(a) Make Synthetic Adversaries

Generator

Perturb

Adv Patch

Source Class
(Photocopier)

Target
Classifier

Target Class
(Printer)

$\hat{y}$

(b) Find Similar Natural Adversaries

Nat Patches

Adv Patches

Target
Classifier

Nat Latents

Adv Latents

Similarity
Matrix

Selected
Nat Patches