International Biometrics+Identity Association

NIST Reauthorization Proposals

House Committee on Science, Space, and Technology

We suggest the following biometrics and identification areas for specific inclusion in the NIST Reauthorization

- Expand focus and testing, including accuracy and demographic performance, on non-contact biometric technologies to meet urgent public health and safety needs that covid-19 has disclosed:
  - Contactless fingerprints
  - Facial recognition
  - Iris recognition
- Develop specifications so that non-contact biometrics are considered the functional equivalent to those using contact fingerprints along with providing Federal Agencies the specifications needed to certify these non-contact methods as acceptable for their systems

Draft additional language:

SEC X. BIOMETRIC IDENTIFICATION RESEARCH

(a) RESEARCH - The Secretary, acting through the Director, shall continue to conduct and expand research, including the convening of experts in public and private sectors, to support and expand **(i)** improved understanding of the relative effectiveness of the full range of modalities of human identification; **(ii)** the protection of public health through collection devices that do not require sensor contact or physical contact; **(iii)** the positive identification of known criminals, terrorists, military and intelligence threats; and **(iv)** the forensic investigation of criminal activities with known error rates and with significantly reduced false positive and negative identification rates, through –

(1) Development of technologies to ascertain public health threats which do not require physical contact, reducing the risk of spreading contagion during epidemics;
(2) Improvement in the accuracy and demographic performance of face recognition technology to enhance human facial recognition;

(3) Convening experts in the public and private sectors to advance the understanding of the achievable identification performance of biographic descriptors, tokens, pagers and other personal electronic devices;
(4) Conducting recurring testing of principal existing biometric identification modalities such as fingerprints, iris, face, vein as well as emerging identification modalities.

(b) STANDARDS COORDINATION – The Secretary, acting through the Director, shall assure that the appropriate Institute staff consult regularly with standards developers, members of the biometrics and identification industry, institutions of higher education, and other stakeholders in order to facilitate the adoption of non-contact standards for human identification; image quality assessment of fingerprint, iris, face, and vein biometric modalities; objective and metrics based comparison of forensic identification imagery; and appropriate thresholds for automated determinations of matches, non-matches, and referral to human examiners for determination that are based on the research and testing results and other information developed by the Institute.

(c) ACQUISITION SUPPORT – The Secretary, acting through the Director, shall continue to develop methods for automating vendor testing of non-contact biometric technologies. Within 180 days of enactment of this Act, the Secretary shall submit a report to the appropriate Congressional Committees that assesses additional internal processes, authorities, and resources necessary to incorporate vendor testing into the federal non-contact biometric technology acquisition decision-making processes.

(d) FUNDING – The Secretary of Commerce shall devote $5,000,000 to carry out this section for fiscal year 2021, subject to the availability of appropriations . . . This section shall be carried out using funds otherwise appropriated by law after the date of enactment of this Act.

Need for Contactless Biometric Identification Solution

1. Non-Contact Fingerprint Capture Devises

We have learned from the COVID-19 pandemic that viruses linger on surfaces, at infectious titer levels, for days.[1] [2] A variety of Federal, State, and Local identification programs mandate fingerprint supported criminal history checks. Currently, only contact collected fingerprints may

[1] Aerosol and Surface Stability of SARS-CoV-2 as Compared with SARS-CoV-1, The New England Journal of Medicine, March 17, 2020, https://www.nejm.org/doi/full/10.1056/NEJMc2004973
[2] Persistence of coronaviruses on inanimate surfaces and their inactivation with biocidal agents, G. Kampf, et. al., Journal of Hospital Infection, January 31, 2020, https://www.journalofhospitalinfection.com/article/S0195-6701(20)30046-3/fulltext

be used for such checks. Transmission of disease from such checks is, under normal circumstances, a negligible and acceptable risk. During epidemics and pandemics it is not.

On a typical day in 2019 there were just under 167,000 fingerprint supported background checks (59%) or criminal inquiries (41%). Week days are considerably busier than weekend days, averaging close to 202,000 transactions a day during the work week.[3] These numbers fluctuate from day to day, and year to year, with the busiest day on record hitting nearly 365,000 fingerprint checks.[4] Criminal inquiries come from roughly 24,000 locations[5], although most locations average only a few arrests, or other submissions, per day, and continue to rely upon rolled ink on cards for arrest processing.

There are, however, several thousands of LiveScan fingerprint devices in use by law enforcement and many see heavy use. The peak use occurs at major cities and regional jails. For example, NYPD central booking, averages more than 142 fingerprinting sessions a day[6]. Civil applicants (positions of trust, licensing, Pre✓, TWIC cards, Global Entry cards, etc.), on the other hand, are largely processed by channeling agencies. The FBI has thirteen approved Channelers[7] offering services at 1701 locations[8] using LiveScan equipment, with mobile enrollment service an available option[9]. Considering the sheer daily volume of activity, even with numerous enrollment locations, many people touch the same sensors each day.

While LiveScan devices are supposed to be cleaned between uses, there is plenty of image quality evidence that indicates, in the past, this has often not happened. At high volume locations it is impractical. On a typical day a large number of people inevitably risk infectious disease while applying for a job or being processed following arrest.

It does not have to be this way. There are non-contact fingerprint capture devices that have proven highly effective for access control. While non-contact fingerprint capture is not approved for operational use, NIST has been studying non-contact devices to assess the prospects for operational use and to develop appropriate standards and certification procedures. To date, this analysis has extended over more than four years. NIST has shared test results with industry partners that indicate performance comparable to Fingerprint Acquisition Profile (FAP) devices approved for mobile/field operational use.

---

[3] Next Generation Identification (NGI) System Status Report, Staff Paper Topic #25, National Crime Prevention and Privacy Compact Council, Compact Council Meeting, Kansas City, Missouri, November 6-7, 2019

[4] November 2019 Next Generation Identification (NGI) System Fact Sheet, https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view

[5] ORI Directory, National Law Enforcement Telecommunications Systems, U.S. Department of Justice, Law Enforcement Assistance Administration, Washington, D.C. 20531, March 4, 1981, https://www.ncjrs.gov/pdffiles1/Digitization/75873NCJRS.pdf

[6] Adult Arrests: 2009-2018, Division of Criminal Justice Services, New York State, https://www.criminaljustice.ny.gov/crimnet/ojsa/arrests/index.htm

[7] https://www.fbi.gov/services/cjis/identity-history-summary-checks/list-of-fbi-approved-channelers-for-departmental-order-submissions

[8] https://www.fingerprintzone.com/fingerprinting-locations.php

[9] https://www.identogo.com/pcmobile

Existing standards and certification procedures were originally developed to convert inked cards to digital format for use in Automated Fingerprint Identification Systems (AFIS). Inked impressions are obtained by rolling the individual fingers against the card, and also taking plain impressions of the four fingers joined of each hand and of the two thumbs. When devices for direct electronic capture of fingerprints were developed, the identical procedures were used with minor modifications to the standards and certification procedures as needed. While the fingers are three dimensional objects, the standards and processes all stem from a time when only two dimensional fingerprint cards were used. They work well.

During an epidemic they also pose a significant risk to public health. There is an urgent need for NIST to develop standards and certification processes, to enable the use of non-contact fingerprint collection to a level of certification for presentation to existing Federal fingerprint systems such as FBI's NGI system and DHS OBIM IDENT. Additional financial resources, and injection of a sense of urgency, needs to be provided to NIST and the various agencies employing contact fingerprint technology today, to enable the use of non-contact fingerprint collection techniques in the near future.

2. Improvement of facial recognition accuracy and demographic performance

There are other biometric modalities used for identification, including more than 50 years of sustained R&D into automated recognition and identification of faces. The most recent and consequential two decades of research has been significantly supported by NIST. It has paid off in a number of algorithms that are more than 99% accurate for portrait style applications, and operationally useful for a broad range of other matching scenarios. For a couple of these algorithms, recognition and identification accuracy across broad demographic categories is also better than 99%. The best algorithms have been shown to perform significantly better than all human groups on identification and verification tasks.

This is singularly important as all, but the blind, are long accustomed to using faces for identification. The face is a primary means to identify family, friends, and acquaintances and always has been. Research has shown that the fusion of algorithms with human examiners can deliver near perfect accuracy, although as yet the requirements are such that it does not practically scale.

For many law enforcement investigative applications, access control, and immigration applications these algorithms prove their worth daily. For some other applications, where relatively small galleries of subjects are involved such as international air entry and exit, a hybrid of automation and referral of questionable results to human officials for determination has proven in pilot testing to be operationally highly effective.

Notwithstanding this progress with Face Recognition Technology (FRT), unlike with friction ridge (fingerprints, palm prints, etc.) and iris modalities, the community of interest does not

believe that sufficient research and validation has been done to pass a Daubert test, the standard for testimony in federal courts. The face modality is not yet ready for positive identification, where erroneous actions might be taken with significant adverse consequences for the subjects. Yet, most experts believe it could be with additional research and development. As we daily see the horrible consequences of not following social distancing recommendations, the prospect of advancing FRT to allow positive identification becomes compelling.

Face identification has been used by law enforcement, with mugshots and rouges galleries, almost since invention of the daguerreotype in 1839. The New York Times reported on a "Daguerreotype Gallery of Criminals at the Detective Police Office" on December 5, 1857. The photo identification card appears to have been first used at the 1876 Centennial Exhibition in Philadelphia but did not become widely used until the 20th century.

US Passports were required to include photographs of the bearer beginning in 1914, and in 1920 the League of Nations standardized the international passport book with a photograph required. Photographs were added to California driver licenses in 1958, gradually adopted by other States, and today are standard in all US driver licenses, although 13 states do allow an exception for religious reasons. The shape and size of identity cards was internationally standardized in 1985. Comparison of the photograph on an identity document, typically a driver license, to the bearer, to establish identity has become universal.

Because we use facial recognition from birth to identify family, friends, and later celebrities of various types, most people believe this is a natural and effective mode of identification. Yet, despite near universal opinion to the contrary, humans are generally not proficient at identifying unfamiliar persons. Not even at comparing recent photographs to a person in front of them. Even highly experienced and trained personnel are only about 85% accurate.[10] A recent, and rigorous, examination amplified this point.[11]

A distinguished group of researchers examined the performance of highly trained forensic face examiners, facial reviewers trained to perform faster and less rigorous identifications, "superrecognizers" (*untrained people with strong skills in face recognition*), professional fingerprint examiners but without face examination training, and undergraduate students as a proxy for the general public. Image pairs were presented for up to 30 seconds, or until a match/no-match decision was made, whichever was less. This scenario is comparable to what is expected of immigration officers, passport and visa examiners, and indeed all persons comparing an identification document to the person presenting it.

Median match accuracy, from most to least accurate, was:

---

[10] White D, Kemp R.I., Jenkins R., Matheson M., Burton A.M., Passport Officers' Errors in Face Matching, PLOS ONE, August 18, 2014 https://doi.org/10.1371/journal.pone.0103510

[11] Phillips P.J., et. al., Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms, Proceedings of the National Academy of Sciences, June 12, 2018, https://www.pnas.org/content/115/24/6171

- Facial examiners (0.93)
- facial reviewers (0.87)
- Superrecognizers (0.83)
- Fingerprint examiners (0.76)
- Students (0.68)

All groups, except student proxies, had one to a few members with perfect accuracy. All groups had one to many members with less than 60% accuracy. Performance, of even the best group, was far from satisfactory in those situations where the subjects face adverse consequences.

Scientists have more than 50 years of experience studying the effects of race on human face recognition ability.[12] People recognize faces of their "own" race more accurately than faces of "other" races. A 2001 study found that participants "were 1.56 times more likely to falsely identify a novel other-race face when compared with performance on own-race faces."[13]

As facial recognition is a nearly universal activity, critical to much of societal functioning, and unaided humans are proven to not perform it well with unfamiliar persons, a key question becomes can technology reliably aide human performance. Beginning in 1993 and continuing to the present, the Army Research Laboratory, then NAVSEA Dahlgren, and since 2002 the NIST have pioneered the "development of automatic face recognition capabilities that could be employed to assist security, intelligence, and law enforcement personnel in the performance of their duties."[14]

Beginning in mid-2017 for Verification (1:1 comparison of images) and late 2019 for Identification (1: N comparison where N is a large gallery), NIST has conducted ongoing testing of voluntarily submitted algorithms with reports and updates roughly monthly. Over the 27 years of research, progress has been extraordinary. As of March 2020:

- The best performing Verification algorithm, on a 100,000-person gallery of Visa quality photographs, at a false match rate less than 1 per million, had a false non-match rate of 0.0026 (99.74% accuracy); Twenty eight algorithms had better than 99% accuracy.

- Identification is a much more challenging technical problem, but here too progress has been extraordinary. Again, as of March 2020 the best performing Identification algorithm, on a 6 million-person gallery of frontal mugshot images, at a false match rate of 1 per thousand, had a false non-match rate of 0.0054 (99.46% accuracy). Only two algorithms had accuracy better than 99%, but eleven were more than 97% accurate.

---

[12] Accuracy comparison across face recognition algorithms: Where are we on measuring race bias?, Cavazos J.G., et. al., arXiv:1912.07398v1, 16 December 2019, https://arxiv.org/pdf/1912.07398.pdf
[13] Thirty Years of Investigating the Own-Race Bias in Memory for Faces: A Meta-Analytic Review, Meissner C.A. and Brigham J.C., Psychology Public Policy and Law, March 2001, https://psycnet.apa.org/doi/10.1037/1076-8971.7.1.3
[14] Face Recognition Vendor Test (FRVT), https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

- Companion reporting on Demographic Effects, from December 2019, reported an algorithm with “undetectable” false positive differentials. On the most demanding demographic comparison, where gender, country of birth, and age cohorts were roughly equal size and comparisons limited to that group, at a false match rate of 1 per 100,000 thousand, the top 50 performing algorithms had false non-match rates less than 0.04 (96% accuracy).

As demographic effects have only recently become a significant focus for research, and adequate galleries of subject images and essential metadata do not exist outside government, NIST is uniquely positioned to aide and advance performance in this area.

3. Iris Recognition

The iris modality also has sufficient accuracy for use in positive identification. It is, however, not widely used because identification systems require a reference gallery of known persons with the biometric on file. Few iris galleries, with the needed accompanying biographic information, exist. Those that do are small compared to fingerprint and face holdings and it is important to enable building up this iris database.