科学研究費助成事業（基盤研究（Ｓ））公表用資料
〔平成３１年度（2019 年度）研究進捗評価用〕

平成２８年度採択分
平成３１年３月１５日現在

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

Communication System for Defending against Attacks of Media Clones

課題番号：16H06302

馬場口　登（BABAGUCHI, NOBORU）

大阪大学・大学院工学研究科・教授

研究の概要
本物に限りなく近いが本物ではないメディアクローンによる攻撃から受け手を防御する系を新たなコミュニケーション系として捉え、その系の構成要素となるフェイク情報化の防止・阻止法、メディアクローン生成法、受け手を攻撃から守る防御シールドの設計・実現法などの詳細を明らかにし、安心で人に優しいメディア・コミュニケーションの実現を目的とする。

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

１．研究開始当初の背景

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。

２．研究の目的

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（MC）と呼び、MC 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、MC 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。

３．研究の方法

MC 攻撃を防御するコミュニケーション系の具体化及びその評価として、以下の５つの研究項目に取り組む。
テーマ（A）【フェイク情報化】：MC の基となる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。
テーマ（B）【MC 生成】：フェイク情報を起源とする MC 生成法の実現可能性を実験的に検証する。表現メディアには、音声、画像、映像、文書、ソーシャルなど多メディアを対象とする。
テーマ（C）【MC 認識】：MC 攻撃の防御シールドを構成する。具体的には、真正メディア／MC を認識・分類問題として定式化し、計算メカニズムを明らかにする。
テーマ（D）【モデリング】：MC 攻撃を防御するコミュニケーション系をモデル化する。
テーマ（E）【実証実験評価】：コミュニケーション系の実証実験と評価を行う。

４．これまでの成果

テーマ（A）【フェイク情報化】
物理空間におけるフェイク情報化の防止法として、市販のカメラにより撮影された指の画像から指紋や静脈の情報が抽出可能と示し、それらの復元防止手法を開発した。
一方、各種センサにより取得されたプライバシー情報を含むメディアが流通し得るサイバー空間におけるフェイク情報化の防止法として、画像や映像中の顔や全身などの外見情報、位置情報などの行動履歴[1]を、メディアの価値を損なうことなく匿名化する手法を開発した。図１、２に示すように、真正メディアと判別できない自然さで、個人が特定されない匿名顔、匿名シルエットが生成できた。

図１：匿名顔

図２：匿名シルエット

テーマ（B）【MC 生成】

音声[2]、発話顔動画、全身動作動画、文書、ソーシャルメディアを対象とした MC 生成技術を具体化した。図３、４、５に示すように、生成ネットワークの他タスクに対する事前学習、他者の動作動画や肉筆の活用などにより、MC 生成対象人物の発話動画、全身画像、肉筆文字を少量与えたのみで、個人の特性を再現した発話顔動画クローン、全身動作動画クローン、文書クローンが生成された。

図３：発話顔動画クローン

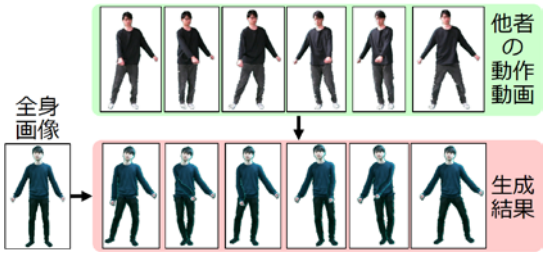

図４：全身動作動画クローン

図５：文書クローン

テーマ（C）【MC 認識】

特定個人のフェイク情報を含む顔動画[3]、全身動作動画、ソーシャルメディアを対象に、主に生体の特徴に起因した信号に着目した MC 認識方法を具体化した。図６に示すように、人の目では判別困難な MC も認識できる。また、環境情報のフェイク情報化を起源とする MC の一種である改ざんされた動画及び改ざん領域を検出する手法を開発した。

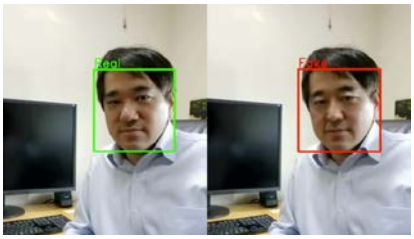

図６：顔動画クローン認識

テーマ（D）【モデリング】

電話を通し、音声により人を騙す MC のオレオレ詐欺において、人が騙されるときの思考を数理論理的アプローチの一種であるチャンネル理論を用いてモデル化し、情報の受け手が意味不定性を伴う情報を推定するプロセスによって騙され得ることを示した[4]。

テーマ（E）【実証実験評価】

音声メディアを対象に、MC生成・認識[5]に関する対戦型循環的チャレンジを開催した。これに伴い、真正メディアである英語話者の音声、MCとして収録音声、高品質な合成音声などで構成されるデータベースを公開した。最大５１チームと多くの参加者を得ており、MC生成・認識技術の向上に大きく貢献した。

５．今後の計画

テーマ(A)から(D)について、手法の完成度を上げると共に、綿密な性能評価を実施する。テーマ(E)について、音声に関する循環的チャレンジを研究コミュニティに浸透、定着させると共に、音声以外のメディアにも展開を試みる。実証実験で作成したデータベースは公開し、当該研究分野の活性化を図る。

６．これまでの発表論文等（受賞等も含む）

1. K. Nakamura, N. Nitta, and N. Babaguchi, Encryption-Free Framework of Privacy-Preserving Image Recognition for Photo-Based Information Services, IEEE Trans. on IFS, 14(5), pp.1264-1279, 2019.
2. X. Wang, S. Takaki, and J. Yamagishi, Autoregressive Neural F0 Model for Statistical Parametric Speech Synthesis, IEEE/ACM Trans. on ASLP, 26(8), pp.1406-1419, 2018.
3. D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, MesoNet: a Compact Facial Video Forgery Detection Network, Proc. WIFS, 7 pages, 2018.
4. S. Myojin and N. Babaguchi, A Logical Consideration on Deceived Person's Thinking, Artificial Life and Robotics, Springer, 24(1), 5 pages, 2018.
5. Z. Wu, J. Yamagishi, T. Kinnunen, C. Hanilci, M. Sahidullah, A. Sizov, N. Evans, M. Todisco, and H. Delgado, ASVspoof: the Automatic Speaker Verification Spoofing and Countermeasures Challenge, Special Issue on Spoofing and Countermeasures for Automatic Speaker Verification, IEEE J-STSP, 11(4), pp.1-17, 2017.

７．ホームページ等

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