



カバードータを自動生成する次世代のセキュリティ技術

概要

○秘密情報を守るために、暗号化技術とステガノグラフィ技術が利用できます。前者は秘密情報を誰も読めないようにコーディングする技術で、後者は秘密情報を「自然な」カバードータに埋め込み、その存在自体を誰もわからないようにする技術です。

○秘密データの存在を隠すためには、自然なカバードータをたくさん作成しないといけません。同じカバードータで異なる秘密を隠すと、秘密情報の存在が第三者にバレやすくなるためです。

○本技術は、GANつまり敵対生成ネットワークをステガノグラフィに利用する方法を提案します。主なポイントは、カバードータ（画像）の生成、カバードータの自然さの検証、ステゴデータが味方によって送られていることの検証などがあります。

実用化の可能性

○近年、生成AIが益々強力なものになっており、本技術は間違いなく実用できます。ただし、秘密情報を守るためには、クラウド型AIではなく、ローカルな専用AIを利用したほうが良い。また、訓練データ、使用時に生成されたデータ、AIモデルなどの厳重管理は課題であり、関連業者との共同研究によって解決したい。

UBICからのメッセージ

GAN(Generative Adversarial Networks)による画像生成によって、秘密情報を埋め込む画像を生成するだけでなく、カバードータ自体の検証や送信元の検証も含まれる技術です。近年の生成AIなどの高度化によって、より複雑かつ他者からの復元不可能な暗号化技術が求められ、セキュリティに関わる広い分野での利活用が期待できます。

研究概要図

