BIOMETRICS

WHAT YOU SHOULD KNOW ABOUT ITS TECHNOLOGY

SECURITY INFRASTRUCTURE - ID CARDS AND READER

Identity Cards and all other specification including National Identity Cards - Driving Licenses - Security Cards with DATA Base and System Manager for issuing and Logging Control at Borders, Airports, Checkpoint with Direct Radio and Data Link to main Information Centre, Immigration, Police, Security Services and many other applications.

biometrics
Exhibition and Conference 2010

Conference: 19-21 October 2010 | Exhibition: 20-21 October 2010
Queen Elizabeth II Conference Centre, London, UK

GOVERNMENT APPLICATIONS

This is the best solution to Africa's **CORRUPTION, FRAUD, SECURITY, NATIONAL ID'S, DRIVER'S LICENSES**

"Biometric" means the measurement of a living, human characteristic". Biometric technologies measure characteristics such as fingerprints, voice recordings, irises, heat patterns, keystroke rhythms, and facial images comparing a person's unique characteristics against previously enrolled images for the purpose of recognition.

Overview

“Finger minutiae holds enormous promise. It offers a near-zero percent false rejection rate and is cost and memory-efficient. Finger memory is safe, repeatable and reliable, yet it does not infringe on consumer's privacy. Because it only requires installation of a compact direct finger reader at the Point of Sale, it is a "small footprint" solution, as opposed to hand geometry readers and iris or retinal scanning equipment, which typically can be both bulky and expensive."

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Biometric technology is a way to achieve fast, user-friendly authentication with a high level of accuracy. This presentation will highlight some of the benefits of using biometrics for authentication. Emerging applications, both within the Government and industry, will be discussed. Also presented will be an overview of the US Government Biometric Consortium and how this group is bringing together technologists from Government and industry to work together on improved standards.

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Examples of human traits used for biometric recognition include fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins. Biometric recognition can be used in *identification* mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match. A system also can be used in *verification* mode, where the biometric system authenticates a person's claimed identity from his/her previously enrolled pattern. Using biometrics for identifying and authenticating human beings offers some unique advantages. Only biometric authentication bases an identification on an intrinsic part of a human being. Tokens, such as smart cards, magnetic stripe cards, physical keys, and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. While all biometric systems have their own advantages and disadvantages, there are some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people.

There is a great deal of scientific data supporting the idea that "no two fingerprints are alike." Newer methods, even those with a great deal of scientific support, such as DNA-based genetic matching, sometimes do not hold up in court. Another key aspect is how *user-friendly* is the system. Most people find it acceptable to have their pictures taken by video cameras or to speak into a microphone. In the United States, using a fingerprint sensor does not seem to be much of a problem. In some other countries, however, there is strong cultural opposition to touching something that has been touched by many other people. While cost is always a concern, most implementers today are sophisticated enough to understand that it is not only the initial cost of the sensor or the matching software that is involved.

Often, the life-cycle support cost of providing system administration support and an enrollment operator can overtake the initial cost of the hardware. Also of key importance is accuracy. Some terms that are used to describe the accuracy of biometric systems include *false-acceptance rate* (percentage of impostors accepted), *false-rejection rate (p*ercentage of authorized users rejected), and *equal-error rate* (when the decision threshold is adjusted so that the false- acceptance rate equals the false-rejection rate). When discussing the accuracy of a biometric system, it is often beneficial to talk about the equal-error rate or at least to consider the false-acceptance rate and false-rejection rate together. For many systems, the threshold can be adjusted to ensure that virtually no impostors will be accepted. Unfortunately, this often means an unreasonably high number of authorized users will be rejected. To summarize, a good biometric system is one that is low cost, fast, accurate, and easy to use.

Examples of Biometric Applications

There are many examples of biometrics being used or considered in Federal, State, local, and foreign government projects. One use is to provide robust authentication for access to computer systems containing sensitive information used by the military services, intelligence agencies, and other security-critical Federal organizations. Physical access control to restricted areas is another key application. There are many law enforcement applications, mostly for fingerprint recognition, at the Federal, State, and local levels. Other law enforcement applications include home incarceration and physical access control in jails and prisons. Perhaps one of the most extensive applications of biometrics is for entitlements. Fraud in entitlement programs is estimated by the General Accounting Office at over $10 billion per year. Pilot programs in several States have demonstrated dramatic savings by requiring biometric authentication when someone is applying for entitlement benefits. There are also significant applications for biometrics in the commercial sector. Some of the biggest potential applications include the use of biometrics for access to Automated Teller Machines (ATMs) or for use with credit or debit cards. Many types of financial transactions are also potential applications; e.g., banking by phone, banking by Internet, and buying and selling securities by telephone or by Internet. Fraud on cellular telephone systems has increased dramatically and is estimated by some sources at over $1 billion per year. Biometrics is being considered to reduce this fraud. Telephone credit card fraud is also a significant problem that may benefit from the use of biometrics.

There are also commercial applications for computer access control, access to web site servers, access through firewalls, and physical access control to protect sensitive information.

Current Applications

Immigration and Naturalization Service's (INS) Passenger Accelerated Service System

(INSPASS)

INSPASS was designed as a means to provide prompt admission for frequent travelers to the US by allowing them to bypass the personal interview/inspection part of the entry process. It uses hand geometry to verify the identity of the traveler at an automated inspection station. INSPASS stations have been installed, for example, at John F. Kennedy Airport in New York and Newark International Airport in New Jersey. INSPASS is available for citizens of 23 countries in the US visa waiver program who visit the US at least 3 times per year. These same 23 countries are planning to participate in the Future Automated Screening for Travelers (FAST) project, which would allow travelers to use automated passport inspection stations in countries participating in FAST.

CANPASS

CANPASS is the Canadian version of INSPASS, except that it uses a fingerprint biometric, rather than hand geometry, for traveler verification. The goal of CANPASS is to ease the transfer of goods and people between the US and Canada. CANPASS is in use at the Vancouver International Airport.

PORTPASS

PORTPASS is another INS initiative similar to INSPASS except that people in vehicles at borders are being monitored and it uses a **voice recognition biometric, instead of hand geometry**. PORTPASS is used at a US/Canadian vehicle border crossing and is planned for use at US/Mexican border crossings. One version of PORTPASS (the Automated Permit Port) requires the vehicle to stop. It will also have a Video Inspection Service, allowing a driver to conference with an Inspector should the biometric fail. Another version, known as the Dedicated Commuter Lane, uses a radio frequency tag affixed to the vehicle in order to obtain the biometric as the vehicle is moving.

Federal Bureau of Prisons

The Federal Bureau of Prisons is using hand geometry units to monitor the movements of prisoners, staff, and visitors within certain Federal prisons. A successful trial with the hand geometry units was conducted at the Federal prison in Jesup, Georgia. Visitors must enroll upon arrival and are given a magnetic stripe card containing information that points to his/her identifying information in a central database.

This card must be carried with the visitor at all times. Staff and inmates must also enroll. Staffs are enrolled to reduce the possibility of mistakenly identifying them as an inmate or for positive identification in the event of a disturbance. Prisoners are enrolled for access control to places such as the cafeteria, recreation lounges, and the hospital. The system also allows for the tracking of prisoners' movements. By the end of 1995, around 30 Federal prisons were to have the hand geometry monitoring system installed.

Automated Fingerprint Image Reporting and Match (AFIRM)

In July of 1991, Los Angeles County in California installed the first AFIRM system. AFIRM was needed to reduce fraudulent and duplicate welfare benefits. The fingerprints of new applicants for welfare benefits are checked against a central database of prior claimants. Within the first 6 months of use, the county saved $5.4 million dollars, and the savings have been growing ever since. The system has been so successful that San Francisco, Alameda County, and Contra Costa County have installed AFIRM and check new claimants' fingerprints against existing recipients in these locales. AFIRM is expected to be in statewide operation in California by some time in 1997.

Spanish National Social Security Identification Card (TASS)

The TASS program is a smart card initiative employing fingerprint technology to eliminate enrollment duplication and provide secure access to personal information upon retrieval. The program is an ambitious one, in that it will combine pension, unemployment, and health benefits all on one card.

The Colombian Legislature

The Colombian Legislature uses hand geometry units to confirm the identity of the members of its two assemblies immediately prior to a vote. The voting has been conducted this way since 1992.Many Federal, State, and local government agencies have purchased biometric systems. The Defense Advanced Research Projects Agency, Drug Enforcement Agency, Department of Defense, Department of Energy, Department of Public Safety, Department of State, Federal Bureau of Investigation, Federal Reserve Bank, Hill Air Force Base, the Pentagon, and the US Mint have approximately 250 biometric devices with 13,000 enrolled users for access control applications.[10]

Applications

Government Accounting Office's Electronic Benefits Transfer (EBT) Task Force

Plans are underway to disburse many of the Federal Government benefits (e.g., retirement, social security, welfare) electronically through ATMs and point-of-sale terminals. It is estimated that $110 billion in Government benefits could be transferred onto and debited from access cards in this way. Initial plans are to implement fingerprint identification at the benefit enrollment phase.

The success of the AFIRM program in Los Angeles County was the inspiration for the EBT plan. Fingerprint identification in the benefit disbursement phase is also under consideration to eliminate what could amount to extensive losses from the abuse of lost or stolen cards.

FBI's Integrated Automated Fingerprint Identification System (IAFIS)

IAFIS is designed to electronically replace the horrendously outdated, mostly manual fingerprint identification system that requires paper-based fingerprint cards, postal submissions of the cards, and labor-intensive searches. IAFIS would replace paper-based fingerprints with electronic ones. Submissions of requests could be made electronically and all searches for fingerprints would be conducted electronically. The goal is to reduce response time to a requesting agency from the current 10 weeks to 24 hours.

National Crime Information Center 2000 (NCIC 2000)

NCIC 2000 offers new and improved capabilities for the National Crime Information Center. Biometric information, such as that contained in the signature, face, and fingerprint, will be used in an automated system. Patrol cars will have the capability to capture fingerprints and eventually relay the information to local, State, and/or Federal Automated Fingerprint Identification Systems (AFISs). The goal is to have the new and improved system fully operational by the fall of 1999.

Interest

- The interest in implementing biometrics for various applications within the Government, industry, and academia is widespread and quite varied. The following examples touch upon a few of the many possible uses of biometrics within the Federal Government.
- The Department of State is considering the use of biometrics to aid in their processing of 4 to 5 million passports/visas per year.
- The Bureau of Printing and Engraving would like to improve their current security methods with the addition of biometrics in order to prevent any loss of currency.
- The Department of Defense is researching biometrics and their implementation for computer network security.
- The Federal Aviation Administration is considering biometrics for airport security applications.