SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

車載カメラの車両・人物検出に対する色調改変攻撃とその対策

Color Alteration Attacks on On-Board Camera's Vehicle/Person Detection and Their Countermeasures

上田　晋生*　一ノ瀬　竜矢*　吉田　直樹*　松本　勉*
Shinsei Ueda　Ryuuya Ichinose　Naoki Yoshida　Tsutomu Matsumoto

キーワード 自動運転車，計測セキュリティ，車両検出，人物検出，色調改変攻撃

あらまし

自動運転にはレーダー，LiDAR，カメラなどの多種多様のセンサが取得する周辺環境情報が必要である．車載カメラが取得した画像による車両・人物検出の情報は自動緊急ブレーキや追従走行機能などに用いられており，搭乗者や周囲の安全を確保する上で大いに役立っている．もしも車載カメラの車両・人物検出のセキュリティが損なわれると人命に関わる事故に繋がる恐れがある．周辺環境情報の正しさを担保するために，車載カメラに対してありえる攻撃を把握して対策を講じることが重要である．これまで，車載カメラが取得する画像の色調を意図的に変化させるような細工を路面や路面危機に施すことで，車線検出機能の検出率を低下させる色調改変攻撃[1]が報告がされている．車両・人物検出機能とその前後の処理を含めた一連のプロセスを図１のモデルで表す．まず，環境部の環境から届く光を知覚部の車載カメラがデジタル画像として出力し，処理部がデジタル画像を基に車両・人物検出を行う．その後，制御部では車両・人物検出情報を利用して自動緊急ブレーキや追従走行機能が動作する．このモデルでは環境部から処理部の間に攻撃を受けると後段の処理に影響を及ぼす．すなわち，環境部において図２のようなカラーフィルタや光源，蛍光塗料を利用した色調改変攻撃を受けたとき，知覚部のデジタル画像の色調が変化し，処理部や制御部に影響を与えることが推測される．本報告では，色調改変攻撃が特定のデータセットで学習された YOLOv2 [2] /YOLOv3 [3] 車両検出器や人物検出器の検出率の低下を引き起こすことを示す．また，対策手法として，検出器に色調改変を施した画像データセットで転移学習をさせることで色調改変攻撃に耐性を持たせる手法を検討した．

図１：車両・人物検出機能のプロセスモデル

図２：色調改変攻撃方法の種類

参考文献

[1]宮園史規，吉田直樹，乃万誉也，松本 勉，“車線検出機能に対する色調改変攻撃とその対策” ,SCIS2021,Jan.2021
[2] J. Redmon and A. Farhadi.” Yolo9000: Better, faster, stronger”, In Computer Vision and Pattern Recognition (CVPR), 2017, IEEE Conference on, pages 6517–6525. IEEE, 2017
[3] J. Redmon and A. Farhadi."Yolov3: An incremental improvement." arXiv preprint arXiv:1804.02767 (2018).

本研究の一部は，国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務「AI エッジデバイスの横断的なセキュリティ評価に必要な基盤技術の研究開発」によって実施されたものである．

*横浜国立大学，〒240-8501 横浜市保土ケ谷区常盤台 79-7
Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan