様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 ２４ 日現在

機関番号：１５２０１
研究種目：若手研究
研究期間：2018～2023
課題番号：１８Ｋ１８０５２

研究課題名（和文）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

研究課題名（英文）Privacy preserved acoustic-falsification detection and speaker verification

研究代表者
黄　緒平（HUANG, Xuping）

島根大学・学術研究院理工学系・准教授

研究者番号：２０７３４１１４

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：　共放送を含む公共の場で録音した音声サンプルを用いて、発話者の声を模擬・再現・発声・変声させることで，個人の許可を得ず他者なりすまし、更に、本人の意図せずに原音そっくりの声によるコンテンツ改ざんができるようになった。本研究では、高音質を維持しながら、人間聴覚システムにおいて知覚しにくい周波数帯域に、原音の電子署名のダイジェスト情報を無損失かつ完全に復元できる電子透かし手法を提案することによって、改ざん検出及び話者識別を含むデータの真正性の保証を実現した。データの完全復元可能な整数コサイン変換アルゴリズムを適応し、高音質を維持しながら、高精度に改ざん検出可能な音声電子透かし手法を提案した。

研究成果の学術的意義や社会的意義
本研究は証拠性の高い音声信号データの信ぴょう性及び完全性を保証する電子透かし技術を提案し、新規性及び有用性の両面において実証実験を行った。本研究を用いることによって、オレオレ詐欺等の他者成りすまし及びコンテンツの偽造を高精度に検出することができた。また、高音質を維持しながら、人間の聴覚に気づかれにくい周波数領域に雑音摂動する手法も提案し、話者の個人プライバシー情報を保護し，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手法を実現した。本手法を用いることで、インターネット上の一般ユーザでも、声が盗まれない、偽造されないような安心安全の社会構築に貢献できた。

研究成果の概要（英文）：　By simulating, reproducing, vocalizing, and altering the speaker's voice using speech samples recorded in public places, it is possible to impersonate another person without the individual's permission, and furthermore, to alter the content by using a voice that sounds exactly like the original voice without the individual's intention. In this research, we propose a reversible digital watermarking method to embed digest information of the original digital signature in the frequency domain for verification of the integrity of the original data, by adapting the integer cosine transform algorithm, which assures the reversibility. The proposed method is imperceptible to the human auditory system while maintaining high sound quality, thereby realizing data authenticity assurance including tamper detection with high precision.

研究分野：情報セキュリティ

キーワード：電子透かし　改ざん検出　成りすまし検出　プライバシー保護　スペクトル解析　音声匿名化　可逆な音声信号処理　雑音摂動

様　式　Ｃ－１９、Ｆ－１９－１（共通）

課題番号：18K18052 提案者：黄　緒平

１．研究開始当初の背景

ソーシャルネットワーク及び自由に移動・撮影できる携帯やドローンなどの録音・録画装置が高速に普及し，その場で採取したデータが高速通信方式にて転送・共有される．個人の顔画像や動画が許可なく成りすまし詐欺などに悪用されることが懸念されている．また，機械学習による音声合成手法が開発され，難病が起因する発話困難の障碍者のため，短時間の機械学習により原話者の声を模擬・再現・発声できるVoiceBank プロジェクトの開発・研究が進んでいる．これが悪用されると，今まで横行したオレオレ詐欺や成りすましが社会的な脅威に成り得る．従来の解決策として話者識別が提案されているが，音声合成技術の発展により，原音と最大限に近似できる模擬音声が合成され，今までの話者識別に使われる混合ガウス分布モデルなどを用いて分析しても，オリジナル話者と偽話者の特徴値の違いを区別出来なくなった．

また，動画の偽造技術において，メル周波数ケプストラム係数を用いて音声の特徴値を抽出し，再帰型ニューラルネットワークを用い，大規模な学習データに基づき，音声の特徴値に合わせて動画話者の口元を動かし，原話者が話しているように，偽動画コンテンツを作成するリップシンク(LipSync) 技術が実現された．動画の背景も違和感なく合成されるため，この技術が悪用されればコンテンツ自体の真偽を判断できなくなる．

２．研究の目的

1) オリジナル話者を識別するための特徴値推定

オリジナル話者を偽話者から区別するため，心理音響システムに基づいて話者の生体信号から特徴量を推定する手法を検討する．具体的にはで確立した整数離散コサイン変換手法（intDCT）を用いて声紋情報を抽出し，使用後に完全に取除けるよう，オリジナル音声データの高周波数成分に付随させるアルゴリズムを新たに提案する．複合データから抽出した特徴値を用いて，オリジナル話者認証の精度を検証する．

2) 音声匿名化をサンプリングデータに部分的に適応するアルゴリズムの実現

二つの音声を物理的に混ぜるのではなく，特定周波数帯域から作られた保護音の模擬ノイズをペイロードとして原音に埋め込む電子透かし手法によって話者のプライバシー保護を可能とする．原音への音質に対する影響を考慮しながら，模擬ノイズと埋め込み場所其々の最適な周波数帯域を探索するアルゴリズムを新たに提案し，音質を保証しつつ，話者照合の精度を低下させることを図る．

３．研究の方法

テーマ1: 偽話者とオリジナル話者を識別できる特徴値の推定

オリジナル話者と擬似他人との分別を目的とする．個人の発声録音データから生体特徴値の検出を行い，主にDCT 成分の分析による声紋の採集・分析を行う．模擬話者の音声作成は原話者のデータから周波数変形，エコー法，マスキング法，雑音付加などにより自動生成させる予定である．その中，どれが識別に影響を与えるかを確認する．

テーマ2: コンテンツの偽造・改竄を検出するアルゴリズムの確立

これまで申請者が音声時系列データの可逆圧縮及び周波数領域のDCT 係数拡張により音声コンテンツのフレーム毎のハッシュ値の埋め込み・抽出・照合に基づいて改竄検出を高

精度で実現したが，攻撃への耐性が課題になっている．本研究はコンテンツの偽造を検出するため，コンテンツ依存の特徴値を原音に埋め込む手法を新たに提案する．具体的には圧縮センシング手法，周波数領域の線形予測，DCT 整数回転と拡張の三つのアルゴリズムを提案し，これにより認証データの埋め込み場所を生成する．

４．研究成果

申請者はこれまでの研究成果として，原音の音質を維持したまま高周波数成分の拡張により特徴値を埋め込むことで，改竄検出を可能にする研究を行ってきた．本研究は話者の個人プライバシー情報を保護し，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，期間中申請者は，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を新たに提案した．人間の聴覚システムにおいて，高い周波数領域における振幅拡張による埋め込み手法を提案し，埋め込み周波数帯域別にて実証実験を行い，音質及び埋め込み容量別において手法の有用性を評価した．更に，攻撃への耐性を考慮しながら埋め込み領域をアダプティブに選定し，原音に依存せず話者成りすましの判別とデータの真偽をブラインドかつ高精度に検出できる電子透かし手法を確立した．新たな音声保護における声紋匿名手法について展開し，アルゴリズムの提案及び実証実験を行った．主な発表概要について，音質の劣化を抑えつつ，ガウシアンノイズによる雑音摂動によって声紋保護を図った．更に，これらの提案手法に対し，LSBゼロ及び周波数帯域のデータ削除，ガウシアンノイズ付加等の攻撃に対する攻撃耐性を評価した．提案手法を用いることで，セキュリティユーティリティを保証しながらより振幅の小さい雑音を生成し，声紋を保護することができた．また，改ざん箇所を100%の正解率，かつ0.032sの前後誤差まで高精度に検出することができた．

５．主な発表論文等

〔雑誌論文〕　計17件（うち査読付論文　8件／うち国際共著　0件／うちオープンアクセス　9件）

１．著者名 Xuping Huang, Shunsuke Mochizuki, Fujita Akira, Katsunari Yoshioka	４．巻 vol.31
２．論文標題 Simulating and Estimating the Effectiveness of Security Notification by ISP to Malware-Infected Users	５．発行年 2023年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 165-173
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.31.165	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Xuping HUANG	４．巻 vol. 16
２．論文標題 Lossless Compression based Audio Watermarking	５．発行年 2023年
３．雑誌名 Bulletin of Advanced Institute of Industrial Technology	６．最初と最後の頁 17-22
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Xuping Huang, Shunsuke Mochizuki,Katsunari Yoshioka	４．巻 vol. 15
２．論文標題 Connection Type Identification and Uplink Speed Estimation of Malware Infected Hosts	５．発行年 2022年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 859-864
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.30.859	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Xuping Huang, Shunsuke Mochizuki, Katsunari Yoshioka	４．巻 2023-DPS-194
２．論文標題 Simulation of Security Notification Towards Malware-Infected Users Considering ISPs Scale	５．発行年 2023年
３．雑誌名 IPSJ SIG Technical Reports	６．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 竹下 虎太朗, 福永 修一, 田中 覚, 黄 緒平	4．巻 Vol.J105-A, No.6
2．論文標題 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	5．発行年 2022年
3．雑誌名 電子情報通信学会誌	6．最初と最後の頁 1-9
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transfunj.2021JAP1023	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Xuping HUANG	4．巻 vol. 15
2．論文標題 A scheme towards medical data confidentiality using scale invariant feature transform	5．発行年 2022年
3．雑誌名 Bulletin of Advanced Institute of Industrial Technology	6．最初と最後の頁 7-14
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 黄　緒平, 望月俊輔, 藤田　彬, 吉岡克成	4．巻 vol. IEICE-121
2．論文標題 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	5．発行年 2022年
3．雑誌名 情報通信システムセキュリティ研究会シンポジウム	6．最初と最後の頁 141-146
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 黄　緒平, 望月俊輔, 吉岡克成	4．巻 2021-CSEC-95(18)
2．論文標題 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	5．発行年 2021年
3．雑誌名 情報処理学会研究報告	6．最初と最後の頁 1-6
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 黄緒平	4．巻 vol. 2020-SPT-38(15)
2．論文標題 スペクトル領域上の雑音摂動法における雑音抑圧手法	5．発行年 2020年
3．雑誌名 情報処理学会報告集Computer Security Symposium	6．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Xuping HUANG, Ryota Kawashima	4．巻 -
2．論文標題 Privacy preserving using differential privacy based on modified integer DCT for noise suppression	5．発行年 2020年
3．雑誌名 International Journal of Machine Learning and Computing	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Xuping Huang	4．巻 -
2．論文標題 A New Watermarking Scheme Based on SIFT Feature Points with Reversible Rotation	5．発行年 2020年
3．雑誌名 IEEE Proc. of 2019 First International Conference on Digital Data Processing (DDP)	6．最初と最後の頁 59-64
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/DDP.2019.00021	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 黄　緒平	4．巻 2019
2．論文標題 SIFT特徴値の可逆回転による電子透かし手法	5．発行年 2019年
3．雑誌名 情報処理学会報告集Computer Security Symposium	6．最初と最後の頁 125-131
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 HUANG Xuping	4．巻 -
2．論文標題 Watermarking Based Data Spoofing Detection Against Speech Synthesis and Impersonation with Spectral Noise Perturbation	5．発行年 2018年
3．雑誌名 Proc. of IEEE International Conference on Big Data (Big Data) 2018	6．最初と最後の頁 4600-4604
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/BigData.2018.8622380	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Huang Xuping	4．巻 -
2．論文標題 Mechanism and Implementation of Watermarked Sample Scanning Method for Speech Data Tampering Detection	5．発行年 2018年
3．雑誌名 Proc. of the 2nd International Workshop on Multimedia Privacy and Security in ACM CCS 2018	6．最初と最後の頁 54-60
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3267357.3267371	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 NAKAO Koji、YOSHIOKA Katsunari、SASAKI Takayuki、TANABE Rui、HUANG Xuping、TAKAHASHI Takeshi、FUJITA Akira、TAKEUCHI Jun'ichi、MURATA Noboru、SHIKATA Junji、IWAMOTO Kazuki、TAKADA Kazuki、ISHIDA Yuki、TAKEUCHI Masaru、YANAI Naoto	4．巻 E106.D
2．論文標題 Mitigate: Toward Comprehensive Research and Development for Analyzing and Combating IoT Malware	5．発行年 2023年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 1302-1315
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2022ici0001	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Huang Xuping、Ito Akinori	4．巻 14
2．論文標題 Imperceptible and Reversible Acoustic Watermarking Based on Modified Integer Discrete Cosine Transform Coefficient Expansion	5．発行年 2024年
3．雑誌名 Applied Sciences	6．最初と最後の頁 2757～2757
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/app14072757	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 黄 緒平 ， 望月俊輔 ， 藤田 彬 ， 吉岡克成	4．巻 2023-CSEC-100
2．論文標題 ISPの規模を考慮したマルウェア感染ユーザへの注意喚起シミュレーション	5．発行年 2023年
3．雑誌名 情報処理学会研究報告	6．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計5件（うち招待講演　0件／うち国際学会　3件）

1．発表者名 Xuping Huang, Shunsuke Mochizuki and Katsunari Yoshioka
2．発表標題 Towards Estimating Radio Resources Wasted by IoT Botnet Attacks
3．学会等名 The 16th International Workshop on Security (IWSEC 2021)（国際学会）
4．発表年 2021年

1．発表者名 Xuping Huang, Ryota Kawashima
2．発表標題 Privacy preserving using spectral differential privacy for noise suppression
3．学会等名 The 3rd International Conference on Information Science and Systems (ICISS2020)（国際学会）
4．発表年 2020年

1．発表者名 Xuping Huang
2．発表標題 Protect Your Voiceprint From Identity Theft: Fast Acoustic Digital Watermarking Against Spoofing
3．学会等名 28th USENIX security symposium（国際学会）
4．発表年 2019年

１．発表者名 Xuping Huang
２．発表標題 Voice Activity Detection Based Audio Information Hiding for Speech Sharing
３．学会等名 The 22nd Information-Based Induction Sciences Workshop (IBIS)
４．発表年 2019年

１．発表者名 黄　緒平，菊池浩明
２．発表標題 音声電子透かし技術を用いた高精度な改ざん検出及び特定手法
３．学会等名 情報処理学会コンピュータセキュリティシンポジウム(CSS 2018，ポスター発表)
４．発表年 2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関