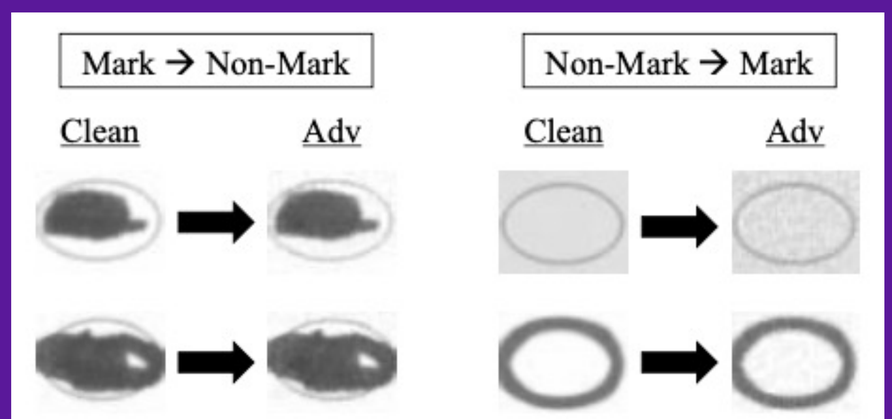
We applied machine learning in the voting domain!



Here's what we found:

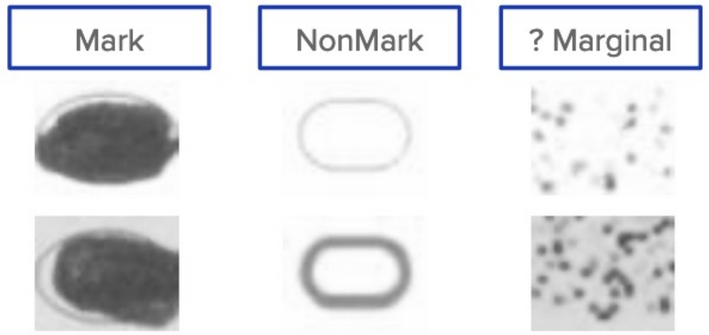
Image classifiers are vulnerable if the data is too complex

Vulnerable models = election flip possibility

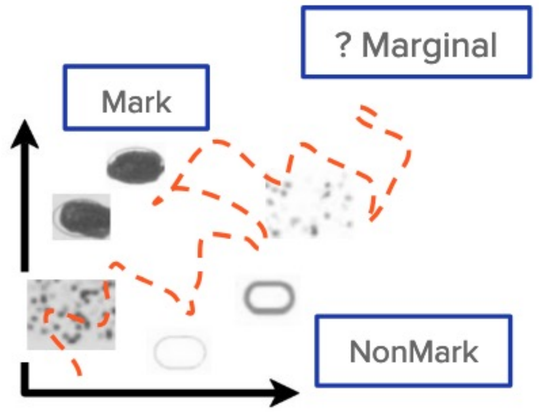
But we can make models more robust by training on complex data

Overview

Voter bubbles are fed to image classifiers to classify as 'Vote/Non-Vote'.



These image classifiers are vulnerable to attacks!



Methods

Field: Deep learning, machine learning, image classification

Models: Support Vector Machine (SVM), Convolutional Neural Network (CNN), Twins vision transformer

Software: Python (PyTorch, numpy, matplotlib), Git/Github

How can YOU get involved?

- Be curious!
- Take initiative!
- Coding & data science classes
- Go the extra mile in your projects
- Talk to your professors

scan me!

Presenter: Aayushi Verma, PhD student in Computer Science
UConn VoTeR Center research