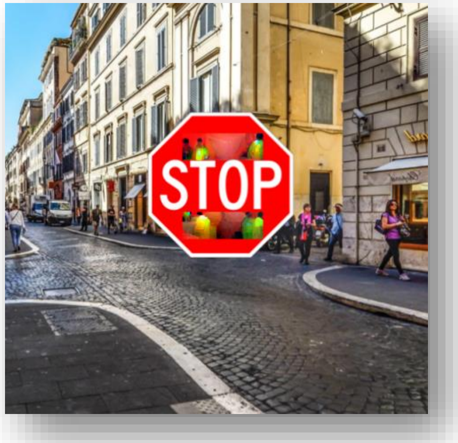
# Adversarial Patch

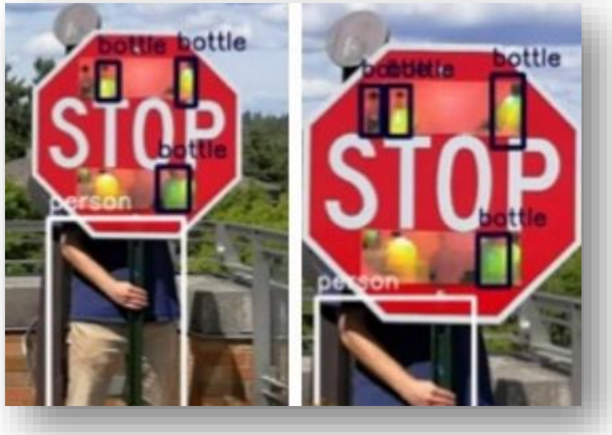
Han Wu

We plan to generate adversarial patches against object detection models in a **simulated environment** by changing the **material** or **texture** of an object, which is a special kind of physical patch.

- Real World

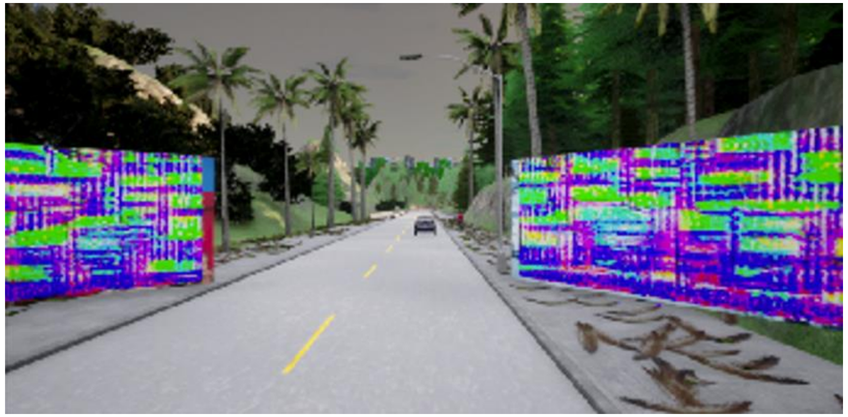


Digital Patch
(directly modify pixel values)

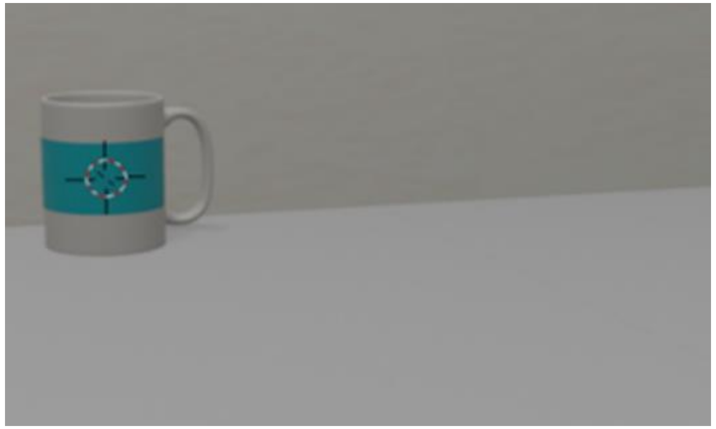


Physical Patch

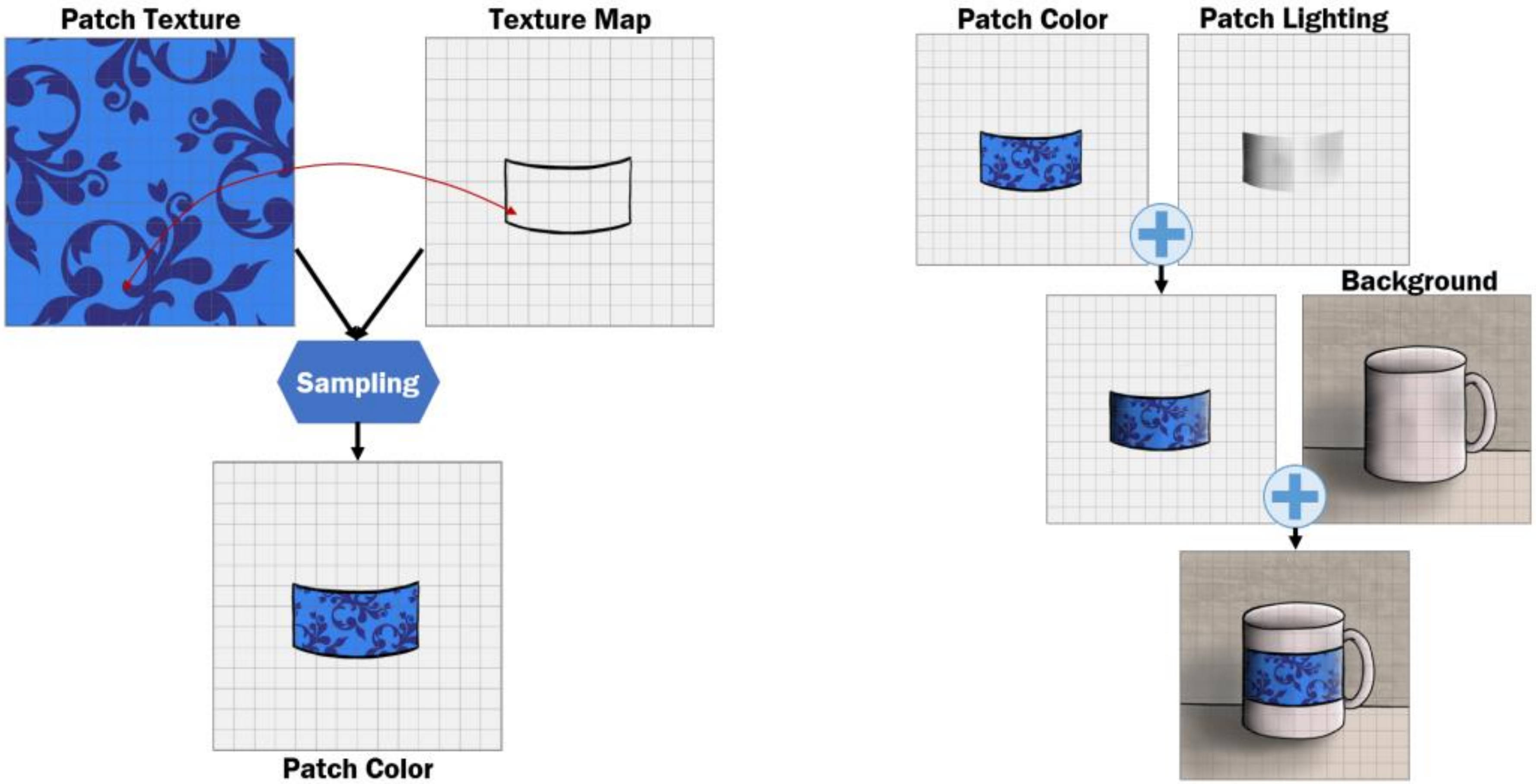
- Simulated Environment



Digital Patch
(directly modify pixel values)



Physical Patch ✓



(a) Sampling the texture

(b) Combining the buffers

Mathov, Yael, Lior Rokach, and Yuval Elovici. "Enhancing real-world adversarial patches through 3D modelling of complex target scenes." *Neurocomputing* 499 (2022): 11-22.