個人研究

スマート社会

人工知能の情報セキュリティ技術への応用

16 平和と公正をすべての人に

人工知能(AI)により、従来技術では検出できなかった攻撃が検知できるようになったり、人間に解析できないものが解析できるようになってきました。一方、誤った評価や、AIによる判断の過信という弊害も起きており、問題解決と問題提起の両面で研究を行っています。

KEYWORDS 情報セキュリティ

RESEARCHER

コンピュータサイエンス学部 准教授　宇田隆哉

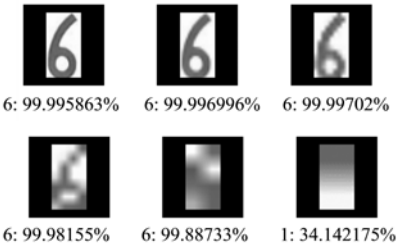
https://www.teu.ac.jp/info/lab/project/com/dep.html?id=121

主な学会発表・論文・著書・社会活動

[1] 鈴木友哉, 宇田隆哉, CNNを用いた予測に有効なナンバープレート写真用トレーニングデータの検討, 情報処理学会論文誌, Vol.62, No.2, pp.484-496, 2021.
[2] 白石将貴, 宇田隆哉, 藤川真樹, Kinectを用いた行動座標によるピッキング行為の検知, 情報処理学会論文誌, Vol.61, No.2, pp.486-499, 2020.
[3] K. Kita and R. Uda, Malware Subspecies Detection Method by Suffix Arrays and Machine Learning, In Proc. of the 55th Annual Conference on Information Sciences and Systems (CISS), 2021.

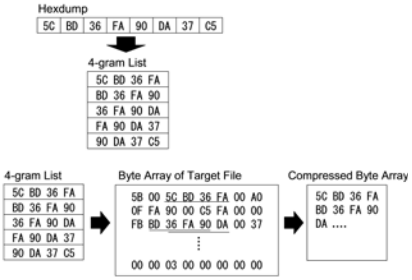
01 AIでナンバープレートを識別する

犯行現場近くの監視カメラに、犯行に使われた自動車が写っていたとしても、ナンバープレートがはっきり写っていなく、人間には読み取ることが難しかったりします。そのような場合でも、人工知能でよく使用されるようになった畳み込みニューラルネットワークを用いて、高い精度で数字の識別を行う研究をしています。



02 AIでマルウェアの亜種を検出する

マルウェア(コンピュータウイルスなどの総称)の中には、パターンマッチングで発見されないように、バイナリパターンを少し変える亜種と呼ばれるものがあります。畳み込みニューラルネットワークを用いて、実際に流行した亜種のマルウェアを見分ける研究を行っています。



東京工科大学　実践研究推進課　https://www.teu.ac.jp/karl/
〒 192-0982　東京都八王子市片倉町 1404-1