〈一般研究課題〉　スマートセンサデータに対する
選択的プライバシー保護に関する研究
助 成 研 究 者　愛知工業大学　　玉森　聡

スマートセンサデータに対する選択的プライバシー保護に関する研究

玉森　聡
(愛知工業大学)

A Study on Selective Privacy Protection for Smart Sensor Data

Akira Tamamori
(Aichi Institute of Technology)

Abstract：

The purpose of this study is to develop a new privacy protection technology that can integrate and selectively handle multiple sensor signals and historical information. Expectations and demand for services that utilize the large amount of sensor signal information obtained from a large number of users are expected to increase further in the future. There is a need to develop identification techniques for individual sensor signals to prepare for assessing their vulnerability to attack. In this paper, we report the results of empirical verification of personal information identification for audio and acceleration signals. As a part of the development of the information hiding technology for privacy protection, we have also studied the information embedding/detection method for audio signals, and have conducted basic experiments to report the results.

1. はじめに

近年の情報通信技術の発展・普及と、コンピュータの小型化・軽量化により、安価なセンサデバイスを用いて多様なセンサ信号を大量に収集することが容易な時代となっている。収集したセンサ信号を活用することで、ヘルスケア・健康管理、ライフログ、エンタテイメントなど、様々な分野におけるサービスやシステムへ応用されている。多数のユーザから取得した大量のセンサ信号情報を活用するサービスへの期待・需要は今後ますます高まると予想される。

各ユーザから収集されるセンサ信号には生体情報や個人情報(氏名、住所、職業、収入、履歴情報)が含まれている場合がある。原則的に、ユーザの同意に基づいてセンサ信号の収集が行われるが、加速度などユーザに依存するセンサ信号からユーザの属性情報(年齢や性別の情報)を暗黙的に収集してしまう可能性がある。ユーザは同意の範囲外の情報が取得されるリスク、またサービス事業者は意図しない個人情報を取得することによるプライバシーの管理・漏洩リスクを新たに負う可能性がある。したがって、センサ信号に対して適切なプライバシー保護を施すことで、これらのリスクを低減することにつなげることができる。センサ信号に対するプライバシー保護は近い将来必ず必要になると予想される。

本研究では複数のセンサ信号と履歴情報を統合的かつ選択的に扱える新たなプライバシー保護技術の開発を目的としている。しかし一方で、個々のセンサ信号に対する個人情報の同定技術を開発し、攻撃に対する脆弱性の評価に備える必要がある。本報告では音声信号と加速度信号を主な対象として、個人情報の同定性能を実証的に検証した結果について報告する。

2. 実験内容

以下の項目について実験を実施した。

- ウェアラブルセンサから収集したセンシングデータを対象とした行動識別実験
- 音声信号を対象とした話者識別実験

3. 実験

3.1 加速度信号を対象とした行動識別実験

ウェアラブルセンサTSND151(図1)を用いて、加速度信号を収集した。行動の種類は「静止、歩行、ジョグ、スキップ、階段登り、階段降り」の6種類とした。各行動について1回の計測時間は20秒とし、各被験者につき合計1時間程度を収録した。なお被験者数は 10 名である。端末の装着位置は付属のベルトを利用して腰の付近に装着した。

図1. ウェアラブルセンサ TSND151

加速度信号の特徴量は予備実験の結果に基づき、平均、分散、および周波数領域上のエネルギーとした。周波数解析の際にはハミング窓を利用し、スライディングウィンドウ方式を用いて特徴量を抽出した。ウィンドウサイズは 4 秒間、ウィンドウのステップサイズは 2 秒間のオーバーラップ 50 % に設定した。スライディングウィンドウによって分割された各データに対して，X 軸，Y 軸，Z 軸とその 3 軸のノルムから特徴量を抽出した。

行動識別モデルとして SVM(Support-Vector-Machine)、決定木、ナイーブベイズ、ランダムフォレストを適用した[1]。ランダムフォレストは決定木アルゴリズムを弱学習器とする集団学習アルゴリズムであり、大量の決定木を作成し、それぞれの決定木が出した答えの多数決によりクラスに分類する手法である。認識精度の評価には F 値を使用した。認識には 4-fold cross validation と呼ばれる手法を用いた。4-fold cross validation では、対象データを 4 分割したのちに、そのう

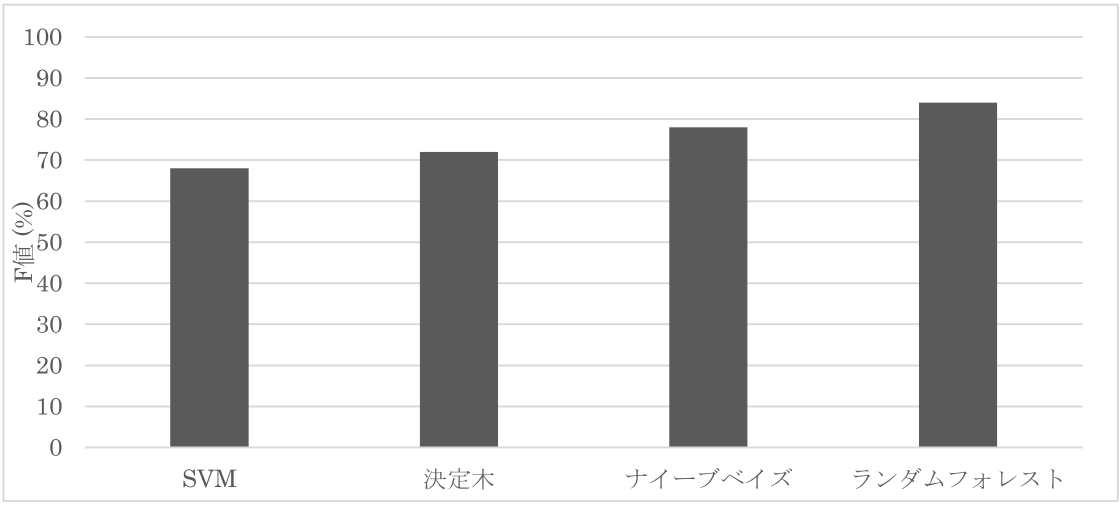

図2. 行動認識結果

ちの 1 つを認識用に用い、残りを訓練データとする。そして、4 個に分割されたデータそれぞれをテスト用データとして 4 回検証を行うものである。

各行動の認識結果を図2に示す。上述のとおり、F値は4-fold cross-validationに基づいて算出した。同図より、ランダムフォレストが最も高い性能を示したことから、行動識別モデルとしてのランダムフォレストの有効性が確認できた。併せて各行動について個人識別率を簡易的に調査したところ、平均識別率は7割程度に留まった。

3.2 音声信号を対象とした話者識別実験

コンデンサマイクと PC を用いて 1 人当たり 500 単語列の音源を収録した。話者識別モデルの学習に用いる単語列を変化させて、残りの単語列を用いて検証を行った。図 3 に単語列の一覧を示す。話者に負担を掛けないことを目的として、単語列を用意した。被験者数は 4 名であり、音源の総時間は 2575 秒である。音声特徴量として MFCC を各話者の音源から抽出し、教師あり学習SVM(Support-Vector-Machine) を用いて、話者識別モデルを作成する。なお MFCC (Mel-Frequency Cepstrum Coefficients) とは、音声認識を行う際に一般的に用いられる特徴量である。また SVM とは、教師あり学習アルゴリズムの一つであり、パターン認識手法の一つである。ここで教師あり学習とは、事前に問題とその解答をコンピュータに与え、機械学習のモデルを作成する学習法を指し、特徴を表すデータ(MFCC)と解答を示すデータ(話者)が必ず存在する。

単語列	読みあげたもの(一例)	語数
幼稚園 (愛知, 岐阜)	・岡崎女子短期大学付属第一早蕨 ・名古屋市立楠西 ・養老町立養北 ・中津川市立山口	200
東海道五十三次	・小田原 ・浜松 ・草津	53
日本の城50選	・五稜郭 ・明石 ・備中松山	50
平安時代	・大同 ・寛平 ・天仁	89
鎌倉時代	・承元 ・暦仁 ・徳治	48
江戸時代	・享保 ・明和 ・安永	35
元素記号	・ネオン ・バナジウム ・タングステン	71

図3. 単語列一覧

収録した 500 単語列のデータから、学習データとして 50 単語列、150 単語列、250 単語列、

350 単語列、450 単語列と増やした際の認識精度はそれぞれ、94.62%、96.69%、97.08, 97.47%、97.80% であった(F 値に基づく値)。この結果より、話者識別モデルとしての SVM が十分な識別性能を持つことを実証することができた。

話者	A	B	C	D	Recall(%)
A	2235	0	1	14	99.33
B	12	2168	25	45	96.36
C	89	94	2004	63	89.07
D	70	50	21	2109	93.73
Precision(%)	92.89	93.77	97.71	94.53	94.62
F値 (%)	96.01	95.05	93.19	94.13	94.62

図4. 50 単語列を用いたときの認識精度

話者	A	B	C	D	Recall(%)
A	1745	0	1	4	99.71
B	8	1717	8	17	98.11
C	44	42	1639	25	93.66
D	47	26	10	1667	95.26
Precision(%)	94.63	96.19	98.85	97.31	96.69
F値 (%)	97.11	97.14	96.19	96.27	96.69

図5. 150 単語列を用いたときの認識精度

話者	A	B	C	D	Recall(%)
A	1242	0	2	6	99.36
B	6	1230	2	12	98.40
C	26	30	1174	20	93.92
D	30	8	4	1208	96.64
Precision(%)	95.25	97.00	99.32	96.95	97.08
F値 (%)	97.26	97.70	96.55	96.79	97.08

図6. 250 単語列を用いたときの認識精度

話者	A	B	C	D	Recall(%)
A	747	0	0	3	99.60
B	3	739	0	8	98.53
C	15	14	710	11	94.67
D	16	4	2	728	97.07
Precision(%)	95.65	97.62	99.72	97.07	97.47
F値 (%)	97.58	98.08	97.13	97.07	97.47

図7. 350 単語列を用いたときの認識精度

話者	A	B	C	D	Recall(%)
A	249	0	0	1	99.60
B	1	248	0	1	99.20
C	5	5	237	3	94.80
D	5	1	0	244	97.60
Precision(%)	95.77	97.64	100.00	97.99	97.80
F値 (%)	97.65	98.41	97.33	97.80	97.80

図8　450 単語列を用いたときの認識精度

4. まとめと今後の課題

本研究では複数のセンサ信号と履歴情報を統合的かつ選択的に扱うためのプライバシー保護技術を目的として、攻撃に対する脆弱性の評価に備えるための基礎的な実証実験を行った。まずウェアラブルセンサを用いて、以降の研究に必要な行動データのコーパスを小規模な範囲で構築した。続いて個々のセンサ信号に対する個人情報の同定技術を開発する必要があるが、本報告では加速度信号と音声信号に対象を絞り、認識精度を調査した。実験により、加速度信号の識別にはランダムフォレストが、音声信号の識別にはサポートベクトルマシンが有効であることが明らかとなった。

今後の課題として、再帰型ニューラルネットなど時系列構造を考慮した行動識別モデルの適用が挙げられる。またセンシングデータの行動コーパスの大規模化も今後の課題である。本研究の目的であるセンサーデータに対する具体的なプライバシー保護技術については、当該年度では十分な成果を挙げることができなかった。今後も引き続き検討していく必要がある。

なお本報告におけるデータ収集実験の被験者は全て愛知工業大学の学生であり、ボランティアとして協力した。事前に研究目的や内容、データの取り扱いについて十分な説明を行い、各人の自由意志により実験を行った。

参考文献

[1] F. Pedregosa, G. Varoquaux, A. Gramfort, and V. Michel. Scikit-learn: Machine learning in Python