Odin

INTELLIGENCE VALUE

The Odin program is developing biometric presentation attack detection technologies to help the government better detect when someone is attempting to hide their identity by spoofing biometric access control or authentication systems.

Biometrics are used by the U.S. government to verify identities and locate persons of interest. However, biometric presentation attacks, known as PAs or spoofs, can prevent correct identification. These PAs can also lead to unauthorized access to sensitive facilities, or information. Compromised biometric systems erode the trust of users. Odin's goal is to identify known and unknown PAs in face, iris, and fingerprint biometric collection systems. Typical PAs utilize a prosthetic to conceal the subject's biometric trait, or present an alternative biometric signature. Odin detects these PAs, with both software and hardware solutions, by applying deep learning and computer vision to visible or multispectral images. The results are used to discriminate between PAs and legitimate samples, based on prior knowledge of the attributes of a true sample, and normalcy modelling for anomaly detection.

Odin's presentation attack detection system's performance is quantified by the detection accuracy with a corresponding false alarm rate. This metric reflects the important balance for real-world usability. The final target metric is 97 percent average detection accuracy, at 0.2 percent false alarm rate. The unique methods developed and tested on large human-scale subjects under the Odin program have met or exceeded research goals and are positioned for deployment in real-world biometrics applications.

PRIME PERFORMERS

- Michigan State University
- University of Southern California Information Sciences Institute
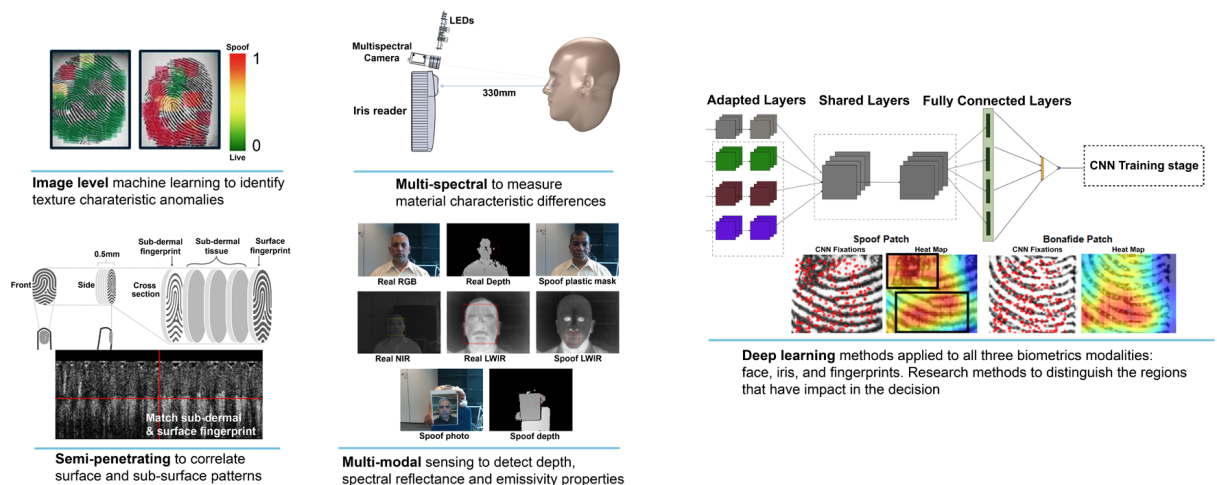- HID Global
- SRI International

TESTING AND EVALUATION PARTNERS

- Johns Hopkins University Applied Physics Laboratory
- National Institute of Standards and Technology

KEYWORDS

- Presentation attack detection
- Spoof detection
- Biometric identity intelligence
- Deep neural networks
- Machine learning
- Computer vision
- Multispectral sensors

Odin OVERVIEW ▶

Image level machine learning to identify texture charateristic anomalies

Semi-penetrating to correlate surface and sub-surface patterns

Multi-spectral to measure material characteristic differences

Multi-modal sensing to detect depth, spectral reflectance and emissivity properties

Deep learning methods applied to all three biometrics modalities: face, iris, and fingerprints. Research methods to distinguish the regions that have impact in the decision

PROGRAM MANAGER

Lars Ericson, Ph.D.
Phone: (301) 243-1817
lars.ericson@iarpa.gov

ODIN

www.iarpa.gov

@IARPAnews

Latest Revision: 03/10/2021