NOVETTA

Biometric Technology Evaluation

PERFORMANCE EVALUATIONS

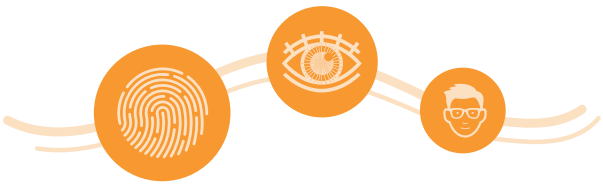
Novetta is closely aligned with the RDT&E needs of the evolving biometric community. Novetta provides technology-neutral, vendor-independent biometric research, consulting, and testing to government and law enforcement agencies, systems integrators, vendors, and commercial deployers. Over the past 20 years, Novetta has conducted hundreds of challenging and novel biometric evaluations, to include:

- First comparative biometric system testing program (1998)
- First test of skin texture technology (2002)
- First independent testing of iris recognition (2005)
- First confirmed false-match iris pair (2002) and interoperability test
- First systematic spoof resistance evaluation program (2007)
- First vascular recognition test (2007)
  - Palm vein test results led directly to global deployment of technology for 1:N fraud detection
- First large-scale evaluation of text-independent 1:N voice (2008)
- First large-scale evaluation of contactless fingerprint technology (2008)
- Development of first presentation attack detection testing standard
- Collection, evaluation, and development of novel behavioral and cognitive biometric matchers
- Development of next-generation fusion methods that are adaptive to operational environment

Novetta's test and evaluation facilities in New York, NY and Tysons Corner, VA, include hundreds of integrated biometric technologies; spoofing facilities; processing hardware for metric generation; experienced biometric systems engineers; and proprietary evaluation frameworks that enable the execution of multi-visit technology evaluations with live subjects. Novetta has tested dozens of technologies using ISO 19795 standards, providing results that vendors can use in outreach to industry (e.g. potential clients, investors). Novetta Subject Matter Experts actively contribute to NIST, ANSI, INCITS, and other organizational efforts to develop biometric testing and evaluation standards.

SPOOFING, PRESENTATION ATTACK, & LIVENESS DETECTION

Novetta performs spoofing and liveness detection, key components of biometric vulnerability assessments, using advanced materials and methods. Novetta generates custom methodologies for security evaluations, to include development and implementation of testing methods, as well as specialized attack scenarios and custom biometric artefacts. Novetta had developed both offensive and defensive spoofing and liveness detection solutions, leveraging deep expertise in biometric sensors and algorithms. These capabilities enable manufacturers, developers, and end users to deploy or use biometric systems with mitigated risks, and also provide a practical, real-world understanding of the time, resources, and expertise required to defeat a biometric sensor. Novetta SMEs are also directly involved in the development of global standards for presentation attack detection.



BIOSYNTHETIC FINGERPRINT, FACE & IRIS GENERATION

Novetta's Biosynthetic software generates realistic, synthetic biometric images of fingerprints, faces, and irises that are optimized for biometric system testing. Images are available in quantities of up to 13 million per dataset (consisting of: 1 million faces, 2 million irises, and 10 million fingerprints), in high-, medium-, and low-quality subsets that generate realistic error rates. Biosynthetics simplify biometric system design and performance evaluation of new matchers, enabling vendors, deployers, and integrators to test accuracy, throughput, and scalability at meaningful volumes. Novetta's Biosynthetic generation capability dramatically reduces the time, effort, cost, and privacy risks associated with human biometric data collection and usage, while enabling testing that is customized to key aspects of biometric systems and operational use cases.

NOVETTA

Biometric Technology Evaluation

DATA COLLECTIONS CAPABILITIES AT U.S. MILITARY ACADEMY, WEST POINT

Novetta is uniquely positioned to conduct biometric and cyber data collections in conjunction with U.S. Military Academy (USMA), West Point. Capabilities at-a-glance include:

- **Human Subjects Research** – Access to hundreds of study participants
- **Rapid Collection** – Automated recruitment system for rapid data subject recruitment; ability to collect thousands of data points in weeks
- **Customized / controlled Protocols** – Developed by SMEs for mission-specific technology usage scenarios
- **Institutional Review Board (IRB) Access** – In-house IRB council for fast IRB protocol development and approvals
- **Experienced Research Technician** – Operates on-site to ensure successful protocol development and execution; expertise in available laboratories and equipment
- **Government Collaboration & Partnership** via US ARMY Mission & Installation Contracting Command (MICC) to facilitate contracting and funding allocation

AVAILABLE DATA COLLECTIONS RESOURCES & LABORATORY FACILITIES

- **Research Departments** – Behavioral Sciences, Engineering & Cognitive Psychology, Anthropometrics & Biomechanics, Sociology (relevant work areas in human automation & human factors engineering; virtual reality; anthropometrics & biomechanics; sensation & perception; immersive & tactical training; more)
- **Advanced Research Equipment** – Laboratory facilities offer access to a variety of resources including advanced hardware, training systems, networking capabilities, and controlled study environments.
- **West Point Simulation (SIM) Center** - 2100+ sq. ft. computer lab space capable of hosting up to 40 networked computers supporting simulation-based research, including access to advanced hardware and controlled environments.
- **The Army Cyber Institute / Cyber Research Center** – Support research and information sharing in cyber domain to enable effective army cyber defense and operations
- **Institute for Creative Technologies (ICT)** – DoD-sponsored UARC supporting innovative research in artificial intelligence, virtual reality, and immersive technologies; partner relationship with University of Southern California (USC) for participant recruitment and facilities access
- USMA provides an extensive array of resources not described here; details on **additional lab facilities** and **advanced research systems** resources available upon request

REPRESENTATIVE WORK AREAS

Starting in 2015, collections efforts have targeted novel cognitive and behavioral biometric data for insider threat detection; behavioral and physiological biometric data with induced-stress protocols for detection of abnormal or malicious behavior; and voice data to validate and analyze speaker dynamics. Potential future work areas include:

- Scenario and operational testing for mission-critical markets e.g. healthcare monitoring and diagnostics, behavioral and physical security applications, public safety
- Performance and vulnerability assessments
- Biometric data collection and evaluation for mobile, multi-modal and multi-INT authentication systems
- Novel biometric data collection and testing for sensor and software development
- Simulation-based testing to support military and operational training