JUNE 6 SAT AM - 597

Generative Adversarial Perturbations with Cross-paradigm Transferability on Localized Crowd Counting

Alabi Mehzabin Anisha; Guangjing Wang; Sriram Chellappan

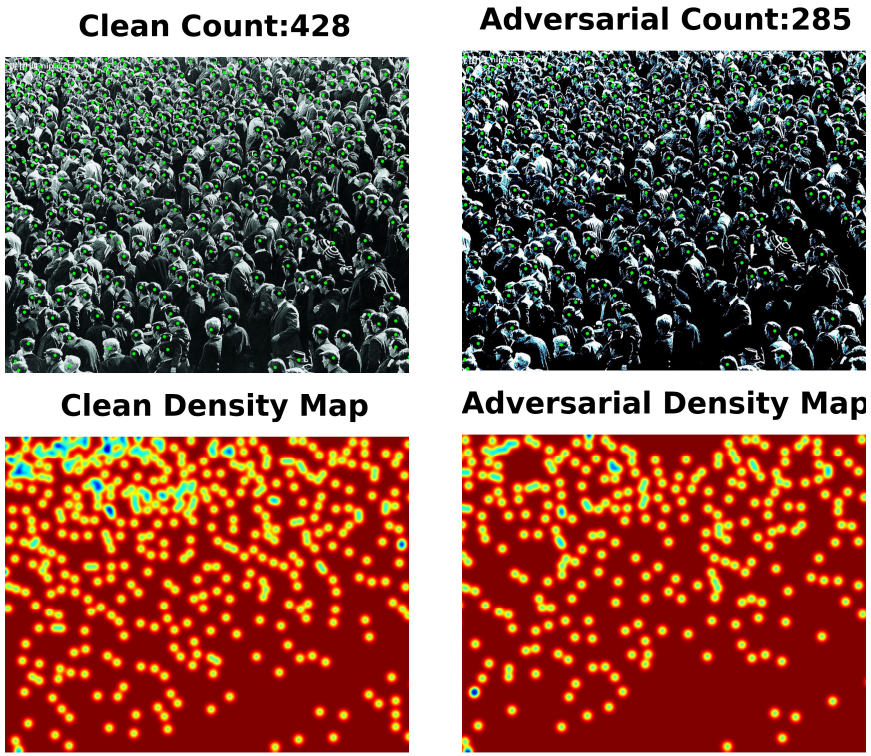
{aanisha, guangjingwang, sriramc} @usf.edu

UNIVERSITY of
SOUTH FLORIDA

Why Evasion matters for Crowd Models?

Crowd Models are

- More complex than Classification tasks
- Lacks inherent robustness
- Deployed in real life
  - Public safety
  - Retail analytics
- Attacks can cause:
  - Undercounting = Safety Risk
  - Overcounting = False Alarm

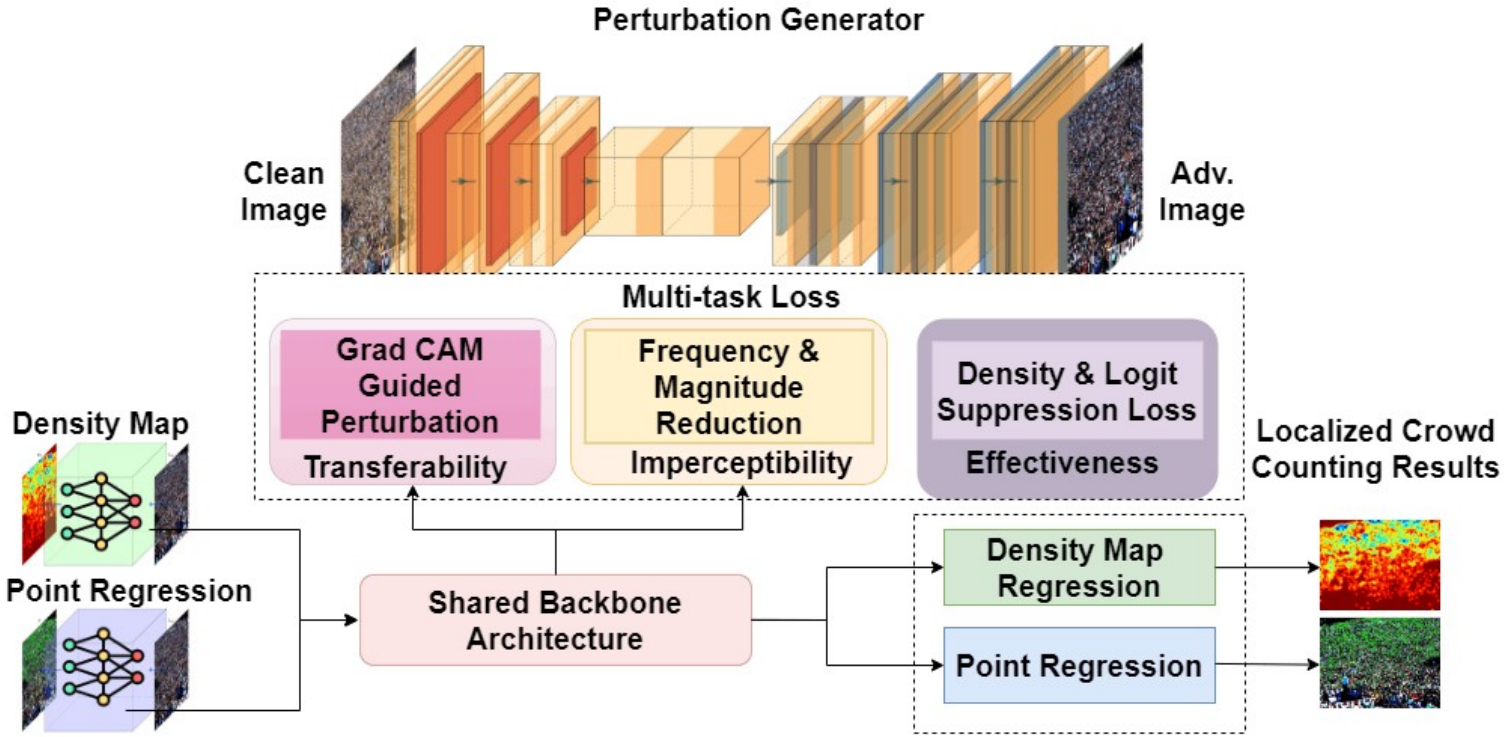


Narrow Scope for Pre-existing Attacks

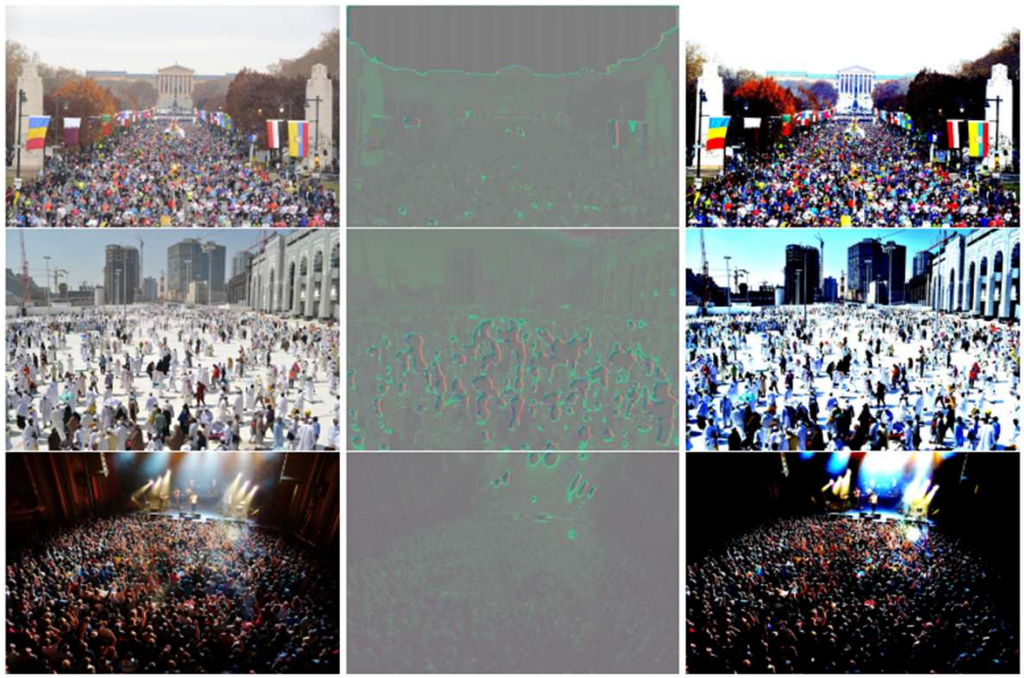
Prior Work	Attack Type	Limitation
PAP (CCS-2022)	Patch-Based	Visible perturbations
APAM (MM- 2021)	Patch-Based	Density-map only
Others	White-box	No transferability study

Q: Can adversarial perturbations transfer across heterogeneous localized crowd counting paradigms – density map and point-regression?

Generator-Based Framework for Cross-Paradigm Transferable Perturbations



Sample Instances of Adversarial Examples

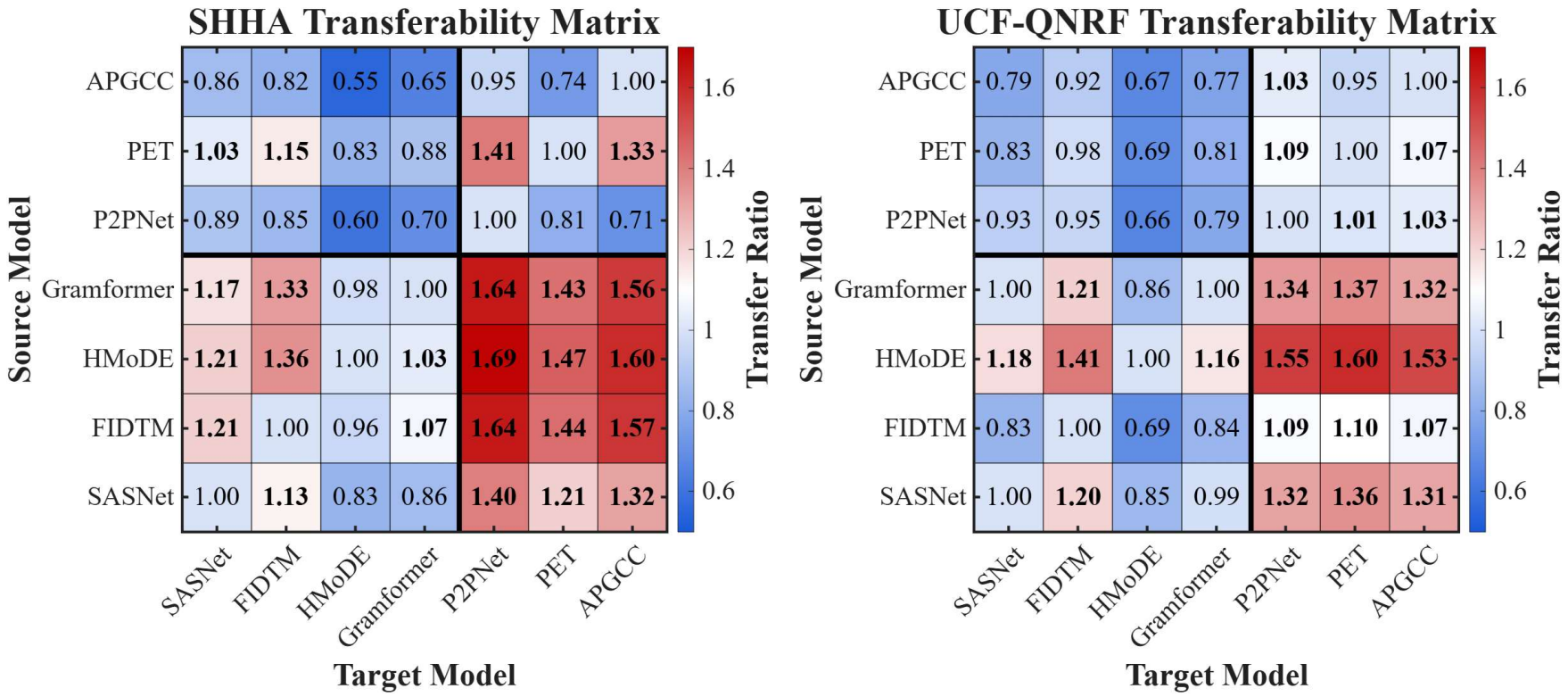


Transferability through Backbone Dependency

(a) Clean (P2PNet) (b) Adversarial (P2PNet) (c) Clean (SASNet) (d) Adversarial (SASNet)

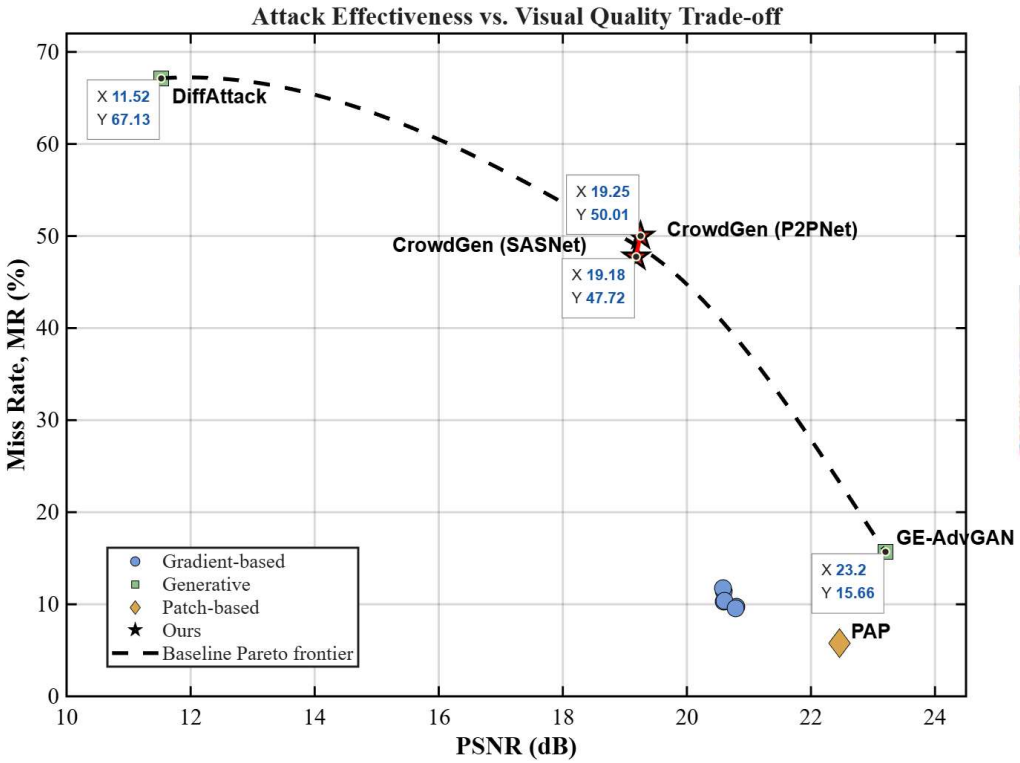
Both P2PNet (Point Regression) and SASNet (Density Map) model has same VGG-16 backbone

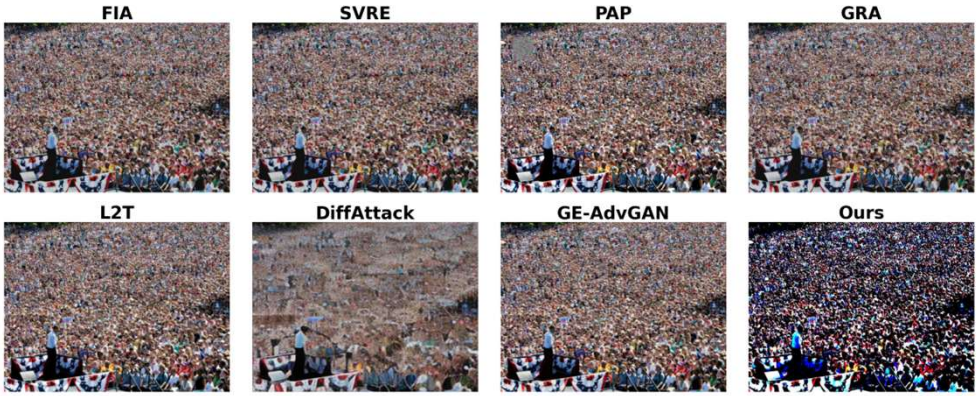
Transferability Analysis



Super Transferability!

Baseline Comparison





- DiffAttack: Very Strong but Visible
- Ge-AdvGAN: Very Stealthy but Weak
- Ours (CrowdGen): Strong + Stealthy

UNIVERSITY of SOUTH FLORIDA

CVPR JUNE 3-7, 2026 DENVER COLORADO

Alabi Mehzabin Anisha

Guangjing Wang

Sriram Chellappan

Paper: https://arxiv.org/abs/2603.24821
Code: https://github.com/simurgh7/CrowdGen