人間と情報環境の共生インタラクション基盤技術の創出と展開　2022 年度
2018 年度採択研究代表者　年次報告書

山岸 順一

情報・システム研究機構 国立情報学研究所
教授

VoicePersonae: 声のアイデンティティクローニングと保護

研究成果の概要

VoicePersonae プロジェクトでは、①声のアイデンティティに関する機械学習を高精度化すると同時に、②生体認証の安全性と頑健性を高め、③プライバシー保護に関する新しい技術を実現する。また④音声変換と生体検知、匿名化と再識別化と言った目的が相反する技術をどちらも加速させる敵対的競争型研究を実施する。更に⑤他のモダリティへ研究成果を適用する事も行っている。

2022 年度は②、③、④、⑤において成果を挙げた。②においては、Self-supervised learned model と呼ばれる自己教師あり学習モデルの内部表現を、音声のディープフェイク検出を行う識別モデルの特徴量と利用することで、未知手法によるフェイクメディアを様々な劣悪条件下で検出できることを示した。さらに学習用データベース自身をダイナミックに自動拡張するアルゴリズムも提案し、ディープフェイク検知モデルの汎化性能をさらに向上させる事にも成功した。③においては、音声の話者性のみを抑圧する話者匿名化システムを言語依存性の少ないシンプルで洗練された枠組みに改良する事に成功し、システム構築に必要な教師データの種類も減らせる事を示した。また話者匿名化システムとほぼ同様の枠組みで、音声中の性別に起因する特徴のみをマスキング処理し、音声を再合成する事も可能にした。④話者匿名化手法を共通データベースで相互比較する Voice Privacy Initiative 2 も開催し、国際ワークショップにおけるスペシャルセッションも開催した。

⑤他のモダリティでの研究成果も挙げた。ディープフェイク顔画像を、背景領域にハイディングした微小ノイズに基づき、改ざん前のオリジナルの顔画像に復元するという新たな課題に取り組み成果を挙げた。また、文章の内容を知識 DB と比較して事実であるかどうかを機械学習により検証する自動ファクトチェック技術において、新しい知識データベースが利用可能になった際に、知識の破壊的忘却が起きない様にしつつモデル更新を行う学習法の提案を行なった。

【代表的な原著論文情報】

1) Xin Wang, Junich Yamagishi, "Investigating Active-learning-based Training Data Selection for Speech Spoofing Countermeasure", The 2022 IEEE Spoken Language Technology Workshop (SLT 2022), 2023 年 1 月

2) Xiaoxiao Miao, Xin Wang, Erica Cooper, Junichi Yamagishi, Natalia Tomashenko, "Language-Independent Speaker Anonymization Approach using Self-Supervised Pre-Trained Models", Odyssey 2022: The Speaker and Language Recognition Workshop, 2022 年 6 月

3) Canasai Kruengkrai, Junichi Yamagishi, "Mitigating the Diminishing Effect of Elastic Weight Consolidation", THE 29TH INTERNATIONAL CONFERENCE ON COMPUTATIONAL LINGUISTICS (COLING 2022), 2022 年 10 月