A Collaborative Case Study: Increasing Undergraduate Research in Cybersecurity at HBCUs

Chutima Boonthum-Denecke and Idongesit Mkpong-Ruffin
Hampton University and Florida A&M University
The AI-CyS Research Partnership Project

NSF CISE-MSI HBCU AI-CyS Research Partnership

Hampton University [Award #2131255], Florida A&M University [Award #2131256], Winston-Salem State University [Award #2131259], Mississippi Valley State University [Award #2131257], University of the District of Columbia [Award #2131258], Norfolk State University [Award# 2131260], and Howard University

NSF CISE-MSI HBCU AI-CyS

The Team

Chutima Boonthum-Denecke

Jean Muhammad

Hampton University

Idongesit Mkpong-Ruffin

Deidre Evans

Florida A&M University

Elva Jones

Rebecca Caldwell

Winston-Salem State University

Latonya Garner-Jackson

Mississippi Valley State University

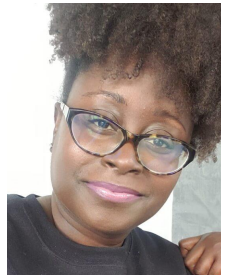
Briana Wellman

Lily Liang

University of the District of Columbia

Felicia Doswell

Norfolk State University



Gloria Washington

Howard University

AI-CyS Overview

Leveraging the collaboration between HBCUs and national research laboratories

- by "***capitalizing on the synergies from current HBCU collaborations***"
- to investigate the use of Artificial Intelligence (AI) to address cyber security challenges
- to increase research in Artificial Intelligence and Cybersecurity with HBCU partners in collaboration with national research laboratories

AI-CyS Approach

The activities of this project will

A. increase institutional capacity at HBCUs research in AI and Cybersecurity and foster the collaboration among HBCU-faculty as well as with national research laboratory;

B. increase the number of students, especially undergraduate students from under-represented groups in conducting research; and

C. provide students with mentoring from their own HBCU, partnered HBCUs, as well as mentors from the national research laboratory.

Goal 1: Research Capacity Building

1. **Training from National Research Laboratories (NRL)**
2. **Technology/Knowledge Transfer from HBCU to HBCU**
3. **HBCU faculty and students visiting National Research Labs**

Goal 2: Research Projects - Faculty and Student Research

Start-up Research Projects:

1. **Reinforcement Learning Autonomous Cyber Security Agents** (UDC, NSU)
2. **Exploration of Ways to Disambiguate Traceroute Data for Improved Understanding of Computer Networks** (WSSU, Howard)
3. **The Universal Adversarial Patch Attack** (HamptonU, FAMU, WSSU)
4. **(Surveillance) Videos Authenticate in Near Real-time** (FAMU, UDC, Howard)
5. **BUILD-SOS - Internet-of-Thing Security** (HamptonU, MVSU)

Collaboration Example

Hampton U

Florida A&M U

Winston-Salem State U

+

Brookhaven National Lab

Brookhaven National Laboratory

Collaboration to help increase HBCU Research Capacity by providing

- summer lecture series: adversarial attacks and forgeries, deep neural network, forgery data sets
- initial start-up research project ideas
- research mentoring support
- future proposal collaboration

Adversarial Patch Attack

Hampton U

Florida A&M U

Winston-Salem State U

+

Brookhaven National Lab

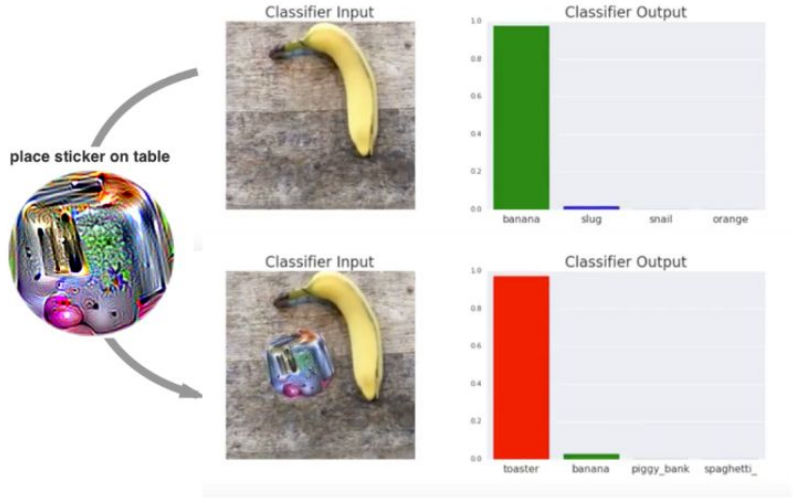


Figure from Brown et al, 2018:
A real-world attack using a generated physical patch:
banana vs. toaster

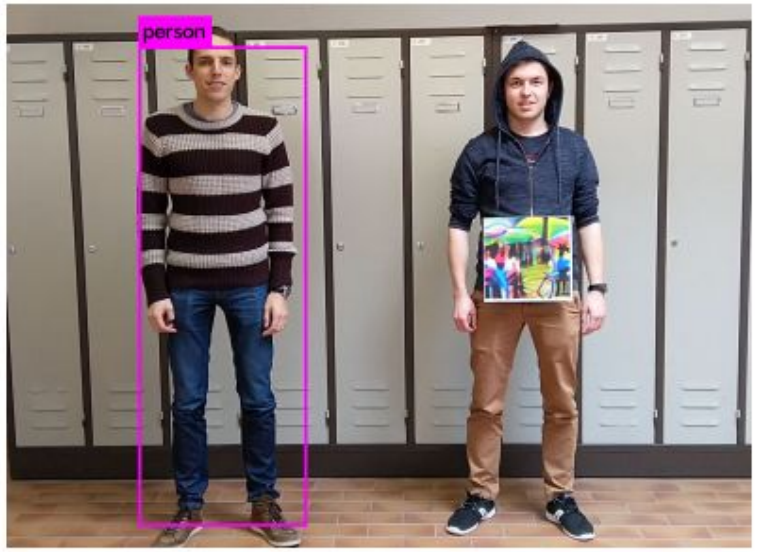
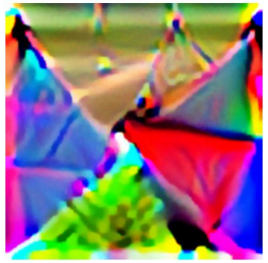


Figure from Thys et al, 2019:
An adversarial patch that is successfully able to hide persons from a person detector.
(Left): The person without a patch is successfully detected.
(Right): The person holding the patch is ignored.

(Below): Sample batches



Current and Future Work

Hampton U

Florida A&M U

Winston-Salem State U

+

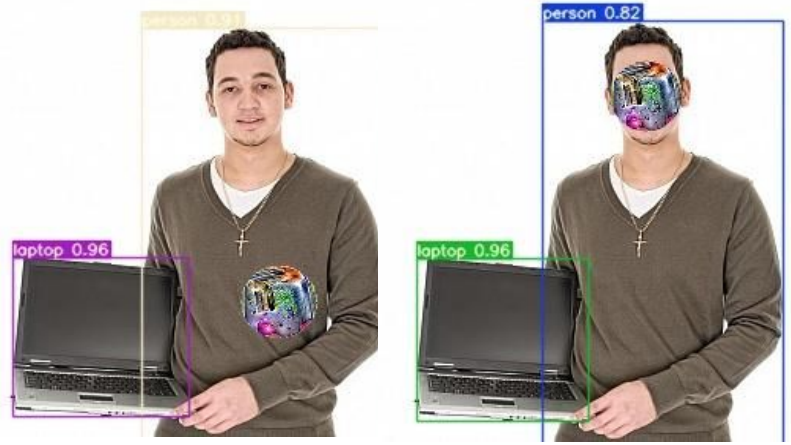
Brookhaven National Lab

Current Sub-Projects this past year:

- Mitigating the Impact of Object Overlapping on YOLOv4 Object Detection
- Impact of Adversarial Patches on Object Detection with YOLOv7
- Revolutionizing YouTube Thumbnails: Homogeneous Decentralization with the Power of YOLOv4 Object Detection Model

Future Work - upcoming year

- Repeat process with a larger data different types of images
- Compare YOLO versions: v2, v4, v7




Questions?