様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ９ 月 １９ 日現在

機関番号：６２６０３
研究種目：挑戦的萌芽研究
研究期間：2014～2015
課題番号：２６５４００８９

研究課題名（和文）プライバシー保護を考慮した個人の同一性判定技術の創出

研究課題名（英文）Study on probabilistic indicator for person-equivalence and anonymity

研究代表者
松井　知子（Matsui, Tomoko）

統計数理研究所・モデリング研究系・教授

研究者番号：１０３７００９０

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：カーネル平均について検討を行い、音声のようなi.i.d.を仮定することが難しい時系列データに対しては、カーネル平均を用いた個人性判定はできない問題があることを明らかにした。この問題に対してWild Bootstrap法による解決を検討したが、音声データはデータ間の相関の強さが動的に変化するためにその方法の適用にも問題があることを確認した。また、DNNを用いて個人性判定を行う方法の検討を行い、個人ごとの音声データが数分の長さで大量に利用できない場合には、DNNがうまく学習できず、十分な精度が得られないことを実験的に確かめた。PIPAについては今後、新たな方向性を検討する必要がある。

研究成果の概要（英文）：We studied on maximum mean discrepancy (MMD) which is an instance of an integral probability metric with kernel methods and found that it is difficult to use MMD as the probabilistic indicator for person-equivalence for non-i.i.d. data. To deal with the problem, we examined to use the wild bootstrap method and found that there were dynamic and strong correlation in speech data and the high performance of the wild bootstrap method was not expected. Morever, we experimentally found that a deep neural network (DNN) based method did not perform well when the available data amount was not sufficient. Future work includes to investigate a new research direction for the probabilistic indicator for person-equivalence.

研究分野：統計的機械学習、音情報処理

キーワード：プライバシー保護　個人認証　音声データ

１．研究開始当初の背景

(1) 様々な分野でビッグデータの利活用が模索されているが、その便益を個人に還元することは難しい。個人への還元のためには、まずは個人の同一性を判定できる必要があるが、現行の個人情報保護法等を遵守した個人の同一性判定技術の開発利用は困難であり、各分野で分散して単独で存在しているビッグデータを連携することも妨げられている。しかし、例えば複数の業態の顧客データを取得し、様々な属性情報（購入商品リストなど）とひも付けることができれば、顧客の詳細な購買パターンの分析ができ、顧客サービスの向上に活用できるであろう。今、プライバシー保護を担保しつつ、ビッグデータを効果的に連携する技術が強く求められている。

(2) 顔画像の生体データによる個人の同一性判定技術に関しては、Google 画像検索サービスが提供されるなど、利用が開始されつつある。しかし、質の低い顔画像や、音声や映像などの動的に変動するデータについてはまだ研究段階にある。ブラジルでは飲酒運転の取締において顔認証技術で個人を特定する取り組みが始まったり、日本の泉州銀行では音声認証技術を用いた本人確認を行うなど、生体データによる個人の特定技術は実用されつつある。しかし、生体データはそもそも体調や経年変化によるゆらぎを含み、利用環境により十分な性能は得られていない。

２．研究の目的

(1) 本研究では、音声や人物画像、行動信号などの生体データによる同一性判定の不確実性を積極的に利用した逆転の発想による「プライバシー保護を考慮した個人の同一性判定」技術の確立を目指す。

(2) 個人の同一性と匿名性を同時に表す確率的指標 PIPA (Probabilistic Indicator for Person-equivalence and Anonymity)、及び PIPA に基づく生体の個人データを用いた「プライバシー保護を考慮した個人の同一性判定」技術 PPED について研究する。

３．研究の方法

(1) 本研究は、PIPA/PPED の方法を開発するチーム（松井、南）と、特徴量解析と実証実験を行うチーム（松井、武田）の２チーム体制で遂行する。

(2) 方法開発チームでは、PIPA として特徴量の分布を柔軟に表現できるカーネル平均[1]を導入することを考える。また、代替アプローチとして Deep Neural Network (DNN)を導入することを考える。

(3) 特徴量解析・実証実験チームでは、音声や行動信号を対象として、PIPA/PPED に有効な特徴量を検討する。

４．研究成果

(1) 方法開発チームでは、カーネル平均について検討を行った。カーネル平均は、入力データを超高次元空間に写像した上で、その分布の形を詳細かつ柔軟に表現する量である。この量に基づく検定は、従来の確率分布に基づく検定よりも、微細な分布の違いを捉えられる可能性がある。しかしながら、そのアルゴリズムの解析を通して、音声のような i.i.d.

を仮定することが難しい時系列データに対しては、カーネル平均を用いた個人性判定は難しいことを明らかにした。

この問題に対して Wild Bootstrap 法[2]による解決を試みた。しかし、音声データはデータ間の相関の強さが動的に変化するために Wild Bootstrap 法の適用にも問題があることを確認した。

また音声データについて、DNN[3]を用いて個人性判定を行う方法の検討を行い、個人ごとの音声データが数分の長さで大量に利用できない場合には、DNN がうまく学習できず、十分な精度が得られないことを実験的に確かめた。

カーネル平均や Wild Bootstrap 法とは異なる方法について、位置情報のプライバシー保護の問題に取り組みながら検討を行った（雑誌論文③)。PIPA については今後、新たな方向性を検討する必要がある。

(2) 特徴量解析・実証実験チームでは、音声データについてケプルトラム特徴量を使用して、Wild Bootstrap 法による個人性判定の実証実験を行い、同一時期に発声した音声データ（話者 5 名）に対しては高い性能が得られるが、異なる時期に発声した時期差変動を含む音声データ（話者 12 名）に対しては十分な性能が得られないことを確かめた。

具体的には、学習用音声データ $X=\{x_1,x_2,x_3,\cdots,x_T\}$、評価用音声データ $Y=\{y_1,y_2,y_3,\cdots,y_T\}$に対して、H0: X = Y （X と Y は同話者が発声した音声であるという仮定)、H1: $X \neq Y$ (X と Y は異なる話者が発声した音声であるという仮定)のカーネル平均による個人性判定を次の二つの実験条件のもとで行った。

実験条件 1：

データベース	同時期に収録
話者数	5
発声内容	15 文章／話者
評価タイプ	Round-Robin
カーネル関数	RBF
特徴量	メルケプストラム 39 次元

実験条件 2：

データベース	複数時期に収録した 10 文章（NTT-VR データ）
話者数	12
発声内容	10 文章／話者
学習時期	1990 年 12 月
評価時期	1991 年 9，12 月
カーネル関数	RBF
特徴量	メルケプストラム 39 次元 メルケプストラム＋Δ, Δ^2 計 60 次元

実験結果を次に示す。なお、謝り率計算では各話者ごとに全文章の判定結果による多数決方式を採用した。

実験結果：

謝り率	本人棄却率	他人受理率
実験条件 1	0%	0%
実験条件 2: 特徴量 39 次元	26.0%	13.3%
実験条件 2： 特徴量 60 次元	28.9%	12.7%

上記の実験結果から特徴量の次元によらず、学習と評価時期が異なる実験条件 2 では謝り率が大きい。

(3) プライバシー保護についてのサーベイを行い、その結果をまとめて論文発表した（雑誌論文①）。

<参考文献>

[1] W. Zaremba, A. Gretton, and M. Blaschko, “B-test: A Non-parametric, Low Variance Kernel Two-sample Test,” NIPS, 2013.

[2] K. Chwialkowski., D. Sejdinovic, and A. Gretton, “A Wild Bootstrap for Degenerate Kernel Tests,” NIPS, 2014.

[3] Theano – CPU/GPU symbolic expression compiler in python: http://deeplearning.net/software/theano/

５．主な論文発表等

〔雑誌論文〕（計３件）

① 南　和宏, “ビッグデータの活用とプライバシー保護技術,” 統計, 査読無, 9巻, 2015, pp. 8-13.

② Nicolas Schwind, Morgan Magnin, Katsumi Inoue, Tenda Okimoto, Taisuke Sato, Kazuhiro Minami and Hiroshi Maruyama, “Formalization of resilience for constraint-based dynamic systems,” Journal of Reliable Intelligent Environments, 査読有, Vol. 2, 2015, pp. 17-35.

③ Tomoya Tanjo, Kazuhiro Minami and Hiroshi Maruyama, “Evaluating data utility of privacy-preserving pseudonymized location datasets,” JoWUA, 査読有, Vol. 5, 2015, pp. 63-78.

〔学会発表〕（計０件）

〔図書〕（計０件）

〔産業財産権〕（計０件）

〔その他〕

特になし。

６．研究組織

(1) 研究代表者

松井　知子 (MATSUI TOMOKO)

統計数理研究所・モデリング研究系・教授

研究者番号：10370090

(2) 研究分担者

武田　一哉 (TAKEDA KAZUYA)

名古屋大学・情報科学研究科・教授

研究者番号：20273295

南　和宏 (MINAMI KAZUHIRO)

統計数理研究所・モデリング研究系・准教授

研究者番号：10579410

(3) 研究連携者

なし。

(4) 研究協力者

なし。