【基盤研究（S）】
総合系（情報学）

研究課題名　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

大阪大学・大学院工学研究科・教授　馬場口（ばばぐち）　登（のぼる）

研究課題番号：16H06302　研究者番号：30156541
研究分野：人間情報学　知覚情報処理
キーワード：視覚メディア処理、音声情報処理、プライバシー保護

【研究の背景・目的】

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、メディアクローンの生成・認識法など、その系を構成する要素の具体化を目的とする。

【研究の方法】

図１に本研究で対象とするコミュニケーション系の枠組と研究課題を示す。情報の送り手 Alice が情報をメディア表現（音声、映像など）し、物理・サイバーチャネルを通して受け手 Bob に送るものとする。このとき、悪意を持った送り手 Eve が存在し、Alice のプライバシー情報や生体情報、並びに Alice が位置する世界の情報（環境情報と呼ぶ）を取得し、Alice 由来のものではないフェイク情報を作成する。そして、フェイク情報に基づき Alice 由来の真正メディアに限りなく近いメディアクローンが作成され、Eve から Bob へ攻撃がなされる。

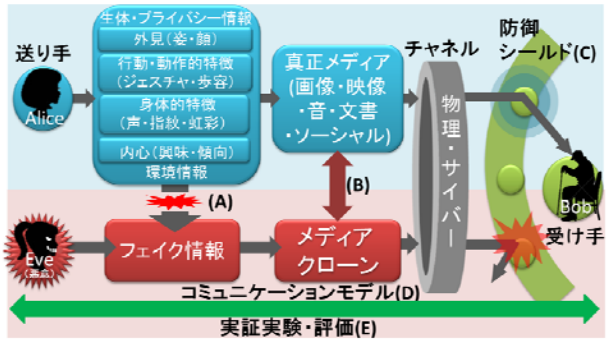

図１メディアクローン攻撃を含むコミュニケーション系

このようなメディアクローン攻撃を防御しうるコミュニケーション系の実現を図るために、以下の５つの研究課題（図１参照）に分けて研究開発を進める。(A)フェイク情報化防止のために、生体情報、プライバシー情報、および環境情報の保護手法を確立する。(B)フェイク情報を起源とするメディアクローン生成法の実現可能性を実験的に検証する。音声、画像、映像、文書、ソーシャルメディアなどを対象とし、個人適応型のメディア生成という統一的枠組で考察する。(C)メディアクローン攻撃の防御シールドをメディアクローンの認識により構成する。特に生体特徴に起因するライブネスの解析に着目する。(D)送り手・受け手の種々の状況を想定したコミュニケーション系をモデル化する。(E)構成要素、全体システムを実証実験により評価する。併せてテスト用データベースを作成し、順次、公開する。

【期待される成果と意義】

本研究を通して、プライバシー・生体情報などの保護と利活用が調和した安心なオープンシステム、老齢者・情報弱者にも優しい安心コミュニケーションの実現が期待される。さらに、メディアクローン生成・認識技術の開発により、時空・文化を超えるメディアの創成、メディアアートや福祉医療工学などの分野での新規イノベーション創出、メディア表現における本物らしさや人間らしさなど微妙な差異や質的変化を認識できる強力なパラダイムへのシフトなどが想定される。また、多様なデータの組織的集積によるデータ科学やオープン科学の展開、メディア処理・セキュリティ・コミュニケーションの境界領域において新規学術分野創成、研究人材育成などに寄与しうる。

【当該研究課題と関連の深い論文・著書】

・Y. Nakashima, T. Ikeno, and N. Babaguchi: “Evaluating Protection Capability for Visual Privacy Information”, IEEE Security & Privacy, Vol. 14, No. 1, pp. 55-61, 2016.
・N. Babaguchi and Y. Nakashima: “Protection and Utilization of Privacy Information via Sensing”, Invited Paper, IEICE Transactions on Information and Systems, Vol. E98-D, No. 1, pp. 2-9, 2015.

【研究期間と研究経費】

平成 28 年度－32 年度　120,700 千円

【ホームページ等】

http://www2c.comm.eng.osaka-u.ac.jp/proj/mc/index.html