プライバシー保護が可能な深層学習方法の開発

安全・安心

情報技術グループ　大平 倫宏
TEL 03-5530-2540

特徴

利用する画像データについて、**プライバシー保護可能な深層学習方法を開発**しました。この技術により、クラウドサーバーなどを利用して、深層学習を行う際にも、従来よりも安全に学習を行うことが可能です。

深層学習を用いた人工知能(AI)の開発は、幅広い分野での利用が行われています。
深層学習のモデルの学習には、数時間から数か月程の非常に長い時間がかかることが多いです。
このため、クラウドサーバーなどに学習用のデータを保存して、サーバー上で学習することが行われています。
しかし、クラウドサーバーなどを利用する際にデータ中にプライバシー情報などが含まれる場合、データの流出などが発生した時に大きな問題となります。

本研究では、データにあらかじめ加工を行うことで、データの流出などが発生した場合でも、元のデータが判別不能な状態で、深層学習を行う方法について研究・開発を行いました。

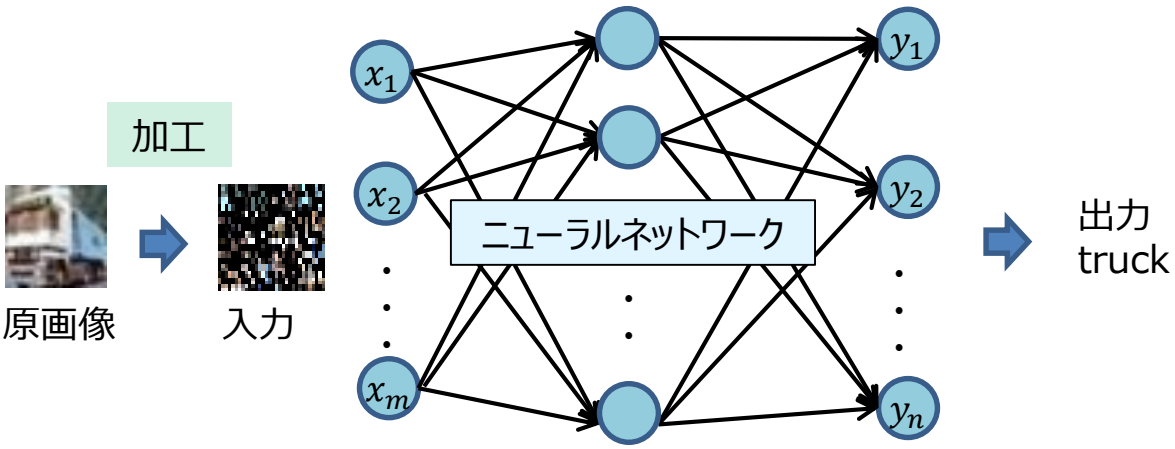

図1 プライバシー保護可能な深層学習

従来技術に比べての優位性

- セキュリティの懸念なく、低コストで深層学習が可能
- プライバシー保護を行った場合でも、認識精度の差が少ない
- 加工時間は、深層学習時間に比べれば微小

今後の展開

- さまざまな画像認識への応用
- 中小企業様などが低コストで人工知能を開発

研究員からのひとこと

この技術で安全・低コストに深層学習が可能です。

人工知能の開発に興味のある企業の皆さまとの共同研究・事業化を目指しています。