Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

ONR Approval #

Topic # N182-127

Fooling Computer Vision Classifiers with Adversarial Examples

Lynntech, Inc.

WHO

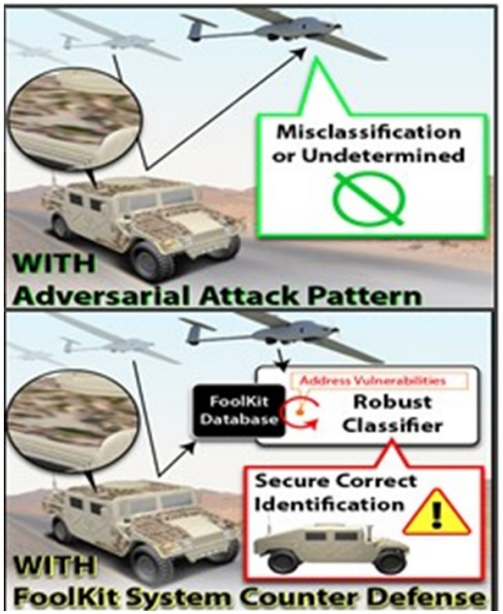
SYSCOM: ONR

Sponsoring Program:

Transition Target: USMC PEO Land Systems

TPOC:
Dr. Michael Qin
michael.qin@navy.mil

Other transition opportunities: Aerial platforms, ISR, ATR, future UAS



2019 Lynntech Inc.

WHAT

Operational Need and Improvement: The increasing amount of sensor data streams and use of unmanned platforms demands the increased automation of many tasks. However, such intelligent systems have vulnerabilities to evasive manipulations of appearances that can fool them. Deploying and/or countering such Computer Vision Camouflage is anticipated to become a pressing operational need in the near future. As it is developed across the EM spectrum this will likely disrupt the performance of established ISR/ATR systems, demanding more robust computer vision detectors and classifiers as well as counter defenses.

Specifications Required: Synthesize robust and transferable attack patterns for a range of view points for five CV FoolKit variants. Successfully degrade object detection/classification with black-box (unknown) computer vision classifiers.
Develop counter defenses to robust physical adversarial examples.

Technology Developed: Lynntech Inc. has developed its Computer Vision FoolKit technology to provide a form of computer vision camouflage that is tailor-made for making an object of interest evasive in appearance to (semi)-automated ISR/ATR systems that are trained with most machine learning approaches. Lynntech has successfully fooled white box (known) classifiers and has developed rigorous synthesis and evaluation procedures to ensure the effectiveness of our camouflage patterns in black box tests against unknown classifiers.

Warfighter Value: Development of Lynntech's computer vision camouflage will lower the probability of detection by the enemy of U.S. warfighters and their allies. The development of the complimentary counter defense to Computer Vision FoolKit will increase the situational awareness of U.S. warfighters and their allies, keeping them safer and giving them an edge on the battlefield.

WHEN

Contract Number: N68335-20-C-0096 **Ending on:** November 19, 2021

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Digital tests of CV FoolKit variants	Low	Decrease known classifier performance in digital realm	3	1st QTR FY21
Lab validation of CV FoolKit variants	Low	Decrease known classifier performance on scale model	3-4	1st QTR FY21
Field tests of CV FoolKit variants	Med	Decrease known classifier performance in field test	4-5	3rd QTR FY21
Design counter defense to CV FoolKit	Med	Evaluate all adversarial patterns	4	4th QTR FY21
Field test prototype camouflage decals	High	Test against unknown classifier	5-6	1st QTR FY22

HOW

Projected Business Model: Lynntech Inc. plans to transition the Computer Vision FoolKit technology by either (i) providing a software as a service (SAAS) to DoD transition partner(s); or (ii) licensing the technology to a defense industry partner(s). The current business strategy is to sell a service or license to an existing defense prime since the base ISR/ATR technology is established, this approach lowers the required investment, it satisfactorily addresses the security restrictions and provides an established customer base.

Company Objectives: Lynntech's objectives for this project are to degrade the performance of state-of-the-art Computer Vision systems as well as develop a breadboard prototype of a counter defense to the FoolKit , and thereby break into the DoD IRS/ATR market. Lynntech is a for-profit small business and believes that if we properly meet the above objectives, sales and profit will follow.

Potential Commercial Applications: Civilian application include providing tools for AI security evaluations unto the development more robust Computer Vision systems for autonomous systems (e.g. self-driving vehicles), industrial inspection, security and the Internet of Things (IoT).

Contact: Brian Hennings, V.P. Business Development
brian.hennings@lynntech.com (979) 764-2234