経営情報学科 | キーワード | マルチメディア（画像・映像・音響・文書）処理、人工知能AI、トラスト・コミュニケーション、機械学習

教授 / 工学博士
馬場口　登
Noboru Babaguchi

学歴

大阪大学工学部通信工学科卒業、大阪大学大学院工学研究科通信工学専攻前期課程修了

経歴

愛媛大学工学部助手、大阪大学工学部助手・講師、同産業科学研究所助教授、工学研究科教授、同教育研究評議員、工学研究科長・工学部長、総長参与、名誉教授、文部省在外研究員（米国・カリフォルニア大学サンディエゴ校）、国立情報学研究所客員教授、日本学術会議連携会員

相談・講演・共同研究に応じられるテーマ

知能メディア工学：AIに基づくマルチメディアの生成と認識
視覚的プライバシー保護、マルチメディア処理全般

メールアドレス

babaguchi@fukui-ut.ac.jp

主な研究と特徴

「メディアクローン攻撃を防御するコミュニケーション系」

本物に限りなく近いが本物ではないメディア（音声、画像、映像、文書など）の流通が、社会的脅威となりつつある。親族・知人の声色を真似ることによる老齢者への特殊詐欺、いわゆるオレオレ詐欺はこの典型例であり、このようなメディアの受け手を、メディア情報の生成解析技術を援用して防御することが、安全安心社会の実現に向けて喫緊かつ重要な課題である。本研究では、実空間で取得される実体を表す真正メディアに限りなく近いが本物ではないメディアをメディアクローン（Media Clone：MC）と呼び、メディアクローン攻撃を防御するコミュニケーション系の設計と実現に関して考察すると共に、フェイク情報化の防止、メディアクローンの生成・認識法など、トラスト・コミュニケーションの構成要素の具体化を目的とする。図１に研究成果の一例として、音声と同期した顔動画クローンの生成枠組を示す。本テーマは日本学術振興会・科学研究費補助金・基盤研究（S）として実施された。

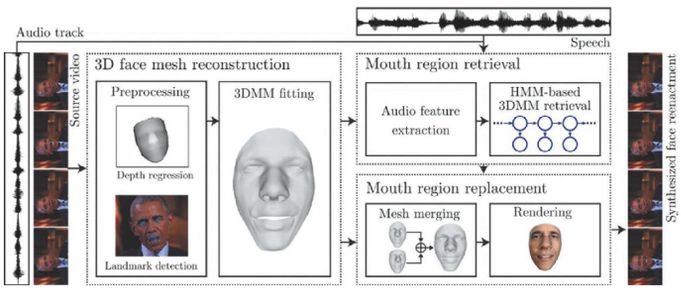

図1. 顔動画クローンの生成の枠組

「インフォデミックを克服するソーシャル情報基盤技術」

本研究は、AIにより生成されたフェイクメディア（Fake Media：FM）がもたらす潜在的な脅威に適切に対処すると同時に、多様なコミュニケーションと意思決定を支援するソーシャル情報基盤技術を確立することを目的とする。具体的には、AIにより生成されたフェイク映像、フェイク音声、フェイク文書などの多様なモダリティによるFMを用いた高度な攻撃を検出・防御する一方で、信頼性の高い多様なメディアを積極的に取り込むことで人間の意思決定や合意形成を促し、サイバー空間における人間の免疫力を高めるソーシャル情報基盤技術を確立する。図２に本研究プロジェクトの概略図を示す。本テーマは、文部科学省が選定した戦略目標「信頼されるAI」のもとに発足したJST/CREST「信頼されるAIシステムを支える基盤技術」の一環として推進され、国立情報学研究所、東京工業大学との共同研究である。

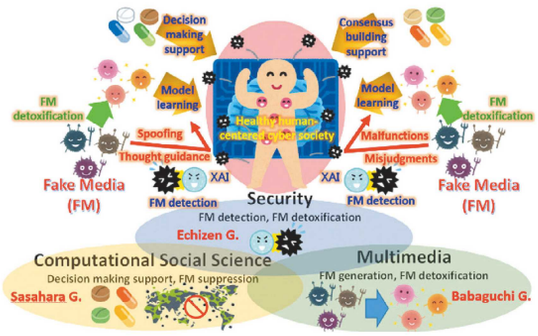

図2. 研究プロジェクトの概略図

今後の展望

AIにより生成されるFMとして3つの型を取り上げ検討を進める。具体的には、本物に限りなく近いが本物ではないメディアクローン（MC）型FM、世論操作などを目的として素材となるメディアを意図的に編集して生成したプロパガンダ（PG）型FM、人間には識別困難だが、AI技術を誤動作・誤判定させることを目的に生成した敵対的サンプル（AE）型FMを取り上げ、これらのFMを生成、検出する技術を確立する。特に、PG型FMの表現メディアである画像と動画（音響を含む）を対象に、人間に対して印象操作を促す表現や編集の技法を、明らかにするとともに、知能メディア技術と機械学習を援用してFMの生成と認識に取り組む。PG画像については、画像表現において、人間の印象にインパクトを与えるオブジェクトの検出を試みる。一方、PG動画については、PG動画に特有の印象操作技法を調べ、大量の動画データでそれらの影響や効果を検証する。

所属学会

電子情報通信学会（フェロー、PRMU/EMM研専委員長）、映像情報メディア学会（関西支部長、副会長）、人工知能学会（評議員）、情報処理学会、IEEE（Senior Member）、ACM（ACM Multimedia2012 General Co-Chair）

主要論文・著書

M. Khosravy, K. Nakamura, Y. Hirose, N. Nitta, N. Babaguchi: “Model Inversion Attack by Integration of Deep Generative Models Privacy-Sensitive Face Generation from a Face Recognition System”, IEEE Transactions on Information Forensics and Security, Vol. 17, pp. 357-372, Jan 2022.

N. Babaguchi, et al.: "Preventing Fake Information Generation Against Media Clone Attacks", IEICE Transactions on Information and Systems, vol. E104-D, no.1, pp. 2-11, January 2021.

馬場口登、山田誠二、“人工知能の基礎　第2版”、オーム社、2015.