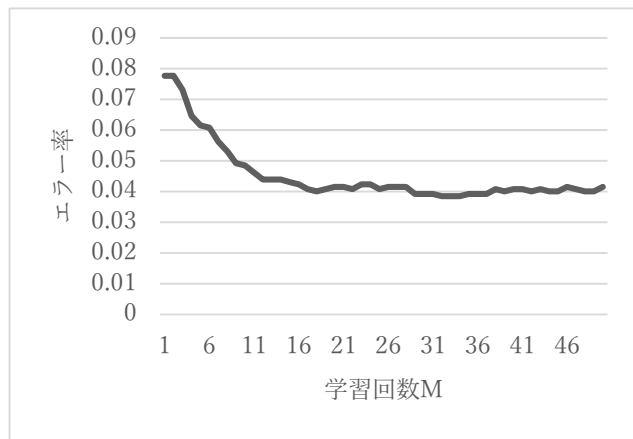


Figure 3 実験 1 AdaBoost の学習回数とエラー率

CC, MI) の分類率を求める。次に、4 種類の特徴量全てを結合したベクトルを SVM に与えた場合 (ALL) の分類率を求める。どちらも電極は 16 チャンネル全てを使用する。最後に、提案手法である AdaBoost を使用した分類率を求める。この場合は、特徴量と電極パターンの組み合わせ 81 種類を使用する。

実験 2 では、提案手法の認証精度を検証する。承認要請の受理と拒否を判別する閾値を変更した場合の認証率を調べる。使用データは登録者 23 人の 1150 個と詐称者 6 人の 150 個である。まず、登録者のデータ 1000 個から FAR と FRR を算出し、EER を求める。次に、登録者の認証率と詐称者の認証率を算出する。どちらも 10 交差検定を行う。

4.2 実験結果

実験 1 の結果について述べる。Figure 2 は PS, CS, CC, MI, ALL, AdaBoost の分類率を示したグラフである。縦軸はエラー率を表している。4 種類の特徴量のうち、分類率の良いものから順に MI, CC, PS, CS となっている。この中では周波数解析を用いた特徴量の分類率が比較的低い。一方、CC と MI においては、1 つの特徴量で 9 割を超える分類率が得られた。周波数解析の分類率が低い原因として、含有率算出時の分割数が少ないことが挙げられる。4 分割

Table 1 実験 1 AdaBoost

特徴量						
PS	CS	CC	MI			
21.8	4.8	46.2	27.2			
電極組み合わせパターン						
p1	p2	p3	p4	p5	p6	p7
0	0	1.6	0	0	0	0
p8	p9	p10	p11	p12	p13	p14
0.2	1.6	0.8	11	0	11	2.2
p15	p16	p17	p18	p19	p20	p21
1.6	0.6	12.8	12.6	15.6	8.4	20

から 13 分割にした場合、PS, CS 双方の分類率は上昇したが、特徴ベクトル数が大幅に増加するため、今回は 4 分割を採用する。また、CS は分類率が他と比べて低いため、個人認証の特徴量として使用するには、工夫が必要だと考えられる。

次に、ALL と AdaBoost の結果について考察する。ALL でのエラー率は 0.042 であった。単一の特徴量と比較すると 1 番分類率が良い。ある程度の分類率が得られる特徴ベクトルを結合させることで、ベクトル長は長くなるが、SVM の分類率は高くなるといえる。提案手法の AdaBoost のエラー率は 0.038 であり、ALL よりも若干良い分類率が得られた。これは学習回数 33-35 回の値であり、この時最も良い結果であった。学習回数と分類率の推移を Figure 3 に示す。このグラフは 10 交差検定の平均値である。1 回の学習ではエラー率が 0.078 であり、これは単一の特徴量で学習した結果と同程度の値である。学習回数を重ねるにつれて、徐々にエラー率は減少している。学習回数 18 回目にエラー率 0.04 となり、以降 50 回目まで 0.04±0.02 程度のエラー率を保っている。

各特徴量と電極の組み合わせパターンの AdaBoost 時の使用頻度について述べる。Table 1 に学習回数 50 回、交差検定 10 回の選択回数 500 回のうち、選択された特徴の内訳を示す。まず、特徴量では CC が半分近くを占めている。事前に行った各特徴量の分類率も CC が 1 番良かったため、想定内の結果である。同様に CS 単独の分類率は 1 番悪かったが、AdaBoost でも 5%程度しか使われていない。次に、電極の組み合わせパターンでは、全チャンネルを使用した p21 が 20%を占めている。その他、10%を超えているパターンは p11, p13, p17-p19 の 5 パターン、次いで 8.4%の p20 である。この結果より、左脳・右脳両方の電極を使用した方が、半球のみを使用した場合より分類に適した特徴量が得られることがわかる。前頭葉と後頭葉では、どちらかといえば後頭葉の分類率が高い傾向にあるが、有意な差は見られない。また、選択率 0 のパターンは使用電極数が

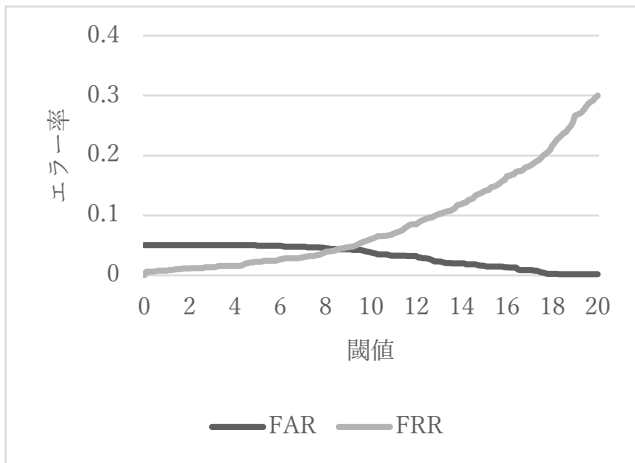


Figure 4 実験2 提案手法のEER

少ない傾向にある。今後は、離れた電極を組み合わせたパターンについても考慮していきたい。

実験2の結果について述べる。閾値を0-20で0.1ずつ変更した場合のFARとFRRのグラフをFigure 4に示す。FARは閾値1-5では0.05で一定であるが、それ以降は徐々に低下し0に近づく。FRRは0から始まり、閾値20で0.3となる。FARとFRRの交点であるEERは閾値8.8のとき0.04である。次にFigure 5に登録データと詐称データのエラー率と、その平均を示す。EERで得られた閾値8.8の場合、登録データのエラー率は0.058であった。しかし、詐称データのエラー率が0.14と高いため、詐称データを考慮する場合は、閾値を上げる必要がある。登録データと詐称データの交点は閾値11.1のときの0.075である。最も平均のエラー率が小さくなったのは、閾値14のときの0.074である。この結果から、適切な閾値の設定により、偽称データの誤認識を防ぐことも可能だといえる。

5. おわりに

本稿では、脳波を用いた複数特徴量の組み合わせによる生体認証の提案を行った。複数特徴量の組み合わせにはSVMによるAdaBoostを使用して、1度の計測データから認証を行う手法を提案した。脳波認証で使われているパワースペクトル、クロスパワースペクトル、相互相関係数、相互情報量の4種類の特徴量と、16チャンネルの電極から21パターンの組み合わせを用いて、AdaBoostで使用する弱識別器候補とした。結果、分類率は96.2%となった。これは全特徴量を使用したSVMの分類率である95.8%よりも、若干良い結果となった。また、SVMを用いた認証では、複数の計測データ数から多数決を行い、受理・拒否を判定する必要があるが、本提案手法ではAdaBoostで得られる信頼度を利用することで1度の計測データから判定を行うことができた。EERは0.04、そのときの登録データの認証率は94.2であった。また、閾値の適切な設定により、偽称

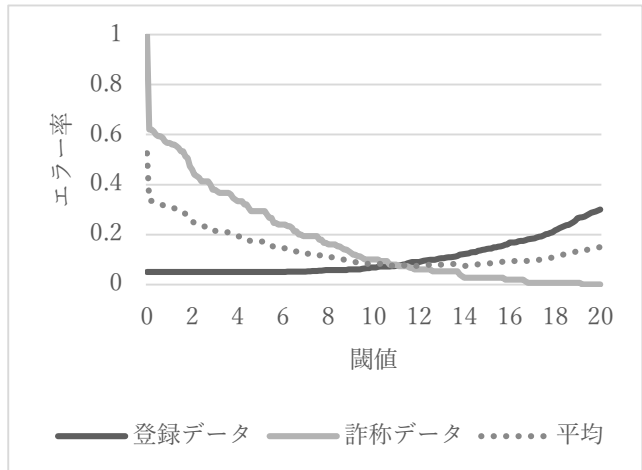


Figure 5 実験2 提案手法の認証精度

データを防ぐことも可能である。

今後の課題は、より適切な特徴量を使用することで認証精度を上げることである。現在では認証に8秒のデータを必要としているが、特徴量の選択により、現在より短時間の計測で認証できる可能性もある。また、今回の実験では周波数解析の分類率が低かったため、弱識別器としての選択率が下がった。含有率算出時の分割数、使用周波数等事前にBoostingすることで、より精度が上がると考えられる。その他にも、適切な閾値の検討方法について考える必要がある。

謝辞 本研究は特別研究員奨励費(16J10436)の助成を受けたものである。

参考文献

- [1] R. B. Paranjape, J. Mahovsky, L. Benedicent and Z. Koles, The Electroencephalogram as a Biometrics, vol. 2, Proc. of 2001 Canadian Conference on Electrical and, 2001, pp. 1363-1366.
- [2] M. Poulos, M. Rangoussi, V. Chrissikopoulos and A. Evangelou, Parametric person identification from the EEG using computational geometry, vol. 2, Proc. of the 6th IEEE Int. Conf. on Electronics, Circuits and Systems, 1999, pp. 1005-1008.
- [3] R. Palaniappan and D. P. Mandic, Biometrics from brain electrical activity: A machine learning approach, vol. 29 no. 4, IEEE Trans. Pattern Anal. Mach. Intell., 2007, pp. 738-742.
- [4] S. Marcel and J. R. Millan, Pearson Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaption, vol. 2, IEEE Trans. on Pattern Analysis and Machine Intelligence, 2007, pp. 743-748.
- [5] T. Yoshikawa, I. Nakanishi, S. Li, Person Authentication Using EEG -Verification Based on 1vs1SVM with Divided EEG Spectra-, Proc. of the 2013 International Workshop on Smart Info-Media System in Asia (SISA 2013), 2013, pp. 367-371.