

CAN TECH CATCH THE COUNTERFEITS?

In recent years, technology developers have created new software that has helped millions of people apply for government services, open bank accounts, or verify social media accounts by submitting identity information online. These technologies typically allow users to take photographs of their identity document and selfie photo to assert their identity online, without having to go to an office in person. The technologies use the images to:

- 1) distinguish between genuine and fraudulent identity documents
- 2) determine “liveness” or genuine presence of an individual in a selfie photo
- 3) match the individual in a selfie photo to a photo ID or other authoritative image

The adoption of these technologies has grown due to significant user convenience and reduced costs to government and private sector service providers who would otherwise need to have staff and physical facilities to allow a user to assert their identity. Mandatory closures and social distancing associated with the COVID-19 pandemic have made in-person identity verification more difficult, further accelerating the adoption of these technologies.

While these capabilities have already achieved widespread adoption, there is little independent or objective data characterizing the performance and fairness of the technologies as well as the degree to which they may reduce fraud at scale.

FRUSTRATING THE FRAUDSTERS

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Biometric and Identity Technology Center (BI-TC) is partnering with multiple federal agencies to host the Remote Identity Validation Technology Demonstration (RIVTD) Challenge, a series of test events to examine the performance of document authentication software as well as selfie photo “liveness” and identity verification using imagery collected with smartphones and other commodity electronic devices.

RIVTD will challenge industry to (1) deliver secure, accurate, and easy-to-use technologies; (2) objectively measure

performance in realistic scenarios and sophisticated attacks; (3) answer questions about the overall performance, risks, and fairness of these technologies for use in commercial or government applications; and (4) inform efforts to standardize and certify technologies that are effective against sophisticated and rapidly evolving attacks.



CORE ACTIVITIES

The S&T BI-TC and its partners will assess the performance of the remote identity validation technologies by evaluating the:

- performance of systems to differentiate between photos of genuine and fraudulent identity documents
- performance of systems to detect attackers attempting to impersonate other people
- variations in performance across different user demographics

The BI-TC will also identify vulnerabilities and risks to inform DHS stakeholders and standards developers, to establish more robust test procedures based on increasing sophistication of attack methods. The RIVTD Challenge will help DHS and federal agencies establish a baseline of current commercial performance, understand gaps that require further investment, and assist industry in innovating to address this widescale problem.

PARTNERS

DHS S&T is partnering with the Transportation Security Administration, Homeland Security Investigations Forensic Laboratory, and the National Institute of Standards and Technology.