UNIVERSITY OF CENTRAL FLORIDA

CCA: Exploring the Possibility of Contextual Camouflage Attack on Object Detection

Shengnan Hu, Yang Zhang, Sumit Laha, Ankit Sharma and Hassan Foroosh
Department of Computer Science
University of Central Florida
{shengnanhu, yangzhang}@knights.ucf.edu, laha@cs.ucf.edu, ankit.sharma285@knights.ucf.edu, hassan.foroosh@ucf.edu

Background

- Object detection has become a crucial part for many applications, such as autonomous driving, law enforcement and orbital surveillance.

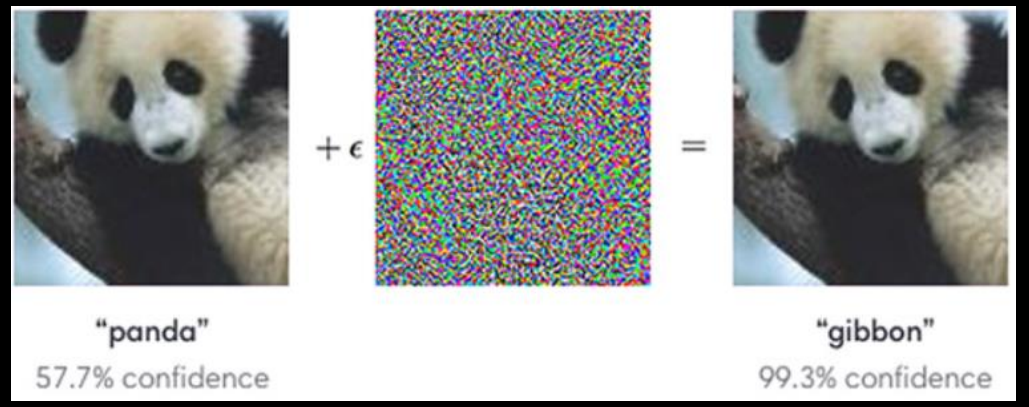


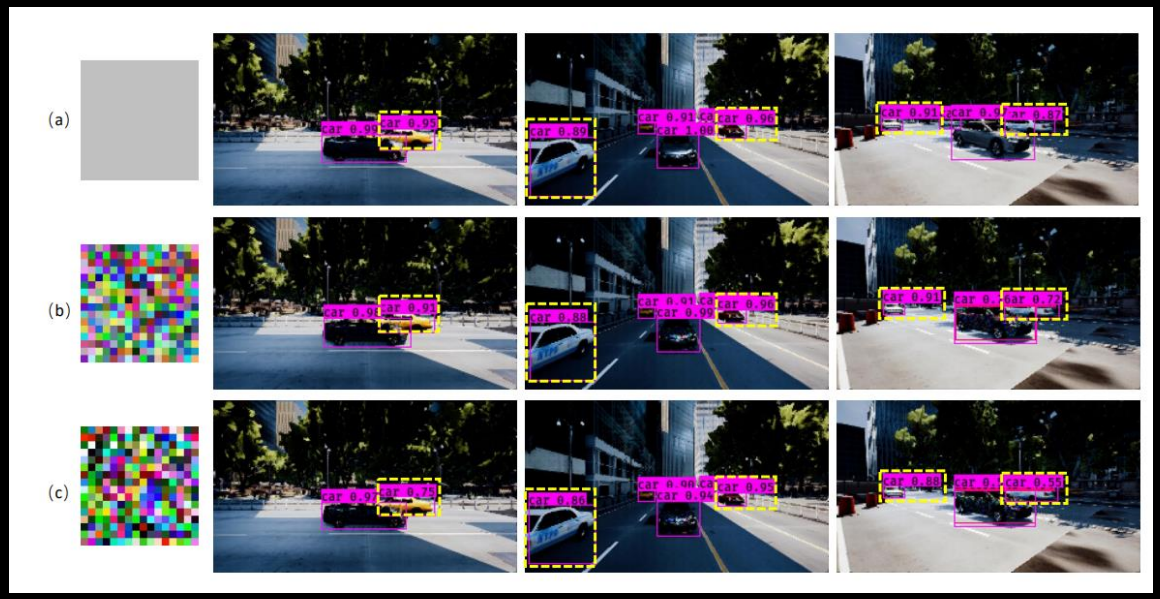
Image: OpenAI

- Adversarial attack—an adversary which can manipulate the CNNs' output by adding imperceptible perturbations to an input image.

Images: Evtimov et al

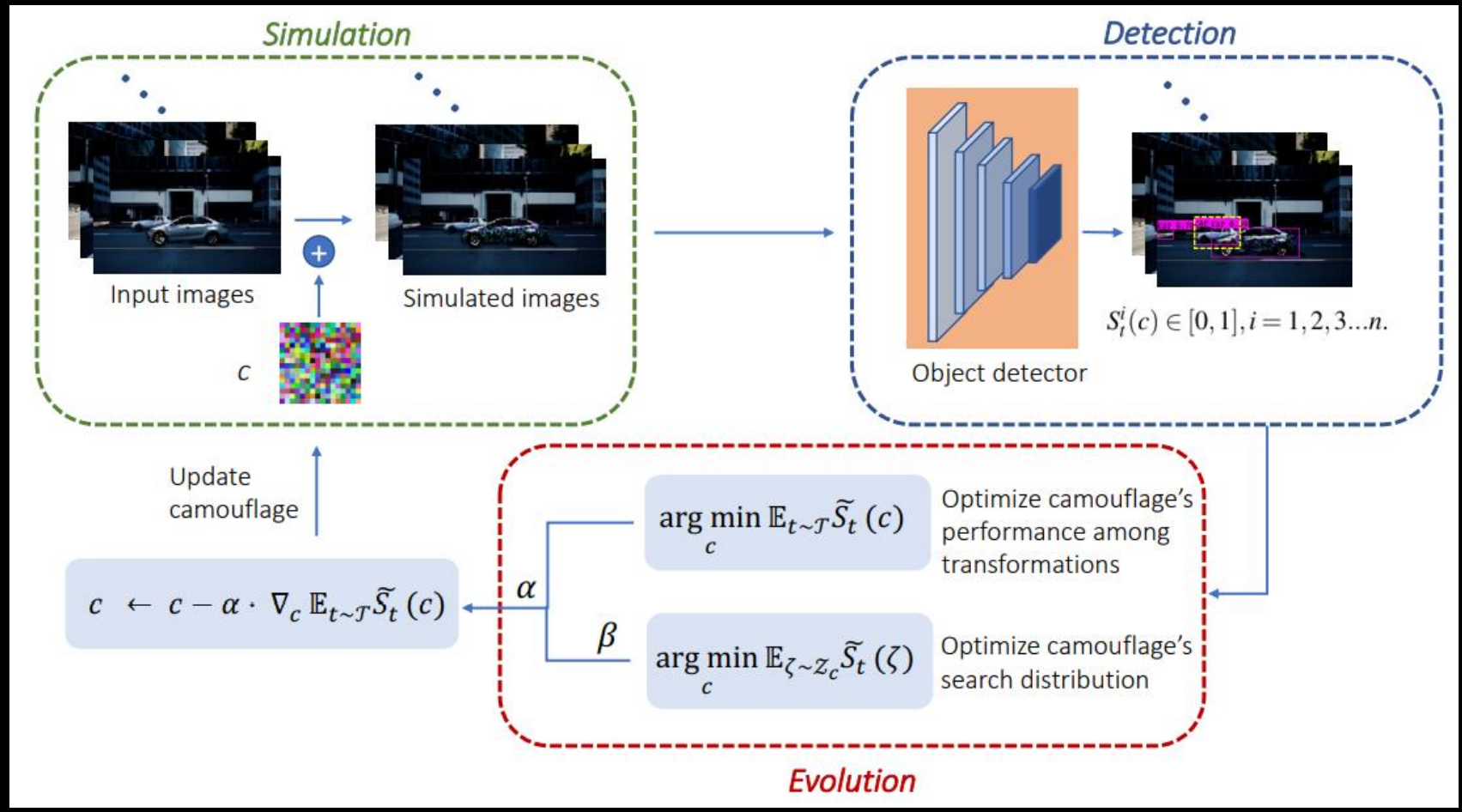
Introduction

- By learning a camouflage on a contextual vehicle, we could attack the detectors' performance on the unpainted vehicles in the same image.
- Proposed a new method that jointly models the transformation distribution and camouflage variations.
- In addition to the contextual adversarial attack, CCA model shows effectiveness on enhancing the performance of object detectors.



YOLOv3 detection on vehicle with silver paint (a), random texture (b) and our learned camouflage (c) in the simulation.

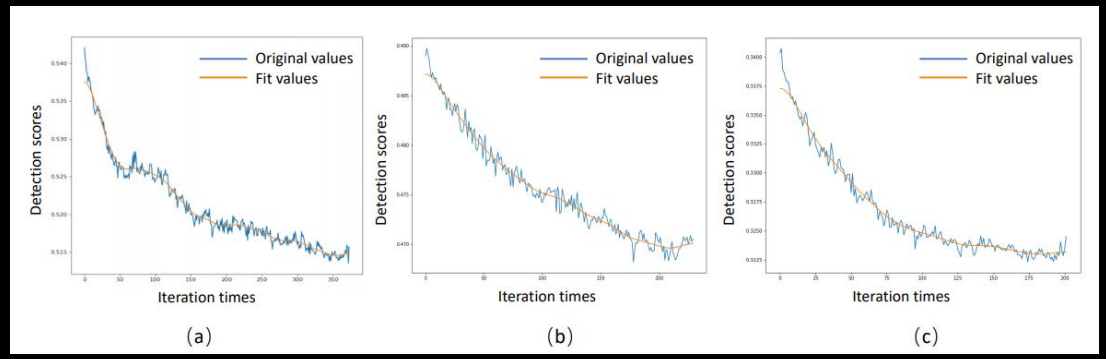
Method



The framework of proposed CCA algorithm.

Results

- Attacking performance of proposed CCA model on object detectors



Training process of our learned camouflage against state-of-the-art object detectors. (a) YOLOv3; (b) MaskRCNN; (c) FCOS.

YOLOv3 detection performance among baseline and CCA:

Camouflages	Training set			Testing set		
	Detection confidence(%)	mIOU(%)	P@0.5(%)	Detection confidence(%)	mIOU(%)	P@0.5(%)
Basic colors	55.87	49.93	65.71	57.10	51.92	63.23
Random camouflage	55.02	48.78	63.70	54.06	48.57	61.77
Ours	**51.35**	**47.25**	**62.35**	**53.25**	**48.15**	**60.48**

MaskRCNN detection performance among baseline and CCA:

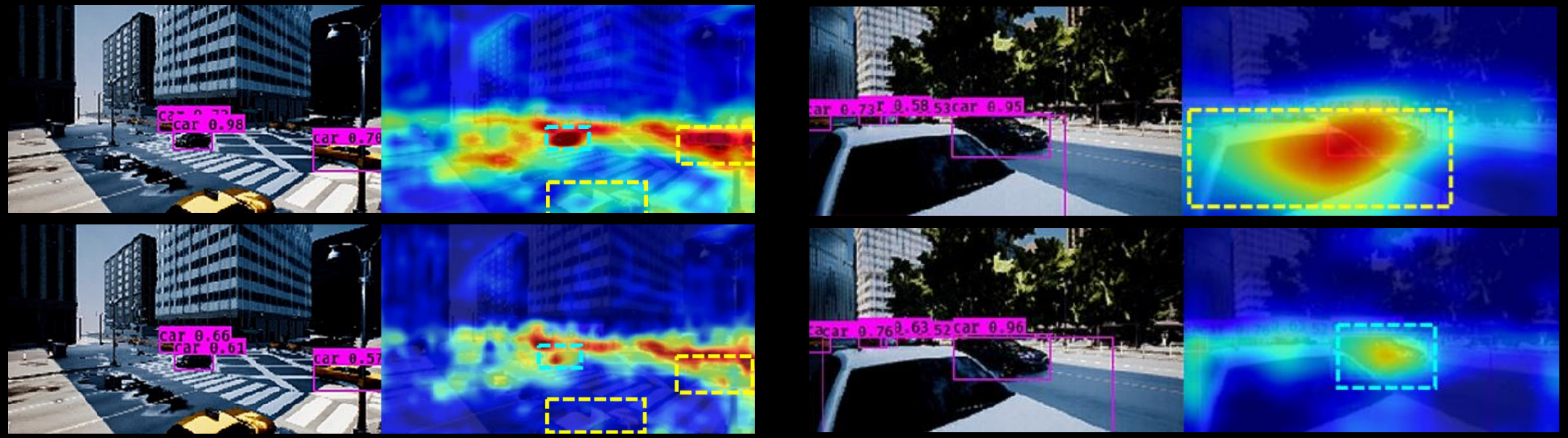
Camouflages	Training set			Testing set		
	Detection confidence(%)	mIOU(%)	P@0.5(%)	Detection confidence(%)	mIOU(%)	P@0.5(%)
Basic colors	48.48	46.61	49.78	48.87	47.54	48.19
Random camouflage	48.90	47.08	49.61	48.79	47.46	47.87
Ours	**46.82**	**45.54**	**47.77**	**47.97**	**46.91**	**46.71**

FCOS detection performance among baseline and CCA:

Camouflages	Training set			Testing set		
	Detection confidence(%)	mIOU(%)	P@0.5(%)	Detection confidence(%)	mIOU(%)	P@0.5(%)
Basic colors	34.44	38.96	46.46	34.02	39.48	46.31
Random camouflage	34.08	38.75	45.78	33.77	39.36	46.39
Ours	**33.02**	**37.81**	**44.83**	**33.60**	**38.53**	**45.42**

Results

- Grad-CAM Results



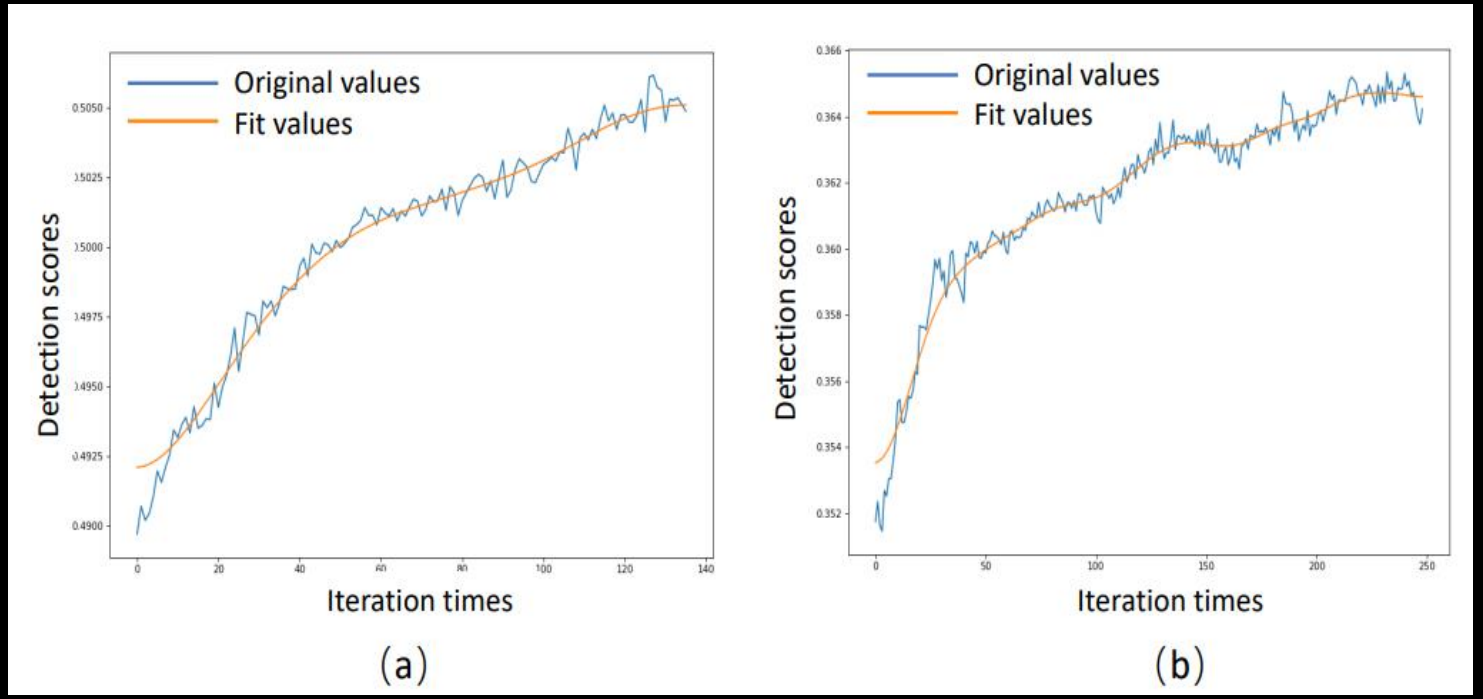
Grad-CAM of YOLOv3 on images with random camouflage (top) and CCA camouflage(bottom).

Results

- Our learned camouflage enhancing state-of-art object detectors

Reset loss function:

$$\arg\min_{c} -\frac{1}{|\mathcal{T}|}\sum_{t\in\mathcal{T}}\widetilde{S}_t(c)$$



Training process of our learned camouflage enhancing (a) MaskRCNN; (b) FCOS.

Conclusion

- We first investigate the problem of learning contextual adversarial object camouflage to attack vehicle detectors.
- We propose an evolutionary based algorithm to learn highly effective camouflages by interacting with a photo-realistic simulation.
- The proposed CCA algorithm not only shows the effectiveness of attacking the state-of-the-art object detectors, but also shows its capability to enhance the detectors.
- The next phase of our work is to generalize the camouflages from simulation to the real world. Both adversarial domain adaptation and domain randomization seem to be promising approaches for this step.

UNIVERSITY OF
CENTRAL FLORIDA

Thanks!