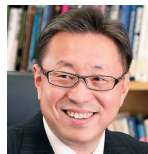


内心プライバシーの漏洩を防ぐ 画像認識フレームワーク

工学研究科 電気電子情報通信工学専攻

教授 馬場 登 助教 中村 和晃



特徴・独自性

AI技術の進展により、利用者から送信された写真に対し画像認識を実行し結果を返送するクラウドサービスが登場しつつある(図1)。しかし、このサービスでは、サービス提供側が画像認識の結果を全て把握できるため、人々が気軽に撮影した様々な写真に対する画像認識結果を蓄積し統計解析を行うことにより、個人の趣味や嗜好といった「内心プライバシー」がサービス提供側に漏洩する危険がある。例えば、写真中の建物の名称や品物の銘柄がAIにより認識・解析されれば、写真の持ち主がどの時間どの場所におり、どのようなモノを好む傾向がある、といった情報が詳らかとなる(図2)。本研究では、この問題を世界で初めて明示的に指摘し、その解決策として新たな画像認識フレームワークを提案した。送信する写真に予め独自の画像変換処理を施すことによりサービス提供側に認識結果を特定させず、その候補を絞ることしかできないようにする一方、利用者側では返送された候補を変換前の元の写真と照合することにより正しい認識結果が得られる(図3)。

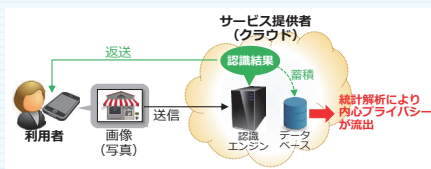


図1 クラウド上の画像認識サービス



図2 画像認識に伴う内心プライバシー漏洩の例

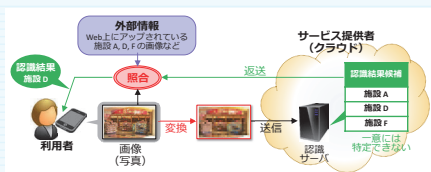


図3 提案フレームワークの概要

研究の先に見据えるビジョン

携帯端末の進化とAI技術の進展により、類似のクラウドサービスは今後も次々登場すると予想される。本研究は、それらのサービスの安心安全な運用と利活用に資するほか、サービス開発者がプライバシーやセキュリティ上の懸念を常に意識する機運の醸成にもつながると期待される。



特 許

論 文

Kazuaki Nakamura, Naoko Nitta, and Noboru Babaguchi: "Encryption-Free Framework of Privacy-Preserving Image Recognition for Photo-Based Information Services," IEEE Transactions on Information Forensics and Security, Vol.14, No.5, pp.1264-1279, 2019.

参考URL

https://resou.osaka-u.ac.jp/ja/research/2018/20181105_2

キーワード 画像認識、プライバシー保護、人工知能、機械学習

研究分野以外の関心分野・テーマ 認知心理、地球環境