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

人工知能を伴う監視カメラによる全方位からの撮影に対する耐人物検出機能を持つ衣類の作成

Creation of Clothes with Human Detection Resistance against Shooting from All Directions by Surveillance Cameras with Artificial Intelligence

金井 春輝 * 宇田 隆哉 *
Haruki Kanai Ryuya Uda

キーワード Adversarial Patch 人物検出 深層学習 機械学習

あらまし

深層学習による分類は既存技術と比べ非常に高い精度で分類が行える場合があるため非常に注目されている．特に，監視カメラシステムでは画像分類を行う深層学習技術が利用され始めており，簡易的な人物検出を行う製品が個人向けとしても販売されている．このような監視カメラシステムは犯罪の抑止や犯罪の解決に貢献しているといえる．しかし一方で，犯罪などとは無関係の個人が人物検出によってリスト化されてしまうなど，プライバシーを侵害されるリスクが高まっていると考えられる．

深層学習画像分類技術において，利用される CNN(畳み込みニューラルネットワーク) は故意に誤分類させる目的で計算された画像に対して脆弱であることが知られている．これを Adversarial Patch と呼ぶ．本研究では CNN の脆弱性をあえて利用し，着用者のプライバシーを守るために様々な方向から監視カメラシステムに撮影された場合でも人物検出に耐性を持つ衣類を作成することに成功した．

関連研究と提案手法

Thys らは，人物検出器による検出に耐性を持つ Adversarial Patch を生成することに成功した [1]．ただし，彼らの Adversarial Patch は衣類へ応用した際に，シワによって Adversarial Patch が歪むことを考慮していない．

そこで Xu らは，Adversarial Patch の生成過程で Thin Plate Spline マッピングを行い，Adversarial Patch を歪ませた．その結果，衣類のシワによって Adversarial Patch が歪んだ際のロバスト性を高めることに成功した [2]．ただし，彼らの研究は人物がカメラに正対していることを前提としており，側面や背面から撮影されることを想定していない．

そこで本研究では，衣類の着用者がどのような向きでカメラに相対したとしても，有効になる Adversarial Patch が存在するように複数の Adversarial Patch を衣類に応用した．生成過程でデータセットの適切な位置にパッチを適用することで当該位置に適した Adversarial Patch を生成し，布面積の大きなマントの適切な位置に応用した．その結果，様々な方向から監視カメラシステムに撮影された場合でも人物検出に耐性を持つ衣類を作成することに成功した．

参考文献

[1] Thys, S. and Van Ranst, W. and Goedemé, T. ,“Fooling automated surveillance cameras: adversarial patches to attack person detection,” CVPRW 2019 pp.49-55, 2019

[2] Xu, K., Zhang, G., Liu, S., Fan, Q., Sun, M., Chen, H., Chen, P., Wang, Y. and Lin, X. ,“Evading Real-Time Person Detectors by Adversarial T-shirt,” dblp computer science bibliography abs-1910-11099, 2019

* 東京工科大学大学院 バイオ情報メディア研究科 コンピュータサイエンス専攻, 〒 192-0982 東京都八王子市片倉町 1404-1, Computer Science Program, Graduate School of Bionics, Computer and Media Sciences, Tokyo University of Technology, 1404-1 Katakuramachi, Hachioji City, Tokyo 192-0982, JAPAN.