Acceptance speech

19 June 2025

Anil K. Jain, awardee in the Information and Communication Technologies category (17th edition)

With deep gratitude and humility, I accept the 17th BBVA Foundation Frontiers of Knowledge Award in the Information and Communication Technologies category for my contributions to pattern recognition with applications to fingerprint recognition.

If you examine your fingertips closely, you will see a beautiful pattern of interleaving ridges and valleys. These ridge-valley patterns — called "friction ridge patterns" — are also present on our palms and the bottoms of our feet. Humans have long been curious about these patterns. In fact, archeological artifacts were found to have thumbprint impressions of the artisans on them and thumbprints are still accepted as signatures on legal documents in many countries.

Fingerprint recognition is the act of authenticating or identifying an individual based on their fingerprints. This idea was initially driven by law enforcement needs. The *Habitual Criminals Act* of 1869 formalized the identification of repeat offenders, grounded in the premise that fingerprints are both *unique* and *permanent*. Scotland Yard adopted fingerprint identification in 1905, as did the FBI in 1924. The identification was conducted manually by trained experts.

The use of computers to recognize fingerprints did not emerge until 1980 when the first Automated Fingerprint Identification Systems became available. In 1990, I was presented with an opportunity to explore the topic of automated fingerprint recognition. When I took up this challenge, no one would have imagined that this research would help spawn the field of biometrics — the technology that identifies individuals based on body traits such as one's face, fingerprints, and the irises of the eyes. Today, biometrics has become commonplace, and it is being used by billions of people every day for various reasons — ranging from unlocking our mobile phones, to making payments, to boarding flights.

What has really changed in the past thirty years is the proliferation and scale of biometric systems. Today, the FBI's criminal fingerprint repository contains about 90 million records. Every country in the world also maintains such a database, which can be searched to find a person of interest. On September

11, 2001, the United States tragically faced its worst terrorist attack. In the aftermath, the United States Congress enacted the Enhanced Border Security and Visa Entry Reform Act of 2002 which allowed the use of fingerprint recognition for entry and exit of visitors to the United States. Most countries followed suit, and international travelers now encounter some form of biometric identification at airports to enhance security.

Biometric recognition has also been applied to prevent fraud, and improve user convenience. Examples include Disney Parks' use to stop ticket sharing, India's Aadhaar—a billion-scale biometric ID program empowering the underprivileged—and Apple's Touch ID and Face ID for unlocking phones and enabling mobile payments. The following statistics are phenomenal: Aadhaar processes over 80 million biometric authentications daily, and about 1 billion mobile phones shipped in 2024 with built-in biometric authentication.

Fortunately, some of my research contributions have played a significant role in enabling this enormous transformation. For instance, to reliably recognize billions of people, we must extract salient information from fingerprints and search for them efficiently. To accomplish this, we developed technology that represents fingerprint images containing hundreds of kilobytes of information, using a compact and salient feature set equivalent to a 24-character PIN, enabling rapid searches across databases of hundreds of millions of fingerprints in seconds.

We also developed sensors and methods to capture and recognize infant fingerprints to enable reliable identification for healthcare and immunizations.

Fingerprint recognition relies on the premise that fingerprints are unique and permanent. However, this was merely a conjecture until we developed statistical models to scientifically validate these claims.

Not surprisingly, the wide deployment of fingerprint recognition systems started attracting the attention of hackers and raised concerns about data privacy. For example, we must ensure that a finger presented to an authentication system is real and not an artificially crafted copy of a fingerprint, or a fingerprint which has been intentionally mutilated in an effort to evade identification as depicted in the movie "Men in Black". To counter such threats, we developed privacy-preserving fingerprint matching algorithms, as well as methods to detect artificial and altered fingerprints.

As seen on CSI, the crime scene investigation TV drama, smudgy and partial fingerprints found at crime scenes provide one of the most valuable clues to identify a suspect. We were able to make many algorithmic contributions for more accurate search with these prints, while minimizing wrongful apprehensions.

Across all of these applications of my research, one of the most gratifying aspects has been witnessing how these contributions have moved beyond the laboratory to make real-world impact. With growing world disorder, security threats, financial fraud, and economic disparity, identifying human beings reliably will continue to require biometric recognition.

Once again, I am humbled to receive this award.