COMPUTING CONVERSATIONS

Anil Jain: 25 Years of Biometric Recognition

Charles Severance, University of Michigan

Computer scientist Anil Jain discusses the evolution of the biometric recognition field.

Today, we don't think twice about swiping our finger to unlock a cell phone or walking into public areas where security cameras are performing real-time face recognition. If you turn on the television, you'll often see biometric technology such as fingerprint matching and facial recognition being used to solve crimes. The speed, memory, and sensors of today's computers make it feasible to use biometrics on a large scale. But it's taken decades of research to understand and build reliable and verifiable algorithms and techniques that underpin this high-stakes space.

I spoke with computer scientist and Michigan State University professor Anil Jain about the early days of biometrics and the field's future. You can see the entire interview at www.computer.org/computingconversations.

See **www.computer.org/computer-multimedia** for multimedia content related to this article.

In the 1980s and 1990s, when mainframes were less powerful than today's wristwatches, there was a lot of focus on developing efficient algorithms for pattern recognition and image processing. For pattern recognition to evolve into biometrics, significantly more computing power was needed for real-time recognition:

> *It was serendipity in 1990 when professor Duncan Buell called me from Washington, DC, and said, "You do good image processing work. The NSA [National Security Agency] has funded the development of an FPGA [field-programmable gate array]—we can give you an FPGA board and some research money. Can you find a civilian application for this hardware?" The FPGA board was called Splash 2 and was an attached processor for Sun SPARCstation hosts.*

Although the FPGA's computational model (an array of Xilinx 4010 FPGAs; see Figure 1) was much simpler than that of general-purpose computers, it was well suited to many basic low-level image-processing algorithms like convolution, smoothing, edge detection, and local filtering as well

0018-9162/15/$31.00 © 2015 IEEE

as high-level operations such as point matching. But once the algorithms were ported on Splash, the question arose of which application areas to target:

> *One possible application of higher-level operations such as point matching is stereo matching in computer vision. There's a left image and a right image, and you find some landmarks in the two images and align them to obtain a depth map. As we were brainstorming other applications for point correspondence, my graduate student Nalini Ratha and I really liked the idea of implementing fingerprint recognition in FPGAs because fingerprint matching is essentially based on point-matching operations.*

The complete solution to fingerprint matching involved a point-matching algorithm combined with low-level filtering operations to enhance fingerprint images that are often of low quality and a bit blurred when captured.

For Anil, an interest in image processing evolved into a 25-year interest in fingerprint recognition. It's rewarding when your latest research finds its way into the mainstream media:

> *If you watch any crime show on TV these days, like* CSI: Crime Scene Investigation*, they'll show a computer extracting the minutia points from a fingerprint and doing the matching instantly.*

But if you watch those shows, you know that the current generation of fingerprint technology is never enough to solve the crime. There's always the next innovation—both on TV and in research:

> *For the past 100 years, fingerprint matching has been based on minutia points [see Figure 2]. But what happens if the fingerprint image doesn't have a sufficient number of points or the image quality is so poor that we can't extract enough reliable points? That's when you need to look at the image texture formed by the ridges and valleys that characterize the fingerprint.*

In 1998, Anil's graduate students, Salil Prabhakar and Sharath Pankanti, came up with a bank of filters that captured the texture characteristics of a fingerprint that could be used for fingerprint matching. Seventeen years later, these texture-matching algorithms are finding their purpose:

Could we reissue a fingerprint representation similar to a credit card number that can be revoked and reissued?

> *The sensors for fingerprint readers in mobile phones are only about 80 × 80 pixels in size. If you only capture a small part of the fingerprint, the number of minutia points isn't enough to establish a correspondence between two different impressions. This is where the texture information becomes especially useful for fingerprint comparison.*

Although many research results from the biometrics field are widely used in authentication systems—ranging from unlocking a mobile phone to large-scale national ID programs like Aadhaar in India (https://uidai.gov.in/aapka-aadhaar.html)—there are still many new areas to explore. As more sensors are embedded in mobile devices, novel approaches to continuously authenticate a device's owner become possible:

> *The traditional model of authentication is that you log in once and then just use your device. But that model revolved around sitting in front of a desktop computer. On a mobile phone, this notion of "authenticate once, use forever" is really not appropriate, which is why we have to keep unlocking our phones. The typical person might unlock his or her phone 40 or 50 times a day. So why doesn't the device learn who you are based on your behavioral patterns, how you swipe the screen, how you hold it, and its GPS location, or even turn the phone's camera on once in a while and capture an image of your face for recognition?*

Another important research area is the uniqueness of biometric traits like your fingerprint, face, or iris:

> *In principle, every fingerprint has a different friction ridge pattern. There are approximately seven billion people living on Earth right now, so there are about 70 billion fingers. We should be able to discriminate between these 70 billion fingerprints, but it doesn't quite work this way in practice because the pattern on the finger could be quite different from the two-dimensional image of the finger you use for recognition.*

Fingerprint recognition systems and other biometric recognition systems have small non-zero error rates that depend on the quality of the acquired biometric data.

A fundamental premise of any biometric trait is its persistence. Will a fingerprint or iris pattern change over time?

It's generally agreed that facial recognition systems become less reliable when the separation between two facial images of the same person exceeds about 10 years or so. But in the case of a fingerprint or iris, we have been led to believe that they last forever.

Because Anil has worked with law enforcement officials for more than 15 years on a wide range of research questions, they sometimes come to him with new questions, ideas, and data to analyze:

Just recently, along with my former student Soweon Yoon, I completed a study on the persistence of fingerprint recognition using data from the Michigan State Police. They gave us fingerprint records of about 16,000 individuals who had been arrested multiple times over a 12-year period. Using a multilevel statistical model, we showed that fingerprint recognition accuracy over this 12-year period doesn't degrade.

But what happens if somebody steals data that contains your biometric trait?

Today, the image or representation of your fingerprint is stored in your mobile phone or local bank. How do we secure it so that even if your data is stolen, it can't be used to impersonate you? This isn't as farfetched as one might think. The recent attack on the federal Office of Personnel Management resulted in the theft of fingerprint images of more than one million individuals. Although there's a need to collect fingerprints, we should avoid retaining the original versions in operational databases. Could we reissue a fingerprint representation similar to a credit card number that can be revoked and reissued?

Biometrics is a fascinating and continuously evolving application area for computing technology. When biometric data is used in critical situations like solving high-profile crimes or authenticating large financial transactions, it's important to have solid research that ensures the reliability and accuracy of these biometric recognition algorithms. C

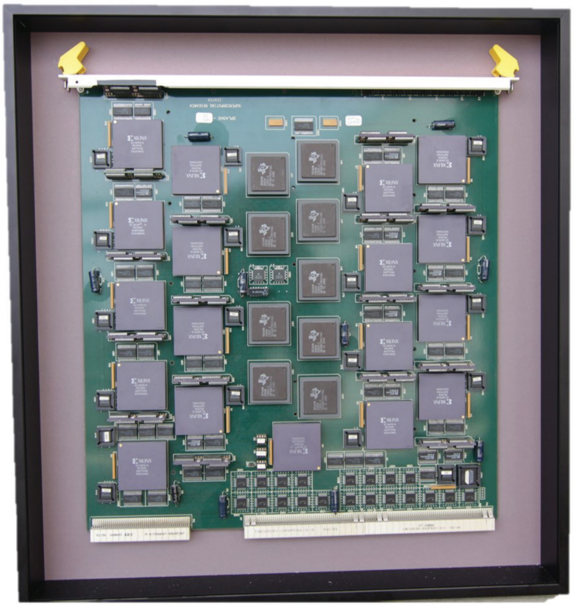

Figure 1. The Splash 2 board consisting of an array of Xilinx 4010 field-programmable gate arrays. A sequential point-matching algorithm (assuming an average of 65 minutia points per fingerprint) executed on a Sun SPARCstation 20 runs at 100 matches per second. The same algorithm implemented on Splash 2 running at 1 MHz executes at 6,300 matches per second. (Source: Duncan Buell, University of South Carolina.)

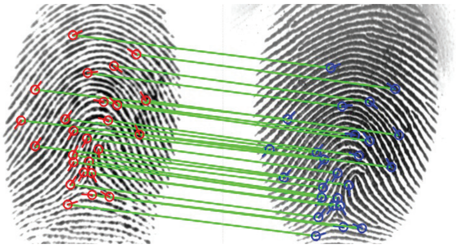

Figure 2. Two different fingerprint impressions (images) of the same finger, showing the corresponding minutia points. The number of paired minutiae is 25.

CHARLES SEVERANCE, Computing Conversations column editor and *Computer*'s multimedia editor, is a clinical associate professor and teaches in the School of Information at the University of Michigan. Follow him on Twitter @drchuck or contact him at csev@umich.edu.