NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Fall 2000 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

Biometrics in Corrections

Simply put, biometric identification is based on the statistical measurement of physiological characteristics. In this sense, biometrics is the science of using a particular biological aspect of the human body to recognize a person for security, attendance, or any other purposes for which proof of identity is required.

A buzzword right now, biometric identification actually has been around for a while. The most widely used biometric is fingerprints. But technological developments over the last decade have added DNA matching; iris and retinal scans; voice, handwriting, or facial recognition; and hand and facial geometry to the list of biometric identifiers.

"Biometrics is about access control," says Jim Wayman, director of the U.S. Department of Defense's (DoD's) National Biometric Test Center in San Jose. "Police can use it to control and track access to evidence lockers. Prisons are using it for access control of their own employees. At a prison in Glasgow [Scotland], the warden uses biometrics for officer control. Any prison officer coming to work for the first time that day has to go through a biometric screening gate and has to go out that gate at night when he leaves."

A survey of correctional facilities funded by the National Institute of Justice (NIJ) found few jails and prisons using biometric identification systems. Those that were used systems based on iris scans, hand geometry, and fingerprints. According to Dr. Al Turner, NIJ visiting scientist, the use of biometrics in corrections varies greatly, partly because it involves such new technologies and few correctional administrators are aware of what they are or how they can be utilized.

"One reason these systems are scarce [in correctional facilities] is that they are still new, relatively unknown, and untried," Turner says. "If you start relying on technology to identify someone in corrections, rather than person-to-person contact, you have to be sure the technology works. Corrections has demanding requirements, and the accuracy and reliability of biometrics technologies will have to mature before they will be implemented on a larger scale."

Biometrics Basics

Fingerprints are the most widely used biometric tool, but other methods of identification through biometrics are coming into general use, such as voice prints and iris scans. In addition, a number of other techniques—some quite unusual and a bit obscure—are still in the early development stage. For example, a company in the United Kingdom now holds the patent on a technology that will identify individuals based on blood vessel patterns in the back of the hand. Also in development are systems that analyze sweat pores on a fingertip, use infrared cameras to find "heat spots" created by veins and arteries in the face (known as "vascular tattoos"), or identify an individual based on his or her unique body odor.

The range of biometrics is as diverse and imaginative as the potential number of the body's scannable parts. The following techniques are the more common biometrics in use today.

Eye Scans. Eye scans can be categorized into two types: iris and retinal. Iris scans digitally process, record, and compare the light and dark patterns in the iris' flecks and rings, something akin to a human bar code. Some claim this technique is more accurate than a fingerprint and can be employed at such a distance that the person being scanned is unaware. Others say these systems can easily be fooled. Researchers testing one system discovered that university students who wore patterned "designer" contacts were wrongly rejected because the contacts were in a different position every time the students' eyes were scanned. Retinal scans, on the other hand, are more intrusive, requiring close-up infrared scanning through the pupil.

Facial Recognition. This biometrics technology is already in use at some border crossings. The term covers several different techniques, including video

Continued on page 2

One NIJ project hopes to push biometrics in that direction. NIJ is working with the DoD Counterdrug Technology Development Program on Facial Recognition 2000, a project that will assess various facial recognition technologies. Those technologies that appear feasible will be tested in a correctional facility to identify staff members. If a system proves successful, it will be used to monitor visitors.

A second project, still in the planning stage, will test biometrics as a way to monitor inmate movement. One possibility, Turner says, is to combine a biometric "key"—probably a fingerprint—and a smart card. "If you put a biometric key on a smart card, you then know that the inmate has the right card and isn't trying to use one that belongs to someone else."

A biometric identification system now in place can be found at the Sarasota County Detention Center in Florida, where iris scans are used to prevent former prisoners from visiting former inmate pals. In place less than 2 years, the system has more than 40,000 iris scans in its database and has logged 8 hits on former inmates trying to enter the prison under false identities.

In another correctional facility, hand geometry helps prevent escape attempts. The system scans visitors' hands as they enter and again as they leave to be sure prisoners are not posing as visitors or staff. The Federal Bureau of Prisons tested another system that uses hand geometry. Not only does it verify the identity of visitors, it helps officials track staff to avoid mistakenly identifying them as inmates and to positively identify them in a disturbance. Inmates use it for access to the cafeteria, recreation lounge, and hospital.

Regardless of the setting or situation, to be effective a system based on biometrics has to have certain characteristics:

- User friendly.
- Acceptable to the community.
- Affordable (in initial installation costs and in long-term operational and maintenance costs).
- Accurate.

A principal concern of utilizing a biometrics system in a correctional facility is the ability of that system to seamlessly integrate into the information and tracking systems already in place. The ability of the biometrics system to connect with databases at other agencies or organizations, known as interoperability, may also be an issue. In addition, biometric systems can create unforeseen problems. In one correctional facility, a system that used hand geometry to monitor visitors simply took too long.

Biometrics Basics *(continued)*

or photo imaging; thermography, which reads the heat pattern around the eyes and cheeks; and the ability to scan the dimensions of an individual's head. This type of biometric is not nearly so accurate as a fingerprint. A similar face or a change in lighting or appearance can confuse the system. The Defense Advanced Research Projects Agency, the central research and development organization for the U.S. Department of Defense, has created a program called Image Understanding for Force Protection (IUFP). This project grew out of the 1996 terrorist bombing of U.S. military barracks in Saudi Arabia, which killed 19 people. Its goal is to create new technologies to identify humans at a distance. One proposed system is modeled after a British system, which uses more than 200 cameras to keep an eye on foot traffic in the East London borough of Newham, "recognizes" known criminals, and alerts authorities.

Hand Geometry. This type of scan reads the outline or the shape of a shadow, not the handprint. It can be used for all types of access, but is not prized for its accuracy. Although it is a quick and sturdy method of verifying identity, too many people have similar hand shapes and sizes for such a system to be dependable in situations that need to be highly secure.

Voice Recognition. This technique has been used at border crossings. Voice, or speaker, recognition employs positive identification that, in this instance, verifies that the person crossing the border is the person already enrolled in the database. Some voice and speaker recognition techniques are highly susceptible to background noise and may not provide accurate verification if the speaker has a cold.

Handwriting and Signature Identification. In the area of identification by a person's handwriting, the U.S. Secret Service's Forensic Science Division has developed the Forensic Information System for Handwriting (FISH) based on work carried out by German law enforcement in the 1980s. FISH takes a block of text and then plots the handwriting as arithmetic and geometric values. Signature recognition programs, however, read signatures written on an electronic pad by measuring the speed, pressure, and direction of the strokes.

DNA Matching. DNA matching has become one of the most touted means of biometric identification during the last several years. In 1998, the FBI's Laboratory Division established CODIS (Combined DNA Index System), an electronic database of DNA profiles that can identify suspects, similar to the AFIS (Automated Fingerprint Identification System) database. Every State

Continued on page 3

"They already had this whole system in place to prevent escapes at visiting time," Wayman says. "They didn't release the visitors until all the prisoners were accounted for. They put waist straps and shoulder bands on the inmates that could only be removed by the guards. In the visiting room, they didn't let the prisoners change clothes or move from their assigned seats. So adding biometrics as an afterthought just didn't make sense. There was no added value. It was just one more hoop the prison officials had to jump through. The system was subsequently abandoned."

Although their use is somewhat limited and some systems are not yet foolproof, biometric identification technologies hold substantial promise for corrections and law enforcement. "I think the corrections field is at the lower end of the learning curve right now," Turner says. "But the more we can make people aware and educate them about biometrics, then the more likely that biometrics is going to become a useful tool."

For more information about biometrics development and testing and evaluation projects for law enforcement and corrections, contact the National Law Enforcement and Corrections Technology Center at 800–248–2742 or visit its World Wide Web site, JUSTNET, at www.nlectc.org.

Biometrics Basics *(continued)*

is in the process of implementing a DNA index of individuals convicted of certain crimes, such as rape, murder, and child abuse. Upon conviction and sample analysis, perpetrators' DNA profiles are entered into the DNA database. Just as fingerprints found at a crime scene can be run through AFIS in search of a suspect or link to another crime scene, DNA profiles from a crime scene can be entered into CODIS. Therefore, law enforcement officers have the ability to identify possible suspects when no prior suspect existed.

This article was reprinted from the Fall 2000 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.