

Testimony of

Charles H. Romine  
Director  
Information Technology Laboratory  
National Institute of Standards and Technology  
United States Department of Commerce

Before the

Committee on Homeland Security  
United States House of Representatives

*Use of Biometric Technologies at the Department of Homeland Security*

July 10, 2019

## **Introduction**

Chairman Thompson, Ranking Member Rogers, and Members of the Committee, I am Chuck Romine, Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). NIST cultivates trust in information technology and metrology through measurements, standards and testing. Thank you for the opportunity to appear before you today to discuss NIST's role in biometrics standards and testing for facial recognition technology.

## **Biometric and Facial Recognition Technology**

Home to five Nobel Prizes, with programs focused on national priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of biometrics, NIST has been working with the public and private sectors since the 1960s. Biometric technologies provide a means to establish or verify the identity of humans based upon one or more physical or behavioral characteristics. Examples of physical characteristics include face, fingerprint, and iris images. An example of a behavioral characteristic is an individual's signature. Used with other authentication technologies, such as passwords, biometric technologies can provide higher degrees of security than other technologies employed alone. For decades, biometric technologies were used primarily in homeland security and law enforcement applications, and they are still a key component of these applications. Over the past several years, the marketplace for biometric solutions has widened significantly and today includes public and private sector applications worldwide, including physical security, banking and retail applications. According to one industry estimate, the biometrics technology market will be worth \$59.31 billion by 2025.<sup>1</sup> There has been a considerable rise in development and adoption of facial recognition, detection and analysis technologies in the past few years.

Facial recognition technology compares an individual's facial features to available images for identification or authentication. Facial detection technology determines whether the image contains a face. Facial analysis technology aims to identify attributes such as gender, age, or emotion from detected faces.

## **NIST's Role in Biometric and Facial Recognition Technology**

NIST responds to government and market requirements for biometric standards, including facial recognition technologies, by collaborating with other federal agencies, law enforcement, industry, and academic partners to:

- research measurement, evaluation, and interoperability to advance the use of biometric technologies including face, fingerprint, iris, voice, and multi-modal techniques;
- develop common models and metrics for identity management, critical standards, and interoperability of electronic identities;
- support the timely development of scientifically valid, fit-for-purpose standards; and

---

<sup>1</sup> <https://www.grandviewresearch.com/industry-analysis/biometrics-industry>

- develop the required conformance testing architectures and testing tools to test implementations of selected standards.

NIST's work improves the accuracy, quality, usability, interoperability, and consistency of identity management systems and ensures that United States interests are represented in the international arena. NIST research has provided state-of-the-art technology benchmarks and guidance to industry and to federal agencies that depend upon biometrics recognition.

Under the provisions of the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) and OMB Circular A-119, NIST is tasked with the role of encouraging and coordinating federal agency use of voluntary consensus standards in lieu of government-unique standards, and federal agency participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards developing organizations such as the International Committee for Information Technology Standards (INCITS), Joint Technical Committee 1 of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), the Organization for the Advancement of Structured Information Standards (OASIS), IEEE, the Internet Engineering Task Force (IETF), and other standards organizations such as the International Civil Aviation Organization (ICAO), and the International Telecommunication Union's Standardization Sector (ITU-T). NIST leads national and international consensus standards activities in biometrics, such as facial recognition technology, but also in cryptography, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing – all essential to accelerate the development and deployment of information and communication systems that are interoperable, reliable, secure, and usable.

Since 2010, NIST has organized the biennial International Biometric Performance Testing Conference; more than one hundred biometric experts from all around the globe traditionally attend. This series of conferences accelerates adoption and effectiveness of biometric technologies by providing a forum to discuss and identify fundamental, relevant, and effective performance metrics, and disseminating best practices for performance design, calibration, evaluation, and monitoring.

### **Facial Recognition Tests and Evaluations**

For more than a decade, NIST biometric evaluations have measured the core algorithmic capability of biometric recognition technologies and reported the accuracy, throughput, reliability, and sensitivity of algorithms with respect to image characteristics such as noise or compression, and to subject characteristics such as age or gender. NIST biometric evaluations advance the technology by identifying and reporting gaps and limitations of current biometric recognition technologies. NIST evaluations advance measurement science by providing a scientific basis for “what to measure” and “how to measure.” NIST evaluations also facilitate development of consensus-based standards by providing quantitative data for development of scientifically sound, fit-for-purpose standards. NIST biometrics evaluations are highly regarded and valued by developers, users, and policy makers.

NIST conducted the Face Recognition Grand Challenge (2004-2006) and Multiple Biometric Grand Challenge (2008-2010) programs to challenge the facial recognition community to break new ground solving research problems on the biometric frontier. Since 2000, NIST's Face Recognition Vendor Testing Program (FRVT) has assessed capabilities of facial recognition algorithms for one-to-many identification and one-to-one verification.

To better align NIST's evaluation schedule with the pace of facial recognition advancement in industry and academia, NIST expanded its facial recognition evaluations in 2017. NIST broadened the scope of its work in this area to understand the upper limits of human capabilities to recognize faces and how these capabilities fit into facial recognition applications. NIST evaluations have quantified accuracy for investigative use-cases which involve human review of candidates from an automated system, as well as for fully automated identification applications in which decisions would be accepted on the basis of an automated search alone.

NIST's work on demographic effects in facial recognition is ongoing. For example, a report addressing demographic effects in mugshots collected in domestic law enforcement applications is under development with an expected publication date of Fall 2019.

NIST provides technical guidance and scientific support for analysis and recommendations for utilization of facial recognition technologies to various federal agencies, including the Federal Bureau of Investigation (FBI), Office of Biometric Identity Management (OBIM) at the Department of Homeland Security (DHS), Department of Homeland Security Science and Technology Directorate (DHS S&T), the Department of Homeland Security's U.S. Customs and Border Protection agency (DHS CBP), and the Intelligence Advanced Research Projects Activity (IARPA) at the Office of the Director of National Intelligence. Further, as DHS S&T works with Transportation Security Administration (TSA) to scientifically analyze data from its biometrics pilots to inform TSA's capability development process, NIST has and will continue to provide consultation to DHS S&T to assure its analysis methodologies meet industry standards.

Historically and currently, NIST biometrics research has assisted DHS. NIST's research was used by DHS in its transition from two to ten prints for the former US-VISIT program and NIST is currently working with DHS CBP to analyze performance impacts due to image quality and traveler demographics and provide recommendations regarding match algorithms, optimal thresholds and match gallery creation for its Traveler Verification Service program. Currently, NIST is collaborating with DHS CBP on the evaluation of their Traveler Verification Service (TVS), and with DHS OBIM on face image quality standards.

### **NIST Face Recognition Vendor Testing Program**

NIST's Face Recognition Vendor Testing Program (FRVT) was established in 2000 to provide independent evaluations of both prototype and commercially available facial recognition algorithms. These evaluations provide the federal government with information to assist in determining where and how facial recognition technology can best be deployed. FRVT results also help identify future research directions for the facial recognition community.

The 2013 FRVT tested facial recognition algorithms submitted by 16 organizations, and showed significant algorithm improvement since NIST's 2010 FRVT test. NIST defined performance

by recognition accuracy—how many times the software correctly identified the photo—and the time the algorithms took to match one photo against large photo data sets.

The 2018 FRVT tested 127 facial recognition algorithms from the research laboratories of 39 commercial developers and one university, using 26 million mugshot images of 12 million individuals provided by the FBI. The 2018 FRVT measured the accuracy and speed of one-to-many facial recognition identification algorithms. The evaluation also contrasted mugshot accuracy with that from lower quality images. The findings, reported in NIST Interagency Report 8238,<sup>2</sup> showed that massive gains in accuracy have been achieved since the FRVT in 2013, which far exceed improvements made in the prior period (2010-2013). The accuracy gains observed in the 2018 FRVT study stem from the integration, or complete replacement, of older facial recognition techniques with those based on deep convolutional neural networks. While the industry gains are broad, there remains a wide range of capabilities, with some developers providing much more accurate algorithms than others. Using FBI mugshots, the most accurate algorithms fail only in about one quarter of one percent of searches. These failures are mostly associated with images of persons with facial injury and those with a long time lapse (17 years or more for the most accurate algorithm) since the first photograph. The success of mugshot searches stems from the new generation of facial recognition algorithms, and from the adoption of portrait photography standards first developed at NIST in the late 1990s.

### **NIST Face in Video Evaluation Program**

The Face in Video Evaluation Program (FIVE) assessed the capability of facial recognition algorithms to correctly identify or ignore persons appearing in video sequences. The outcomes of FIVE are documented in NIST Interagency Report 8173,<sup>3</sup> which enumerates accuracy and speed of facial recognition algorithms applied to the identification of persons appearing in video sequences drawn from six different video datasets. NIST completed this program in 2017.

### **Human Factors: Facial Forensic Examiners**

NIST is researching how to measure the accuracy of forensic examiners matching identity across different photographs. The study measures face identification accuracy for an international group of professional forensic facial examiners working under circumstances approximating real-world casework. The findings, published in the proceedings of the National Academy of Sciences,<sup>4</sup> showed that examiners and other human face “specialists,” including forensically trained facial reviewers and untrained super-recognizers, were more accurate than the control groups on a challenging test of face identification. It also presented data comparing state-of-the-art facial recognition algorithms with the best human face identifiers. The best machine performed in the range of the best-performing humans, who were professional facial examiners. However, optimal face identification was achieved only when humans and machines collaborated.

### **Voluntary Consensus Standards**

When properly conducted, standards development can increase productivity and efficiency in government and industry, expand innovation and competition, broaden opportunities for

---

<sup>2</sup> <https://www.nist.gov/publications/ongoing-face-recognition-vendor-test-frvt-part-2-identification>

<sup>3</sup> <https://www.nist.gov/publications/face-video-evaluation-five-face-recognition-non-cooperative-subjects>

<sup>4</sup> <https://www.pnas.org/content/115/24/6171>

international trade, conserve resources, provide consumer benefit and choice, improve the environment, and promote health and safety.

In the U.S., most standards development organizations are industry-led private sector organizations. Many voluntary consensus standards from those standards development organizations are appropriate or adaptable for the government's purposes. OMB Circular A-119 directs the use of such standards by federal agencies, whenever practicable and appropriate, to achieve the following goals:

- eliminating the cost to the federal government of developing its own standards and decreasing the cost of goods procured and the burden of complying with agency regulation;
- providing incentives and opportunities to establish standards that serve national needs, encouraging long-term growth for U.S. enterprises and promoting efficiency, economic competition, and trade; and
- furthering the reliance upon private sector expertise to supply the federal government with cost-efficient goods and services.

### **Examples of NIST Consensus Standards Development Activities**

**ANSI/NIST-ITL** – The ANSI/NIST-ITL standard for biometric information is used in 160 countries to ensure biometric data exchange across jurisdictional lines and between dissimilar systems. One of the important effects of NIST work on this standard is that it allows accurate and interoperable exchange of biometrics information by law enforcement globally and enables them to identify criminals and terrorists. NIST's own Information Technology Laboratory is an American National Standards Institute (ANSI)-accredited standards development organization. Under accreditation by ANSI, the private-sector U.S. standards federation, NIST continues to develop consensus biometric data interchange standards. Starting in 1986, NIST has developed and approved a succession of data format standards for the interchange of biometric data. The current version of this standard is ANSI/NIST-ITL 1: 2015, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information.<sup>5</sup> This standard continues to evolve to support government applications including law enforcement and homeland security, as well as other identity management applications. Virtually all law enforcement biometric collections worldwide use the ANSI/NIST-ITL standard. NIST biometric technology evaluations in fingerprint, face, and iris have provided the government with timely analysis of market capabilities to guide biometric technology procurements and deployments.

### **ISO/IEC Joint Technical Committee 1, Subcommittee 37 (JTC1/SC37) - Biometrics**

From the inception of the ISO Subcommittee on Biometrics in 2002, NIST has led and provided technical expertise to develop international biometric standards in this subcommittee. Standards developed by the Subcommittee on Biometrics have received widespread international and national market acceptance. Documents issued by large international organizations, such as the International Civil Aviation Organization for Machine Readable Travel Documents and the International Labour Office (ILO) of the United Nations for the verification and identification of

---

<sup>5</sup> <https://www.nist.gov/publications/data-format-interchange-fingerprint-facial-other-biometric-information-ansinist-itl-1-1>

seafarers, specify in their requirements the use of some of the international biometric standards developed by this subcommittee.

Since 2006, JTC1/SC37 has published a series of standards on biometric performance testing and reporting, many of which are based on NIST technical contributions. These documents provide guidance on the principles and framework, testing methodologies, modality-specific testing, interoperability performance testing, access control scenarios, and testing of on-card comparison algorithms for biometric performance testing and reporting. NIST plays a leading role in the development of these documents and follows their guidance and metrics in its evaluations, such as the FRVT.

### **Conclusion**

NIST is proud of the positive impact it has had in the last 60 years on the evolution of biometrics capabilities. With NIST's extensive experience and broad expertise, both in its laboratories and in successful collaborations with the private sector and other government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy interoperable, secure, reliable, and usable identity management systems.

Thank you for the opportunity to testify on NIST's activities in facial recognition and identity management. I would be happy to answer any questions that you may have.

## Charles H. Romine



Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of six research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of \$160 million, nearly 400 employees, and approximately 300 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission, to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the Nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

### **Education:**

Ph.D. in Applied Mathematics from the University of Virginia.

B.A. in Mathematics from the University of Virginia.