2021 年度　傾斜的研究費（全学分）　研究報告書

【研究代表者所属】：東京都立産業技術大学院大学　産業技術研究科
【研究代表者氏名】：黄 緒平
【研究代表者氏名フリガナ】：コウ　ショヘイ
【研究代表者職】：助教
【国内研究分担者（所属、氏名、職）】
・無
【国外研究分担者（所属、氏名、職）】
・無

【研究課題名】：
IoT デバイスを用いたコロナ禍における遠隔学習効果の匿名解析手法と応用

【研究実績の概要（600～800 字程度で記入。図、グラフ等の使用も可。）】

本研究ではスマートバンドを用いて採集した脈拍等の生体情報にスペクトル解析を適用することで、遠隔授業時のストレス度合いを推定する手法を提案した。

また、遠隔会議の過程で採集できる生体データ画像を第三者に不正に二次利用されないよう、画像に電子透かしを埋め込む手法も提案した。写真が流出しても、顔認証等に悪用されないよう、画質に劣化を与えないように特徴値の位置に特化した埋め込みを行った。顔写真を入力データとし、スケール不変特徴変換（SIFT）特徴値への可逆回転に基づいた電子透かし埋め込み場所の特定手法を提案する。また、電子透かしを除去する際、元のデータに無損失に復号できるよう、特徴値の位置への整数回転方式を提案した。座標に角度パラメータによる可逆な整数回転を適応した後、スケールのヒストグラム及び劣化の期待値を用い、回転された位置に埋め込みを行う。平均ステゴデータ生成の計算時間は 0.397s で、ピーク信号対雑音比 は 50.595 dB 及びエントロピーは 5.216 であり、本手法の有効性を示した。

更に、遠隔会議や遠隔学習の過程で録画されている音声データのプライバシー保護にも着目した。音声合成の高速な発展により、他人の声紋から声を模擬・生成できるようになった。オレオレ詐欺等一般公共放送や録音データから入手した DC 変換後の音声データが不正に利用されるケースが増えている。悪用を防ぐために音声データを匿名化し、保護することが喫緊な課題である。本研究は話者の個人プライバシー情報の保護、録音データから取得する声紋などの個人情報から話者を特定されにくいよう、音声匿名化手法を提案した。更に、音声コンテンツの偽造の検出、話者の成りすましを高精度に識別出来る電子透かし手法及び機械学習を用いた話者感情検出による話者なりすましの検出手法を提案し、実装した。主に音声信号を時系列から周波数領域へ整数コサイン変換を適用し、ラプラス雑音及びガウシアンノイズを生成し、時系列に付加することによって，声紋保護を図った。対外公表に国際会議 IEEE ICIP 併設ワークショップの招待論文を１件予定している。

【学会発表（発表題目、発表大会名、年月を記入）】

[1] Xuping Huang, Shunsuke Mochizuki and Katsunari Yoshioka, "Towards Estimating Radio Resources Wasted by IoT Botnet Attacks", The 16th International Workshop on Security (IWSEC 2021), Tokyo, Sep,2021

【論文発表又は著書発行（発表題目、著者、発表誌又は出版社、年月を記入）】

[2]黄緒平，望月俊輔，吉岡克成，IoT マルウェア感染解析における通信形態及びアップリンク速度の推定手法，情報処理学会研究報告，vol. 2021-CSEC-95(18), pp.1-6, Sep, 2021
[3] Xuping Huang, “A scheme towards medical data confidentiality using scale invariant feature transform”, Bulletin of Advanced Institute of Industrial Technology, vol. 15, pp. 7-14, Jan, 2022
[4]黄緒平，望月俊輔，藤田　彬，吉岡克成，マルウェア感染ユーザへの ISP による注意喚起活動のシミュレーション，信学技報，情報通信システムセキュリティ研究会シンポジウム，March, 2022
[5] 竹下虎太朗，福永修一，田中覚，黄緒平，プライバシ保護機能を持つベータダイバージェンスを用いたロバスト線形回帰，電子情報通信学会誌，Vol.J105-A, No.6，2022 年 6 月（採録済、掲載予定）

【作品等】

無し

【科学研究費助成事業への応募状況、採択状況】

・科研費・若手研究，プライバシー保護した音源偽造及び話者成りすましの識別に関する研究，研究代表者（継続）

【国等の提案公募型研究費、企業からの受託研究費・共同研究費の獲得状況】

・無し

【受賞等】

・受賞 2 件：

1)　情報処理学会コンピュータセキュリティ研究会 CSEC95 優秀研究賞，2022 年 3 月

2)　Best Poster Award, 16th International Workshop on Security (IWSEC 2021), 2021, 9

【その他社会貢献】

[公的審議会・委員会等の公的貢献、生涯学習支援・普及啓発、国際貢献・国際交流等]

・情報処理学会のコンピュータセキュリティ研究会（CSEC）　運営委員

・情報処理学会ジャーナル特集号「量子時代をみすえたコンピュータセキュリティ技術」　編集委員

・国際会議 ACM Multimedia や ICISS 等　　テクニカルプログラム委員

・国際会議 International workshop of security（IWSEC）　実行委員

【研究成果による特許等の工業所有権の出願・取得状況】

（工業所有権の名称、発明者、権利者、工業所有権の種類・番号、出願年月日、取得年月日）

・無し

【研究分担額】

（研究代表者・分担者名、所属、金額（円））

・研究代表者：黄緒平，東京都立産業技術大学院大学，40 万円