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

平成　３０　年　　６　月　２０　日現在

機関番号：　６２６１５
研究種目：　基盤研究(A)（一般）
研究期間：　2015～2017
課題番号：　１５Ｈ０１６８６

研究課題名（和文）個人の意思反映となりすまし検知を実現するマルチメディア保護活用基盤

研究課題名（英文）Platform for multimedia data protection and practical use based on user preferences against spoofing attacks in biometric information

研究代表者

越前　功（Echizen, Isao）

国立情報学研究所・情報社会相関研究系・教授

研究者番号：３０４６２１８８

交付決定額（研究期間全体）：（直接経費）　　32,500,000円

研究成果の概要（和文）：カメラやマイクロフォンなどのセンサの普及により，現実世界で取得した顔，音声，身体情報をバーチャル世界で無秩序に共有するプライバシー侵害が懸念されている．また，マルチメディア情報処理技術の進展により，バーチャル世界において，現実世界の任意の人間への「なりすまし」が可能になりつつある．本研究では，現実世界とバーチャル世界の境界で生じるこれらのプライバシーやセキュリティ問題を克服するために，個人の意思を反映したプライバシーコントロールおよび生体特徴を用いた「なりすまし」検知を実現するマルチメディア保護活用基盤を確立する．

研究成果の概要（英文）：Growing popularity of mobile devices equipped with features such as cameras and microphones has given rise to issues whereby biometric information in physical world such as face, speech, and gait can be exposed with ease.
Moreover advances in multimedia information processing have made it possible for computers to generate realistic multimedia contents that are very difficult to distinguish from non-computer generated contents, which leads to spoofing attacks with biometric information collected. This research is aim to establish a platform for multimedia data protection and practical use based on user preferences against spoofing attacks with biometric information.

研究分野：　情報学

キーワード：　コンテンツ流通・管理　プライバシー　セキュリティ

１．研究開始当初の背景

１．１．背景

Cyber-Physical Systems の進展により，現実世界の様々な情報をバーチャル世界に収集して分析することで，生活のあらゆる時間・空間で有益なサービスが受けられるようになった．一方で，カメラやマイクロフォンを内蔵した携帯端末の急速な普及により，人間という知的センサによって，現実世界で取得した画像，映像，音響信号などのマルチメディア情報をバーチャル世界で無秩序に共有・収集することによるプライバシー侵害が懸念されている．米国家安全保障局(NSA)による顔画像の大量収集や，Facebook によるスマートフォンを経由した周辺音の収集・解析サービスなど，現実世界の人間の意思とは無関係にセンシティブな情報が第三者により収集・利用されており，深刻な社会問題になっている．

さらに，画像，映像，音響信号処理などのマルチメディア情報処理技術の進展により，バーチャル世界において，現実世界の任意の人間への「なりすまし」が可能になりつつある．顔の特徴抽出を用いて他人の顔にリアルタイムに変装するスマートフォン上のアプリケーションや，音声合成を用いた他人の声の生成技術が公開されており，バーチャル世界における不正者の「なりすまし」が詐欺や詐称といった深刻なセキュリティ問題を引き起こす可能性がある．

このような，現実世界とバーチャル世界との境界におけるプライバシーやセキュリティ問題を解決するための本質的な対策が必要である．具体的には，現実世界で取得した顔，音声，身体などのマルチメディア情報を，現実世界由来の情報であることを保証しながら，現実世界の人間の意思に基づいて適切に保護・活用する技術群の確立が急務である．

１．２．国内・国外の研究動向

マルチメディア情報のプライバシー保護技術の従来研究は，Video surveillance systems を対象として 2005 年頃から多数の研究がなされ，マルチメディア関連の著名な国際会議（ACMMM，ICME，ICASSP など）においても多くの研究発表がある．これまでに顔などのセンシティブな部位のマスク処理や，特定の場所の音声のみを再生する Video surveillance systems が開発されてきた．

マルチメディア情報の「なりすまし」に関わるセキュリティ問題への対策技術は，指紋認証や虹彩認証などの生体認証機器を対象として，2006 年頃から ICIP や CVPR などで画像分野を中心に多数の研究発表がある．他人の指紋画像や虹彩画像を不正に取得した上で人工指や人工眼として作成し，認証を成功させるといった「なりすまし」問題に対して，指内部の脈拍や，光に対する瞳孔の収縮を検知する機能を生体認証器に組み込むことで認証の対象が生体であることを検知する生体検知手法 (Biometric liveness detection)が提案されてきた．

１．３．研究の位置づけ

上述した従来研究は，Video surveillance systems や指紋認証器，虹彩認証器などのクローズドな環境における特定のサービスやセンサを対象とするに留まっており，SNS や，携帯端末のイメージセンサやマイクロフォンなど，オープンな環境において不特定多数の人間が関わるサービスやセンサ群を対象としたものではない．本研究では，このようなオープンな環境において，現実世界とバーチャル世界の境界で生じるマルチメディア情報のプライバシーやセキュリティ問題を解決する技術群を確立することを目的とする．

２．研究の目的

本研究では，現実世界からセンシングされた画像，映像，音声などのマルチメディア情報を，現実世界由来の情報であることを保証しながら，センシングされた人間の意図に基づいて情報を保護・活用する技術として実現する．期間内の研究目的は以下の 3 つである．

[目的 1] 現実世界の人間の意思に基づいたマルチメディア情報の保護・活用：現実世界の人間の意思に基づいて，自身の特定に結びつくマルチメディア情報の流通を保護または活用する技術群を確立する．

[目的 2] バーチャル世界におけるマルチメディア情報の「なりすまし」検知：バーチャル世界において，現実世界の人物への「なりすまし」を検知する手法を確立する．

[目的 3] 個人の意思反映となりすまし検知を実現するマルチメディア保護活用基盤の構築：[目的 1]および[目的 2]で取り組んだ研究成果を統合したマルチメディア保護活用基盤を構築するとともに，実証実験を実施する．

３．研究の方法

２章で述べた 3 つの目的における課題は以下の通りである．

[目的 1] 現実世界の人間の意思に基づいたマルチメディア情報の保護・活用では，[課題 1-1]人間とアルゴリズムの認識の差異に基づくバーチャル世界における個人識別妨害，および，[課題 1-2]ポリシハイディング：ポリシ着用による柔軟なプライバシーコントロールに取り組む．[課題 1-1]では，人間の表情認知や発話内容に影響を与えずに，顔認識や話者認識の精度を著しく低下または向上させる個人識別妨害／特徴強調の手法を検討する．[課題 1-2]では，サービス毎の個人識別の

可否をプライバシーポリシとして定義し，当該ポリシ情報を情報ハイディングにより，[課題 1-1]で検討した顔面への貼付領域や妨害音・強調音に埋め込み・抽出するポリシハイディング手法を検討する．

[目的 2] バーチャル世界におけるマルチメディア情報の「なりすまし」検知では，[課題 2-1]バーチャル世界で再現困難な顔，声，身体の生体特徴の解明，および，[課題 2-2]生体検知による現実世界データの真正性検証に取り組む．[課題 2-1]では，顔（目・口元の自然な変化），声（呼気によるポップノイズ），身体（各部位の姿勢的調和，運動の滑らかさ）の生体特徴を分析し，バーチャル世界における「なりすまし」が困難な生体特徴量を定義する．[課題 2-2]では，[課題 2-1]で検討した生体特徴を用いてマルチメディア情報の「なりすまし」を検知する手法を検討する．

[目的 3] 個人の意思反映となりすまし検知を実現するマルチメディア保護活用基盤の構築では，[課題 3-1]顔，声，身体情報の匿名化とエンハンスメントの基本検討，[課題 3-2]送り手と受け手の意思を反映したマルチメディア情報の保護・活用手法の検討，[課題 3-3]マルチメディア保護活用基盤の構築・実証実験に取り組む．

４．研究成果

平成 27 年度は，[目的 1]現実世界の人間の意思に基づいたマルチメディア情報の保護・活用の 2 つの課題，[課題 1-1]人間とアルゴリズムの認識の差異に基づくバーチャル世界における個人識別妨害および[課題 1-2]ポリシハイディング：ポリシ着用による柔軟なプライバシーコントロールに取り組んだ．

[課題 1-1]では，人間の表情認知や発話内容に影響を与えずに，バーチャル世界における顔認識や話者認識の精度を著しく低下させる個人識別妨害手法を検討した．顔認識の精度を低下させる妨害手法については，顔面への可視光反射素材の貼付領域の検討，および貼付する眼鏡状のフレーム角度の検討を行い，基本方式を確立したが，屋外で予備評価を行ったところ，外光の顔面への写りこみや屋外の光量が顔認識の精度に影響することが判明したため，基本方式の実装には予定より多くの工数を必要とした．話者認識の精度を低下させる妨害手法については，音声の持つ個人性に着目し，人間の会話を阻害せずに音声の持つ個人性のみを隠す音を発生させることで話者認識の精度を著しく低下させる手法を確立し，基本評価を行った．

[課題 1-2]では，サービスやコミュニティにおける個人識別の可否をプライバシーポリシとして定義し，当該ポリシ情報を現実空間において人間が着用することで，サイバー空間における個人識別情報の流通を制御する手法を検討した．具体的には，プライバシーポリシとして定義可能なペイロードの定義を行うとともに，着用物からも安定して情報を抽出可能な方式の検討および基本実装を行った．

平成 28 年度には，[目的 2]バーチャル世界におけるマルチメディア情報の「なりすまし」検知の 2 つの課題，[課題 2-1]バーチャル世界で再現困難な顔，声，身体の生体特徴の解明，および[課題 2-2]生体検知による現実世界データの真正性検証に取り組んだ．

[課題 2-1]では，人間の顔と声に着目し，「なりすまし」時に用いられる顔の特徴模倣や音声合成では再現困難な顔と声の生体特徴を分析した．具体的には，カメラやマイクロフォンなどのセンサを介して取得された顔と声の情報と，特徴模倣や音声合成により生成された顔と声の情報を比較し，かつ，生体構造（目・口元の自然な変化，呼気・吸気等）との関連を分析した．その結果，顔面の輪郭の複雑さと発声時の空気流（ポップノイズ）の有無をバーチャル世界における「なりすまし」検知に用いることとした．

[課題 2-2]では，[課題 2-1]で検討した「なりすまし」検知の判断基準に基づいて不正者によるバーチャル世界の「なりすまし」を検知する手法を検討し，人間を含む現実世界由来のマルチメディア情報を正しく選別する基本手法を確立した．検討内容を現実世界データの真正性検証アルゴリズムとして実装し，検知精度の評価を行った．

平成 27 年度は個人識別妨害手法の実装・評価が予定より多くの工数を必要としたため，ポリシハイディングの実装および，なりすまし困難な生体特徴の基礎検討の検討に遅延が生じたが，H27 年度中に評価実験体制が整ったため，H28 年度には研究計画の遅延が解消された．

平成 29 年度は，[目的 3]個人の意思反映となりすまし検知を実現するマルチメディア保護活用基盤の構築の３つの課題，[課題 3-1]顔，声，身体情報の匿名化とエンハンスメントの基本検討，[課題 3-2]送り手と受け手の意思を反映したマルチメディア情報の保護・活用手法の検討，および[課題 3-3]マルチメディア保護活用基盤の構築・実証実験に取り組んだ．

[課題 3-1]では，歩容から個人が許可なく特定されてしまうことを防ぐため，オートエンコーダ型のニューラルネットワークにより歩容を匿名化する新たな技術を提案した．本発表は高く評価され，WIFS2017 で Best paper award を受賞した．

[課題 3-2]では，CG 画像と自然な画像を自動で識別するニューラルネットワークを提案し，その有効性も示し WIFS2017 で発表を行った．さらに，コンピュータにより生成されたテキストと人間が作成したテキストを識別する手法を提案し，PACLING2017 および APSIPA ASC 2017 で発表を行った．

[課題 3-3]では，2015 年に開催した話者照

合システムの生体検知精度を競った ASVSpoof2015 を詳細に分析し，また，その後発表された生体検知技術も含め，声の詐称検出がどこまで向上しているかをジャーナル論文としてまとめることも行い，Impact factor が 5.301 と非常に高い The Journal of Selected Topics in Signal Processing (J-STSP)に採択された．また，被写体が属するコミュニティ内外におけるプライバシーポリシを埋め込んだタグ：PrivacyTag を用いて，コミュニティ内外で当該人物の顔領域を適応的に保護する手法を検討・評価した．本発表は高く評価され，IFIP I3E2017 で Best paper award を受賞した．

５．主な発表論文等

〔雑誌論文〕（計 11 件）
（研究代表者、研究分担者及び連携研究者には下線）

①Wang Xin，Takaki Shinji，Yamagishi Junichi，“Investigating very deep highway networks for parametric speech synthesis” Speech Communication，Vol.96，pp.1-9，February 2018【査読有り】

②Wu Zhizheng，Yamagishi Junichi、Kinnunen Tomi、Hanilci Cemal、Sahidullah Mohammed、Sizov Aleksandr、Evans Nicholas、Todisco Massimiliano、Delgado Hector，“ASVspoof: The Automatic Speaker Verification Spoofing and Countermeasures Challenge” IEEE Journal of Selected Topics in Signal Processing, Volume: 11,pp. 588-604, June 2017【査読有り】

③Yamagishi Junichi，Kinnunen Tomi H. , Evans Nicholas, Leon Phillip De, Trancoso Isabel，“Introduction to the Issue on Spoofing and Countermeasures for Automatic Speaker Verification” IEEE Journal of Selected Topics in Signal Processing，Vol.11，pp. 585 – 587，June 2017【査読有り】

④X. Huang，N. Ono，A. Nishimura，I. Echizen，“Reversible Audio Information Hiding for Tampering Detection and Localization Using SampleScanning Method” Journal of Information Processing (JIP), vol. 58(7)，pp. 469 – 476，July 2017【査読有り】

⑤T. Truong，T. Tran，D. Duong，and I. Echizen，“Provable identity based user authentication scheme on ECC in multi-serverenvironment” Wireless Personal Communications，vol. 92，pp.2785-2801，Springer，August 2017【査読有り】

⑥Zhizheng Wu, Junichi Yamagishi, Tomi Kinnunen，Cemal Hanilci，Md Sahidullah, Aleksandr Sizov，Nicholas Evans，Massimiliano, Todisco, Hector Delgado，“ASVspoof: the Automatic Speaker Verification Spoofing and Countermeasures Challenge” IEEE Journal of Selected Topics in Signal Processing，Volume：11，Issue：4，pp. 588-604，June 2017【査読有り】

⑦Zhizheng Wu, Phillip L. De Leon, Cenk Demiroglu，Ali Khodabakhsh, Simon King，Zhen-Hua Ling, Daisuke Saito, Bryan Stewart，Tomoki Toda，Mirjam Wester，and Junichi Yamagishi，“Anti-Spoofing for Text-Independent Speaker Verification： An Initial Database，Comparison of Countermeasures, and Human Performance” IEEE/ACM Transactions on Audio，Speech，and Language Processing，Volume: 24, Issue: 4, pp. 768 – 783，April 2016【査読有り】

〔学会発表〕（計 50 件）

①生野祐輝，中村和晃，新田直子，馬場口登，「歩容シルエットクローン識別のための輪特徴量の検討」第 20 回画像の認識・理解シンポジウム（MIRU 2017），August 2017

②廣瀬雄基，中村和晃，新田直子，馬場口登，「映像中の歩容情報保護を目的とした匿名歩容シルエットの生成」2018 年電子情報通信学会総合大会，March 2018

③Tomi Kinnunen，Md Sahidullah，Hector Delgado，Massimiliano Todisco，Nicholas Evans，Junichi Yamagishi，Kong Aik Lee，“The ASVspoof 2017 Challenge: Assessing the Limits of Replay Spoofing Attack Detection” Proc. Interspeech 2017，August 2017

④T.Ngoc-Dung Tieu，Huy H. Nguyen，Hoang-Quoc Nguyen-Son，Junichi Yamagishi，Isao Echizen，“An Approach for Gait Anonymization Using Deep Learning” Proc. 9th IEEE International Workshop on Information Forensics and Security (WIFS)，December 2017 **[Best Paper Award]**

⑤Fuming Fang, Junichi Yamagishi, Isao Echizen, Jaime Lorenzo-Trueba, "HIGH-QUALITY NONPARALLEL VOICE CONVERSION BASED ON CYCLE-CONSISTENT ADVERSARIAL NETWORK" Proc. ICASSP 2018, April 2018

⑥Jaime Lorenzo-Trueba, Junichi Yamagishi, Tomoki Toda, Daisuke Saito, Fernando Villavicencio, Tomi Kinnunen and Zhenhua Ling, "The Voice Conversion Challenge 2018: Promoting Development of Parallel and Nonparallel Methods" Proc. Odyssey 2018, June 2018

⑦Jaime Lorenzo-Trueba, Fuming Fang, Xin Wang, Isao Echizen, Junichi Yamagishi and Tomi Kinnunen, "Can we steal your vocal identity from the Internet?: Initial investigation of cloning Obama's voice using GAN, WaveNet and low-quality found data" Proc. Odyssey 2018, June 2018

⑧H´ector Delgado, Massimiliano Todisco, Md Sahidullah, Nicholas Evans, Tomi Kinnunen, Kong Aik Lee and Junichi Yamagishi, "ASVspoof 2017 Version 2.0: meta-data analysis and baseline enhancements" Proc. Odyssey 2018, June 2018

⑨H.-Q. Nguyen-Son and I. Echizen, "Detecting Computer-Generated Text Using Fluency and Noise Features," Proc. of the 2017 Conference of the Pacific Association for Computational Linguistics (Pacling2017), August 2017

⑩S. Machida, A. Dabrowski, E. Weippl, and Isao Echizen, "PrivacyTag: A Community-based Method for Protecting Privacy of Photographed Subjects in Online Social Networks," Proc. of , The 16th IFIP Conference on e-Business, e-Services and e-Society (I3E2017) , November 2017**[Best Paper Award]**

⑪N. Rahmouni, V. Nozick, J. Yamagishi, and I. Echizen, "Distinguishing Computer Graphics from Natural Images Using Convolution Neural Networks," Proc of the 9th IEEE International Workshop on Information Forensics and Security 2017 (WIFS2017), December 2017

〔図書〕（計　0　件）

〔産業財産権〕

○出願状況（計　1　件）

名称：生体特徴盗撮防止装着具及び盗撮防止方法
発明者：越前 功, 大金 建夫
権利者：同上
種類：特許
番号：2017-051969
出願年月日：2017-03-16
国内外の別：国内

○取得状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
国立情報学研究所ニュースリリース(2017 年 3 月 17 日)

６．研究組織
(1)研究代表者
越前　功（ECHIZEN,Isao）
国立情報学研究所, 情報社会相関研究系, 教授
研究者番号：30462188

(2)研究分担者
馬場口　登（BABAGUCHI,Noboru）
大阪大学, 工学研究科, 教授
研究者番号： 30156541

(2)研究分担者
山岸　順一（YAMAGISHI,Junichi）
国立情報学研究所, コンテンツ科学研究系, 准教授
研究者番号： 70709352

(3)連携研究者
該当なし

(4)研究協力者
該当なし