

NIST Contributions to Biometric Technology

Brad Wing, *US National Institute of Standards and Technology*

Standardizing biometric data and developing tools to evaluate data quality have been essential parts of NIST's IT contributions to this field for almost 50 years. The result has been improved reliability, fidelity, and accuracy in the processing of biometric data.

NIST has been at the forefront of IT contributions to biometric and identification management technology for almost 50 years.¹ In 1966, Carl Voelker of the Federal Bureau of Investigation (FBI) approached Raymond Moore at the National Bureau of Standards (NBS, later renamed as NIST) and told him that, without some form of automation, manual evaluation of fingerprints would soon overwhelm FBI capabilities.

Moore and Joseph Wegstein, another NBS researcher, examined the issue from two perspectives: automated fingerprint capture (hardware)² and automated matching algorithms to compare previously captured images against recently captured images. Wegstein developed the initial descriptors for fingerprint minutiae (such as ridge endings) to be used in automated systems, including their locations,

and orientations.³ Over the next 15 years, the FBI used the algorithms Wegstein developed in their implementations of automated fingerprint-identification systems.

By the 1980s, NBS had formed another group that worked directly with the Defense Advanced Research Projects Agency (DARPA) on speech recognition. The group, led by David Pallett, published the first NIST benchmark tests for quantitative performance measures of speech-recognition programs in 1986.⁴

Also in 1986, ANSI published the NBS's Institute for Computer Sciences and Technology (ICST) standard for fingerprint identification data.⁵ The ANSI/NBS-ICST standard supported the exchange of fingerprint minutiae among law enforcement agencies. It eventually grew to the present ANSI/NIST-ITL standard, incorporating many other biometric modalities.⁶

This early work laid the foundation for NIST's continuing emphasis on and support of biometric and identity management projects⁷ under the leadership of Charles Wilson, Mike Garis and Mark Przybocki.

Research and Evaluation Projects

NIST research has led to substantial improvements in many biometrics products and services by providing (and testing) appropriate, realistic data for identifying and verifying a person's identity.

NIST follows strict guidelines established by institutional review boards in assembling data. For example, any data collected from living persons requires their full, informed consent. The data is subsequently anonymized through coded identifiers, and its use is restricted to the purpose for which consent was originally obtained. Many specialized fingerprint databases also include data about deceased individuals.

These publicly available databases contain fingerprint and facial biometric data. Fingerprint data includes

- mated fingerprint pairs,
- digital video of live-scan fingerprints,
- fingerprint minutiae from latent and matching 10-print images,
- plain and rolled images from paired-fingerprint cards, and
- dual-resolution images from paired-fingerprint cards.

Facial data includes mug-shot identification images and high-resolution paired facial images.

By making portions of these databases available to researchers and product development teams, NIST provides a testing resource that's beyond what most organizations could acquire.

In addition, NIST uses specialized databases in conjunction with its evaluations of technologies and algorithms. The databases are typically partitioned to make a portion of the entire data available to researchers while reserving a portion as *sequestered data* that NIST uses in evaluating algorithm performance. This avoids the possibility of an algorithm becoming so finely tuned to the test data that it wouldn't function well with other representative samples.

Figure 1 shows NIST biometric evaluations in the modalities of face recognition, iris recognition, and fingerprint analyses from 2002 to 2012. Some of these evaluations are ongoing.

Fingerprint Matching

Fingerprint analyses have been a major part of NIST's biometrics work for many years.⁸ In 1987, the organization developed a benchmark for testing the performance of automated fingerprint identification systems.⁹ As Figure 1 shows, several NIST evaluations are now associated with fingerprints. For example, Fingerprint Vendor Technology evaluations (FpVTEs) range from testing whether images captured on single-finger-capture devices are interoperable with systems other than those developed by the device manufacturer to evaluating fingerprint-matcher algorithms on large databases. In 2012, under the guidance of Craig Watson, the FpVTE was divided into three parts—A, B, and C—as shown in Tables 1 and 2. The tables clearly indicate the complexity and size of these evaluations.

Over the years, NIST's ongoing research on friction-ridge impressions (fingerprint, palm prints, and footprints) has included the scalability of large matching systems, latent-print characterization, image-compression algorithms, and 3D-to-2D comparisons. In 2004, Elham Tabassi developed the NIST Fingerprint Image Quality (NFIQ) algorithm, based upon scientific research as to why matching algorithms fail.¹⁰ NFIQ allows operators to analyze a fingerprint image at the time of capture according to how well an automated system will be able to use it, rather than how "good" it appears to a human. In many circumstances, this makes it possible to recapture a sample from a person while that individual is still at the biometric-capture site. NFIQ also can assist in evaluating databases of existing images to determine their usefulness for matching. Tabassi is now developing a second-generation NFIQ algorithm.

Face Recognition

When Jonathon Phillips joined NIST in 1998, he built on his work from 1993 to 1997 at the US Army Research Laboratory (ARL), expanding NIST research in face recognition beyond posed, full-frontal images taken under relatively good conditions in an interior setting. Phillips'

NIST CONTRIBUTIONS TO IT

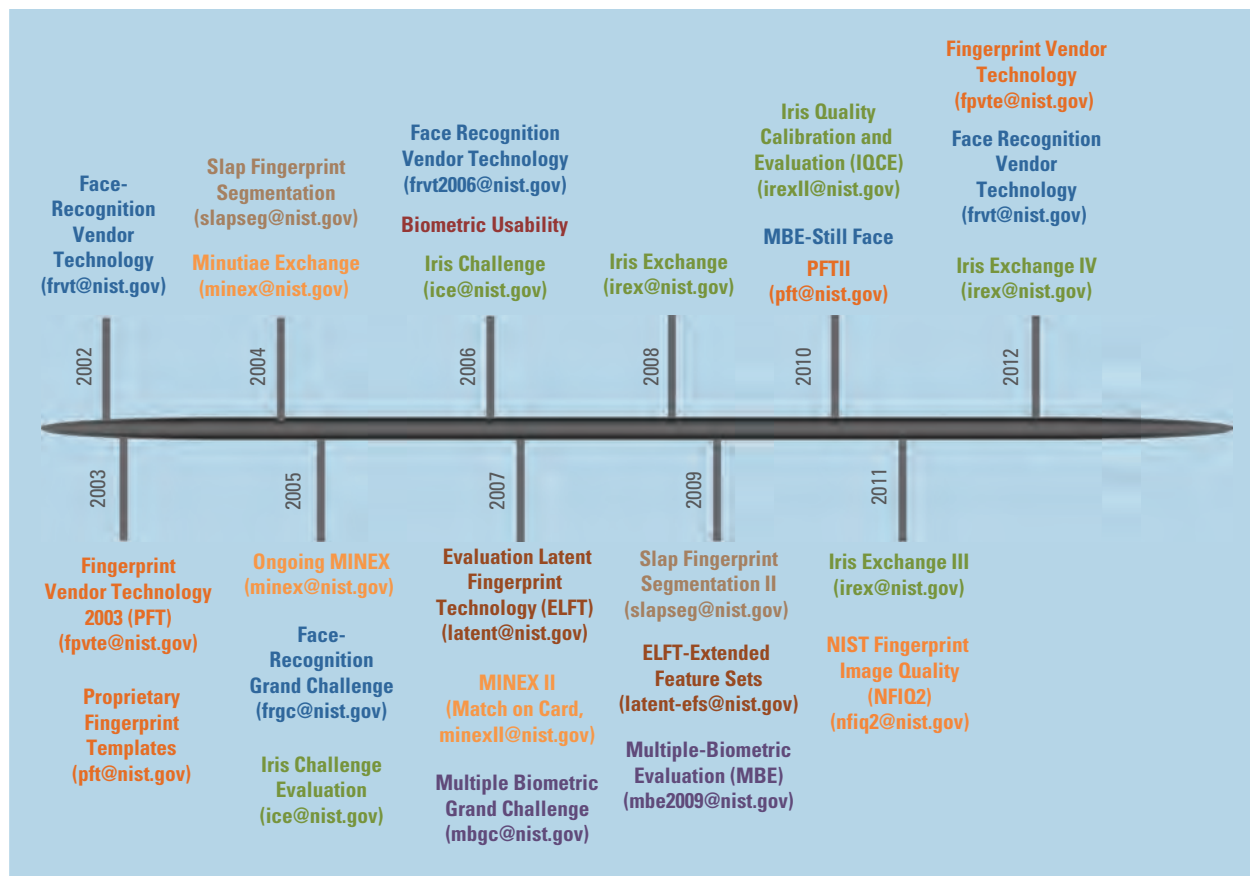


Figure 1. NIST biometric evaluations and challenge events from 2002 to 2012 (www.nist.gov/itl/iad/ig/biometric_evaluations.cfm). The evaluations are color-coded by modality. Many events are ongoing, such as the Face-Recognition Vendor Technology and the Minutiae Exchange (Minex) evaluations.

Table 1. Computation requirements in Fingerprint Vendor Technology Evaluation (FpVTE) 2012: Search and subject enrollment data.

Class	Dataset type	Search data	Search subject size	Enrollment data	Enrolled subject sizes
A	Single print, plain capture	1 finger, right or left index 2 fingers, right and left index	200,000 mates 400,000 nonmates	1 finger, plain capture 2 fingers, plain capture	5K, 10K, 100K 10K, 100K, 500K, 1.6M
B	Identification flats	10 fingers, plain (4-4-2) 8 fingers, right and left slap 4 fingers, right or left slap	200,000 mates 400,000 nonmates	10 fingers, plain (4-4-2)	500K, 1.6M, 3M
C	10-print capture	10 fingers, rolled 10 fingers, plain (4-4-1-1)	200,000 mates 400,000 nonmates	10 fingers, rolled 10 fingers, plain (4-4-1-1)	500K, 1.6M, 3M, 5M

research concentrated on the challenges of unposed, outdoor images and video sequences.¹¹ These challenges remain an important focus of current research, and results have contributed

directly to measurable improvements in face recognition technology, as shown in Figure 2. All biometrics trade off false rejection rates (FRR) with false acceptance rates (FAR), with the

Table 2. Computation requirements in Fingerprint Vendor Technology Evaluation (FpVTE) 2012: Number of enrollments and searches.

Class	Dataset type	No. of single-finger enrollments	No. of searches (phase 1)	No. of searches (phase 2) planned	Enrolled subject sizes
A	Single print, plain capture	8,832,000	90,000	1,800,000	5K, 10K, 100K 10K, 100K, 500K, 1.6M
B	Identification flats	93,990,000	120,000	2,400,000	500K, 1.6M, 3M
C	10-print capture	112,500,000	90,000	1,800,000	500K, 1.6M, 3M, 5M

balance between the two being specified for a particular application. To compare progress over time, it is necessary to fix one of these variables. In Figure 2, FAR is fixed, thus showing the improvement in FRR. It's most desirable to have low values for both FAR and FRR.

Patrick Grother leads the IRis EX-change (IREX) project, which he initiated to support an expanded marketplace of applications based on standardized interoperable iris imagery.¹² IREX grew out of NIST research that showed the feasibility of compressing the images to such an extent that it's possible to store the image on access cards while retaining characteristics necessary for automated matching. This work directly improved the efficiency and quality of iris-capture systems and data-transmission formats used around the world.

Recently, NIST research has focused on such topics as the impact of aging on iris recognition systems. IREX III and IREX IV extended the evaluations to include one-to-many iris recognition in large-scale applications. In 2013, NIST initiated two new projects in this area: the Iris Device Qualification Test and the Video-Based Automatic System for Iris Recognition.

Other Research Areas

NIST has conducted biannual speaker-recognition evaluations since 1996. The 2012 evaluation included 58 participating sites from 24 countries and six continents. The earlier evaluations concentrated on conversational telephone speech. More recently, assessments have extended to the

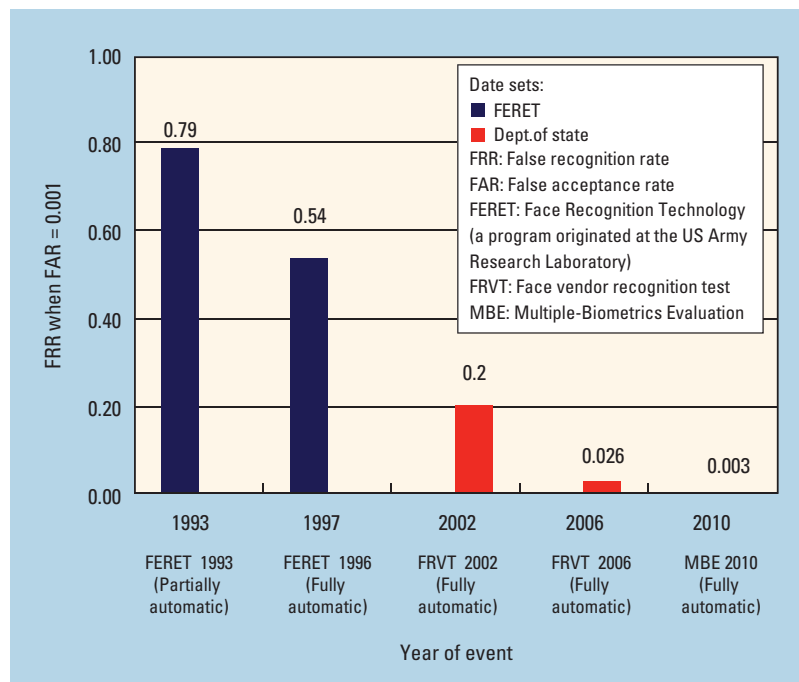


Figure 2. Progress in automated face matching using full-frontal images. All biometrics trade off false rejection rates (FRR) with false acceptance rates (FAR). To compare progress over time, it is necessary to fix one of these variables. Here, FAR is fixed, thus showing the improvement in FRR.

performance effects of variously located in-room microphone channels as well as the effects of in-room interview-style and conversational-style speech, multiple languages, additive or environmental noise, and high or low vocal effort. Analyses of demographic factors, such as sex, age, and education, have also been part of the evaluations.

DNA research has many biometric applications, and NIST has been active in it. For example, Peter Vallone and his team are working with other US Federal agencies to evaluate rapid DNA technology, which aims to reduce the time required for DNA analysis from days to hours.

Capturing a good quality sample is essential to an effective and accurately functioning biometric system. It requires making capture devices easy to use as well as providing a clear, intuitive user interface for data analysis. NIST's work in this area has improved systems such as fingerprint capture from foreign visitors to the US at the US ports of entry. Mary Theofanos and her team conducted extensive tests with human subjects and found the capture device's angle to be a major factor in a traveler's perception of the biometric-sample-capture process.¹³ A related key area of investigation is iconography—that is, developing signage for people who don't read English but need instructions as to how biometric samples will be collected.

NIST's challenge problems and evaluations have expanded beyond biometrics to several related fields, including speech recognition, multimedia event and surveillance detection, person tracking, automated transcription and translation, keyword searching, and handwriting evaluations.

Standardization and Best-Practice Guidelines

When the ANSI/NBS-ICST standard was published in 1986, it was the first attempt to codify the rules for exchanging fingerprint minutiae data. Beginning with the standard's next version in 1993, through 2007, Mike McCabe worked to forge consensus on fingerprint standards in the law enforcement community as well as with the major fingerprint-matcher vendors and capture-device manufacturers. McCabe expanded the standard to cover mug shots (face images), scar and tattoo images, fingerprint and palm images (as well as minutiae), and iris images. The resulting ANSI/NIST-ITL standard became the basis for biometric data exchange around the world. McCabe also worked with Shahram Orandi to develop best-practice requirements for mobile biometrics devices.¹⁴

Under my guidance, revisions to the NIST-ITL standard in 2011 and 2013 expanded its coverage to include

- an extended feature set for markups of latent print image;
- photographic images of all body parts;
- footprint image data (plantars);
- DNA data;

- information-assurance procedures for a transaction's authenticity;
- audio and video clips;
- data handling and processing logs;
- geographic location information for biometric samples;
- disaster victims and unknown deceased (such as homicide victims) identification records, including forensic dental records, nonphotographic imagery (such as x-rays, sonograms, orthodontic 3D cast models), implanted medical device identifiers, and more;
- cheiloscopy (lip prints);
- patterned injuries (such as possible bite marks or whip marks);
- voice-recognition data; and
- additional encoding formats, such as XML.

NIST also continues to work extensively with other organizations that develop biometrics standards, including the International Organization for Standardization (ISO), the Organization for the Advancement of Structured Information Standards (OASIS), the International Committee for Information Technology Standards (INCITS), the American Dental Association (ADA), and the International Civil Aviation Organization (ICAO).

The introduction of e-passports exemplifies the importance of working with these organizations. An e-passport includes a chip with biometric and biographic data in it. NIST worked with INCITS and ISO to develop the ISO standards for face images, fingerprint data, and iris images that ICAO incorporated in its e-passport specifications. At the US Department of Homeland Security's request, NIST also participated in trials of e-passport chips and data based on these standards.¹⁵ These efforts are making passports reliable and practical throughout the world.

NIST developed the Federal Information Processing Standard (FIPS) standard to which the Personal Identity Verification (PIV) credential issued to US government staff and contractors conforms.¹⁶ Each PIV card contains fingerprint data, and its chip can store additional biometric data that meets NIST specifications. The card is used for both logical and physical computer access control. NIST initially published PIV specifications in 2005. A July 2013 revision added capabilities for using iris data and on-card fingerprint matching.

NIST Goals

In testimony before the US House of Representatives in May 2013, Charles Romine, the director of the Information Technology Laboratory (ITL) at the US National Institute of Technology and Standards (NIST), summarized the organization's role in responding to government and market requirements for biometric standards.¹ By collaborating with other federal agencies, academia, and industry partners, NIST aims to

- support the timely development of biometric standards;
- develop the required conformance-testing architectures and tools to test implementations of selected biometric standards;
- research measurement, evaluation, and standards to develop and advance the use of biometric

technologies including multimodal techniques and emerging identity-determination technologies from video; and

- develop common models and metrics for identity management, critical standards, and interoperability of electronic identities.

References

1. *The Current and Future Applications of Biometric Technologies*, Joint Hearing before the Subcommittee on Research, Committee on Science, US House of Representatives, 113th Congress, testimony of C. Romine, 21 May 2013, pp. 164–172; www.gpo.gov/fdsys/pkg/CHRG-113hhrg81193/html/CHRG-113hhrg81193.htm.


Conformance testing is another important aspect of standardization. Fernando Podio and his NIST team supported this work by developing a suite of test tools for both the ANSI/NIST-ITL standard and selected ISO biometric standards.

NIST also performs tests of vendor products that implement wavelet scalar quantization (WSQ) compression. The FBI lists the WSQ-related products that pass the testing procedure.

NIST has several Guidance Groups for forensics that bring together experts in their fields. Of particular interest to biometrics are the Scientific Working Group for Disaster Victim Identification, Scientific Working Group on Friction Ridge Analysis,¹⁷ Facial Identification Scientific Working Group, and Scientific Working Group on DNA Analysis Methods.

Finally, the NIST Biometrics Laboratory Accreditation Program¹⁸ enables manufacturers, vendors, and customers to verify that products conform to published standards and produce a usable biometric output. The program accredits laboratories that test biometrics products for standards conformance, interoperability, technology performance, and operational and usability scenarios.

NIST foresees a future where it will continue to work with its Federal Government partners and with academia and industry to further strengthen the scientific foundation and improve the practical, operational capabilities of systems for biometrics and for human identity forensics through research, challenges, and the development of best practices and standards (see

the “NIST Goals” sidebar). As new issues arise in these fields, NIST will continue, through the ongoing work of its Information Technology Laboratory, to provide unbiased, effective, and timely analysis. 

Acknowledgments

Certain trade names and company products are mentioned or identified in the text. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor does it imply that the products are necessarily the best available for the purpose.

References

1. J. Schooley, *Responding to National Needs: The National Bureau of Standards Becomes The National Institute of Standards and Technology 1969–1993*, NIST Special Publication 955, 2000, p. 139.
2. R.T. Moore and J.R. Park, “The Graphic Pen: An Economical Semiautomatic Fingerprint Reader,” *Proc. 1977 Carnahan Conf. Crime Countermeasures*, Carnahan House, Apr. 1977, pp. 59–62.
3. J.H. Wegstein, J.F. Rafferty, and W. Pencak, *Matching Fingerprints by Computer*, NBS tech. note 466, July 1968.
4. D. Pallett, “A Look at NIST’s Benchmark ASR Tests: Past, Present and Future,” *Proc. IEEE Workshop on Automatic Speech Recognition and Understanding (ASRU 03)*, IEEE, 2003, pp 483–488.
5. *ANSI/NBS-ICST 1-1986, American National Standard for Information Systems: Fingerprint Identification—Data Format for Information Interchange*, ANSI, 25 Aug. 1986.
6. *ANSI/NIST-ITL 1-2011 Update: 2013, American National Standard for Information Systems: Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*, NIST Special Publication 500-290, Rev. 1, 2013.

NIST CONTRIBUTIONS TO IT

7. *Biometrics in Government Post 9/11*, tech. report, Nat'l Science and Technology Council, Aug. 2008; www.fas.org/irp/eprint/biometrics.pdf.
8. C. Wilson et al., *Studies of Fingerprint Matching Using the NIST Verification Test Bed (VTB)*, NIST Interagency Report 7020, 2003.
9. R. Moore, "Automated Fingerprint Identification Standard and Performance Benchmarks," *Proc. Ann. Int'l Symp. Latent Prints*, Nat'l Criminal Justice Reference Service, 1987; <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=113517> (abstract only).
10. E. Tabassi, C. Wilson, and C. Watson, *Fingerprint Image Quality*, NIST Interagency Report 7151, Aug. 2004; ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7151/ir_7151.pdf.
11. P.J. Phillips, "Improving Face Recognition Technology," *Computer*, vol. 44, no. 3, 2011, pp. 96–98.
12. P. Grother et al., *Performance of Iris Recognition Algorithms on Standard Images*, NIST Interagency Report 7629, NIST, 30 Oct. 2009.
13. M. Theofanos et al., *Effects of Scanner Height on Fingerprint Capture*, NIST Interagency Report 7382, Dec. 2006.
14. S. Orandi and R.M. McCabe, *Mobile ID Device Best Practice Recommendation Version 1.0*, NIST Special Publication 500-280, Aug. 2009.
15. B. Wing, *e-Passports Interoperability Test Session July 27–29*, Dept. Homeland Security US-VISIT (United States Visitor and Immigrant Status Indicator Technology) Program Report, Department of Homeland Security US-VISIT Program, Aug. 2004.
16. NIST Information Technology Lab Computer Security Division (NIST-ITL-CSD), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Fed. Information Processing Standards Publication FIPS PUB 201-1, Mar. 2006.
17. Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST), *The Fingerprint Sourcebook*, Nat'l Inst. Justice, Aug. 2011.
18. B. Moore and M. Iorga, *National Voluntary Laboratory Accreditation Program: Biometrics Testing*, NIST Handbook 150-25, July 2009.

Brad Wing is biometrics standards coordinator for the National Institute of Standards and Technology. Contact him at brad.wing@nist.gov.

ADVERTISER INFORMATION

Advertising Personnel

Marian Anderson: Sr. Advertising Coordinator
Email: manderson@computer.org
Phone: +1 714 816 2139 | Fax: +1 714 821 4010

Sandy Brown: Sr. Business Development Mgr.
Email: sbrown@computer.org
Phone: +1 714 816 2144 | Fax: +1 714 821 4010

Advertising Sales Representatives (display)

Central, Northwest, Far East:
Eric Kincaid
Email: e.kincaid@computer.org
Phone: +1 214 673 3742
Fax: +1 888 886 8599

Northeast, Midwest, Europe, Middle East:
Ann & David Schissler
Email: a.schissler@computer.org, d.schissler@computer.org
Phone: +1 508 394 4026
Fax: +1 508 394 1707

Southwest, California:
Mike Hughes
Email: mikehughes@computer.org
Phone: +1 805 529 6790

Southeast:
Heather Buonadies
Email: h.buonadies@computer.org
Phone: +1 973 304 4123
Fax: +1 973 585 7071

Advertising Sales Representatives (Classified Line)

Heather Buonadies
Email: h.buonadies@computer.org
Phone: +1 973 304 4123
Fax: +1 973 585 7071

Advertising Sales Representatives (Jobs Board)

Heather Buonadies
Email: h.buonadies@computer.org
Phone: +1 973 304 4123
Fax: +1 973 585 7071