FEDERAL NEWS NETWORK

EXECUTIVE BRIEFING SERIES:

Biometrics and Government Transformation

Sponsored by NEC

BORDER PATROL
VISA

Facial recognition technology goes faster and lighter

BY TOM TEMIN

Frictionless motion through public spaces, ease of exit and entry of trusted personnel in sensitive federal facilities, better service to the flying public when it comes to going in or out of the country or a busy international hub, and online transactions by citizens. These are among the use cases for which federal agencies are adopting or planning to adopt facial recognition.

This occurs as elastic cloud computing, artificial intelligence and Internet of Things technologies are combining to enable a new generation of biometric applications and rev up legacy ones. Facial recognition algorithms are constantly improving, too, helping developers sidestep skewed or biased results they might have gotten earlier.

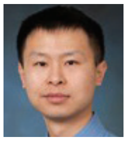
Challenges remain. Thanks in part to sensational stories, some distrust facial recognition, which has also sparked attention in Congress. Data sets robust enough to test powerful algorithms can be difficult to obtain. Without carefully vetted test data, algorithm selection, and transparent test procedures, the risk of uneven or biased matching results remains. Facial data must always be handled in conformance to myriad privacy laws and regulations.

To delve into the latest thinking on facial recognition and its application in federal settings, Federal News Network and NEC Technologies convened a roundtable of program, oversight and standards professionals to discuss the issues.

PANEL OF EXPERTS

Dr. Angela Landress, Program Manager, Cyber Innovation Office, Defense Information Systems Agency

Sung Ha, Officer and Program Manager, Entry/Exit Transformation Office, U.S. Customs and Border Protection



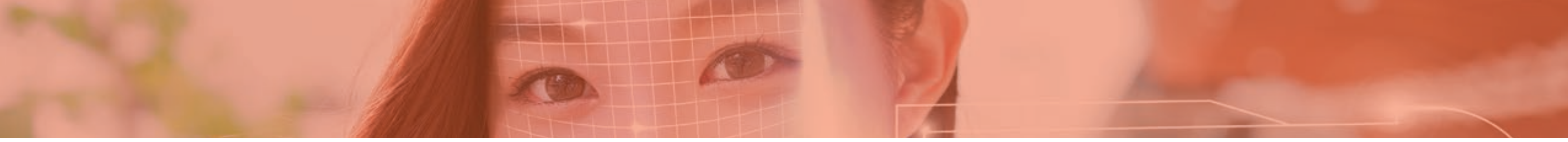
Dr. Shuowen (Sean) Hu, Electronics Engineer, Army Research Lab

Benji Hutchinson, Vice President, Federal Operations, NEC Corporation of America

Ryan Koder, Branch Chief, System Business Operations, Office of Biometric Identity Management, Department of Homeland Security

Dr. Tim Persons, Chief Scientist, Government Accountability Office

Dr. P. Jonathon Phillips, Electronic Engineer, Information Technology Laboratory, National Institute of Standards and Technology



Compelling use cases

As the technology evolves, agencies are finding facial recognition applications that enhance their missions.

For example, at U.S. Customs and Border Protection (CBP), facial has become the “primary modality” for moving people in airports, according to Sung Ha, officer and program manager in the Entry/Exit Transformation Office.

“As technology advances, we’ve found a way to streamline the process for passengers.” Unless required by statute or some extenuating circumstance, fingerprints aren’t even required any more, Ha said.

Ha said the facial recognition system also boosts the productivity of officers, who no longer need to do the visual matching themselves. Now it’s a matter of machines imaging a person and comparing a derived file to one derived from the passport photo. It frees officers to focus on their larger screening mission, what he termed “intent and purpose.”

“As this technology develops, the sky’s the limit,” Ha said.

At the Defense Information Systems Agency, where users routinely handle sensitive data, facial enables device authentication in a zero-trust security architecture.

Dr. Angela Landress, program manager in DISA’s Cyber Innovation Office, said, “We use machine learning algorithms to analyze a mix of contextual, behavioral and biometric factors to continuously authenticate users into devices.”

She noted ongoing research programs to ensure future efficacy of recognition algorithms and of mobile device-related applications. DISA engineers are testing the authentication on a widely used chip-set, which Landress said could lead to wider deployment across the Defense Department.

Electronics Engineer Shuowen Hu, of the Army Research Lab, described work to extend facial recognition to difficult tactical situations, including nighttime and other low-light situations, and from long distances.

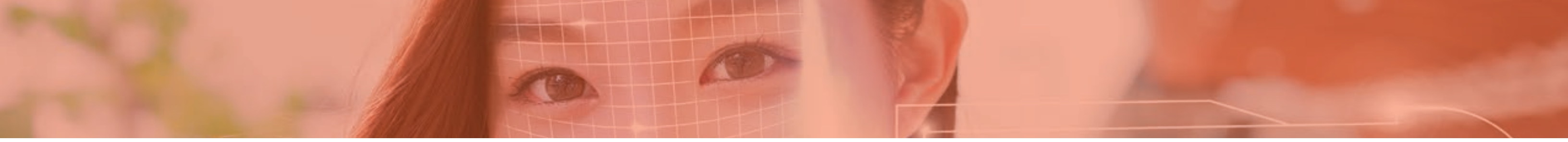
The fundamental capability his group seeks is to take an infrared image “and be able to develop the artificial intelligence and machine learning algorithms to match it against traditional watch lists or galleries.” Hu called the developing technology “cross-spectrum matching.”

Hu’s program is among many that are seeking light-weight algorithms that can execute in limited compute power, Internet of Things devices.

Benji Hutchinson, the vice president of federal operations of NEC Corporation of North America, said these applications demonstrate the maturation of biometric algorithms and surrounding technologies. And, not to be overlooked, falling price points.

“We’re seeing around the world,” Hutchinson said, “a maturation of biometrics in general. You’re seeing a deeper integration across platforms and across use cases.” The result? “More users are becoming habituated with the technology. It’s becoming more commonplace.”

What was nearly science fiction a decade ago is a common app on smart phones, Hutchinson



said. He echoed the Army's Hu in predicting facial recognition will move to the network edge on IoT devices, "where it requires less and less code" without sacrificing accuracy or performance.

Privacy, bias and data

Biometrics applications, especially facial recognition, require care in design and deployment. Risks come from a variety of sources.

Some are technical. Any given algorithm — and there are many to choose from — might contain a bias such as inflated false negative or false positive percentages for certain facial types. An agency might have chosen an incomplete data set to train an algorithm. Or it may not have done a complete enough validation of the machine learning exercise.

Experts say stories of bias are overblown, and that bias can be neutralized.

"We process numerous ethnicities, numerous skin colors." CBP's Ha said. But rigorous testing has resulted in a system in which "thus far, our matches are doing very well when it comes to all the races, all the skin tones, all the ethnicities." This is true, Ha said, even at an airport like Dulles International when planes from Europe, Africa and the Middle East all land at the same time and send thousands of people through CBP facilities.

Ha and others said the use of combined algorithms can overcome biases that might be introduced by any one of them. "One algorithm may be biased in one direction. Another might be biased in another direction. As we proceed forward, fusion of different algorithms will become much more common," he said.

Whether it's accounting for various facial characteristics and skin colors, or other variables such as atmospheric distortions from long-distance recognition, recognition in low light, or one-to-many comparisons when the many might be small or blurry as in video surveillance, data is an important ingredient in remedying false or unreliable outcomes.

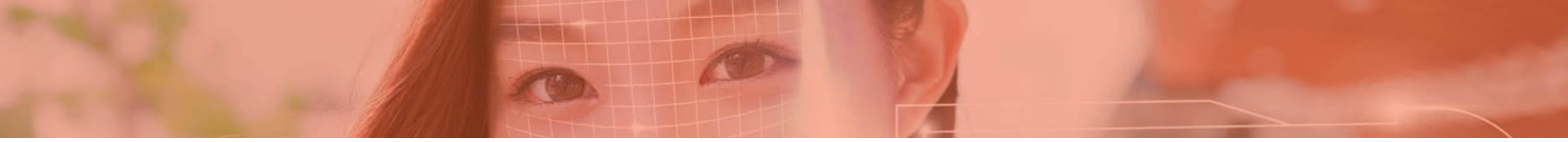
Said the Army's Hu, in such situations "how do you train the algorithm to be robust? You need appropriate data to train these algorithms."

Obtaining sufficient training data is becoming more difficult because of privacy concerns. Dr. P. Jonathan Phillips, an electronic engineer in NIST's Information Technology Laboratory, said how to obtain sufficiently large and diverse sets of faces to train algorithms is the subject of ongoing research. He said the use of public figure and celebrity faces available on the Internet means "we are really good at matching celebrities."

Phillips added, "The computer vision community is working on what it calls augmented data. There are many situations where you can't get tens of millions of samples either ethically or they don't exist." A technique called augmented data holds promise, he said, by expanding the range of "faces" in a sample using artificial means.

Hutchinson said when imagery becomes dicier, the problems of matching "are much nastier, requiring a different set of mathematics and approach. That's where artificial intelligence has helped out and where it will continue to help out."

Other facial recognition challenges are regulatory or legal. Agencies must do privacy impact



assessments. They must demonstrate security assurance of data they use for testing and in production.

For Dr. Tim Persons, chief scientist of the Government Accountability Office, “context is incredibly important” to the policies agencies apply to biometric programs and to how they conduct privacy impact studies. He added that a concern in Congress is that “computational forensics,” such as biometric identification, are executed in a way that is transparent.

“That does matter greatly,” Persons said, “the quality of the data and the way in which you validate the algorithms.” He said GAO urges agencies to avoid going too quickly from development of computational forensics systems to operation deployment “without the crucial re-risking” first. “It takes time but it’s worth it for this technology, which is high-risk, high-reward, high-consequence.”

NIST, Persons and Phillips noted, is another source on both technical and compliance topics. Phillips, who’s been working in facial recognition for 25 years, said in his time at NIST, the error rates in facial matching have been halving every two years.

He cited work in the criminal investigation field showing that certain people known as super-recognizers can match the accuracy of modern algorithms, “and when we fused them together we got even better performance. So the role of the average human in the [facial recognition process] is something that needs to be investigated.”

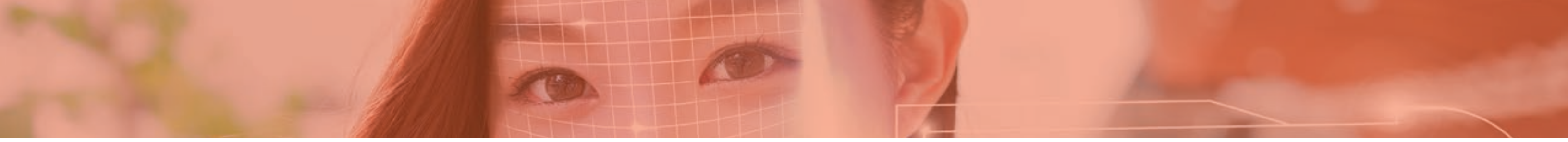
Solid supporting infrastructure

The governmentwide move to adopt elastic cloud computing and other new infrastructure technologies has become an enabler of facial recognition applications.

A case in point is the Homeland Security Department. Ryan Koder, branch chief for system business operations in the Office of Biometric Identity Management, said his program, known as IDENT, has moved away from government-owned data centers.

“IDENT started in the ‘90s and has been modernized over time,” Koder said. Now DHS is building a cloud system to replace government-owned compute and storage. “It’s called Homeland Advanced Recognition Technology, and we’re building it fully within AWS GovCloud,” Koder said. “That will give us increased efficiency from a management perspective, lower operations and maintenance costs long term, and we’re not going to be buying hardware to put inside a rack space when we want to do something else or increase our compute power.”

He cited a hypothetical increase in accuracy of biometics, which can slow performance in the absence of added processing power. This situation favors use of elastic cloud. Also, because biometric application loads are often highly cyclical, agencies can gain efficiencies by only paying the cloud provider when the application is running. The alternative is the cost of maintaining an idle data center during slow periods.



At DISA, Landress said, they're testing a cloud-enabled browser isolation technology prototype to protect data and prevent malicious code from running on mobile devices. Browser traffic goes to a cloud provider, which returns to the user video-like representation of the results.

Hutchinson said NEC's own matching and recognition algorithms run in a commercial cloud. When combined with, for example, CBP applications, this setup allows multiple instances to be "spun up" as needed, avoiding the need to squeeze data facilities into space-constrained airports.

For the military, cloud computing isn't necessarily the answer to all biometric or any other applications. That's because warfighters are likely to operate in austere environments often with low or spotty connectivity, rendering cloud reach-back an iffy proposition.

The Army's Hu said that results in more reliance on local hardware. The Army, he said, is seeking edge — as opposed to cloud — processing in very lightweight equipment that can be carried by a soldier.

Continued refinement of algorithms has led, in some cases, to reductions in the file sizes required for recognition to work, in turn easing the storage and network bandwidth requirements.

Koder of DHS said, extraction templates required by the algorithms are also shrinking. "At one point it was how much information could you get into the templates from the images," he said. "It's gone the complete other direction of finding the smallest templates. It's completely changed the performance landscape. Template size is bytes, where it used to be kilobytes." This is what allows, in applications such as airport entry/exit, two-second matching of low resolution camera images with passport photos.

In summary, for facial recognition, algorithms and data are getting faster, lighter and more accurate. But challenges remain in obtaining sufficient datasets to properly train them. Artificial intelligence leading to augmentation of smaller data sets holds promise here.