研究室 インテリジェントメディア通信研究室 教員 酒澤 茂之

カテゴリー

IT·loT·AI・ロボティクス

ネットワーク、セキュリティ

学習済みディープラーニングモデルの著作権保護

ディープラーニングの応用例

道路交通画像

物体認識

- ・信号機
- ・重
- ・単 ・歩行者
- ・建物
- ・道路標識
- 推論や生成 ・道路状況
- ・自動運転の制御

ディープラーニングの学習コスト

2012年にディープラーニングブームを 巻き起こしたトロント大学のモデル

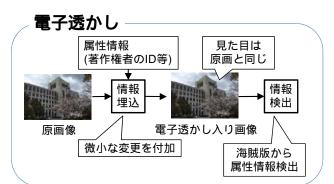
データ量:画像100万枚

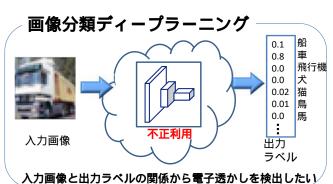
学習時間:2週間

モデルのコピーや 再利用は容易

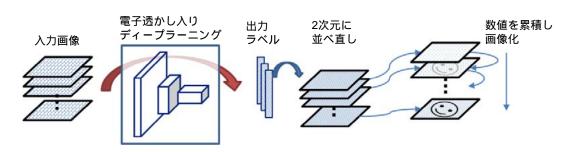


知的財産権の保護 技術が必要





視覚的に復号可能なディープラーニング電子透かし技術



<電子透かし検出用画像>















複数の出力ラベル値を累積

<出力ロゴ> 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.5 0.6 0.5 0.0 0.0 0.5 0.0 0.0 0.5 0.6 0.0 0.0 0.6 0.0 0.0 0.5 0.0 0.0 0.0 0.6 0.0 0.0 0.5 0.0 0.0 0.5 0.0 0.0 0.0 0.6 00 00 05 00 00 06 00 00 00 0.6 0.6 0.6 0.0 0.0 0.6 0.0 0.0 0.0 0.6 0.0

直観的にわかりやすい著作権表示が可能

本来の画像認識タスク(100種類の画像の分類)には、ほとんど影響なし

電子透かし無しでの精度:0.7487 電子透かし有りでの精度:0.7370 本研究の一部はJSPS科研費 JP18K11309の 助成を受けたものです。