

# Using Technology to Authenticate Individuals, A Case Study

By Kimberly Woods and Thomas McLaughlin  
West Virginia High Technology Consortium Foundation, October 2005

---

*Abstract* - Identity theft is an increasing threat that infringes on the benefits of a free society. Identity theft occurs when someone uses an individual's personal information to take on that person's identity. A deterrent to identity theft not only includes discretion when disclosing personal information and all the precautions necessary to safeguard the data during storage and transport, but the presentation of unique information that excludes any other individual. How can we confidently and uniquely identify or verify ourselves? A key component of any identity confirmation process is the information presented that is distinctive to the individual. Identity validation techniques used to be reserved only for those accessing classified information related to national security. But increasingly these techniques are being considered for transactions ranging from purchases at a grocery store to work release programs in a detention facility. Strong authentication can involve something you have (token, card), something you know (PIN, password), and something unique to yourself (biometric, DNA).

---

## 1. BIOMETRICS USED BY LAW ENFORCEMENT

The identification and or verification of an individual become strikingly clear in a detention facility. Offenders are notorious for hiding their identity. When an inmate has been entrusted to a facility, extraordinary precautions must be taken to ensure everyone is accounted for. One of the earliest adopters of biometric technology has been law enforcement. There is a rich history of using biometric identifiers to recognize prisoners and repeat malefactors. Individuals arrested have their fingerprints taken and computers enable us to make rapid comparisons and to establish links to other crimes. Investigators look for fingerprints and DNA at a crime scene. Biometrics includes the measurement of a person's physical characteristics or traits. Biometrics becomes a powerful tool when combined with mechanisms that can automate the process. We have unique characteristics that, if correctly recorded and securely handled, can be used to compare against a live sample for a positive match.

## 2. CATEGORIES OF BIOMETRIC TECHNOLOGY

Some of the main categories of biometric technologies include fingerprint, face, hand, iris, voice, signature, and keystroke. Each biometric technology employs an enrollment function, where a sample(s) or measurement is taken and stored as a template. Identification is achieved when a sample is taken and successfully matched against the stored template.

## 3. THE BIOMETRIC PROCESS

Biometric devices can compare a properly "enrolled" sample with a live sample and attempt to make a match. Each biometric system has its

own operational method; however, the authentication process of every biometric system can be broken down into a four step process: capture, process, enroll, and authenticate.

**Capture:** A user presents his/her biometric sample (such as a fingerprint) to a sensing device (such as a fingerprint scanner) for capture.

**Process:** Once the sample is captured, features are extracted from the sample into a mathematical representation of the original sample. This processed sample is called a biometric template. A template can vary in size depending on the system. It is during this process where the biometric systems' methods most differ from one another.

**Enroll:** Once the template(s) is created, it is then stored in a database for later comparison for authentication. This process is called enrollment.

**Authenticate:** When a user approaches a biometric system to establish validity after enrollment, the sample is compared against the database of stored templates. This process is called authentication. There are two types of authentication:

**Identification:** The process by which the biometric system identifies a person by performing a one-to-many (1: n) search against the entire enrolled population. Identification answers the question "Who am I?"

**Verification:** During verification (or 1:1 matching), users possess a credential such as a token, password, or username, to claim an identity. That credential is mapped to the enrolled template and the newly captured sample is compared to the template corresponding to that credential.

Verification answers the question, "Am I who I say I am?"

#### 4. MEASURING BIOMETRIC PERFORMANCE

The performances of biometric systems usually are measured in the form of decision, matching, or image acquisition error rates.

##### Decision Error Rates

False Accept Rate: The probability that a biometric system will fail to reject an imposter.

False Reject Rate: The probability that a biometric system will fail to identify an enrollee.

##### Matching Error Rates

False Match Rate: The probability that a sample will be falsely matched against a "non-self" template.

False Non-Match Rate: The probability that a sample will not match a template of the same user.

##### Image Acquisition Error Rates

Failure to enroll rate: The portion of the population for whom the system is unable to generate repeatable templates.

Failure to acquire rate: The portion of the population for which the system is unable to capture an image of sufficient quality.

The definition of decision errors and matching errors seem similar; however, decision errors include failure to acquire rates.

#### 5. A CASE STUDY

Each application requires careful examination to determine which biometric(s) to incorporate and how to successfully put into operation. The technology is selected not only by the accuracy of the system and the cost, but in many instances the primary concern is the implementation of the technology.

Last year the Jefferson County Sheriff's Office (JCSO) jail in Colorado housed an average of 1153 offenders [1], with capacity for 1300. On a typical day, anywhere from 50-80 persons would be booked [2]. Also, approximately 200 offenders would typically be released on pass from the facility to work, seek employment or take advantage of educational opportunities [3]. Because of the responsibility to not release the wrong person, management searched for a system that could identify an individual quickly, reliably, and provide an audit trail of inmate movements.

The JCSO chose iris biometric technology because of its accuracy, ease and speed of use. The colored part of the eye is called the iris, but the color is not included in the biometric. The iris controls light levels inside the eye, similar to the aperture of a camera. The iris is layered beneath the cornea and exhibits intricate patterns with many furrows and ridges. Iris recognition technology is less intrusive to a subject because the device doesn't actually touch the person. Hands-free video capture occurs at a distance without coming in contact with the individual. Compared to finger scanning, the iris is an internal organ and not subject to environmental hardships. The iris is unique and constant throughout one's life. Comparatively, fingerprint ridges are not always discernible among certain individuals and minutia extractions are more difficult among the elderly. However, the major drawback is that currently there are no existing iris criminal databases accessible nationally.

The JCSO uses the Offender ID™ by SecuriMetrics [4]. The SecuriMetrics package provides the middleware, computers, and training necessary to implement the identification process. SecuriMetrics incorporates stationary and portable iris scanning devices at the JCSO jail. Iris templates then are searched within the database to determine if the person has already been enrolled. If the person has not been enrolled previously, the officer is then prompted to enter the pertinent identification information. If the person has already been enrolled previously, the offender's information will be displayed on the computer screen. The un-tethered portable devices (Portable Iris Enrollment and Recognition Device, PIER™) can store up to 100,000 iris subjects. The PIER™ is a self-contained iris enrollment and recognition system that operates in combination with network applications for identity recognition and tracking.

The JCSO utilizes five stations for processing offenders at the jail. These include booking, work release outbound, work release inbound, transportation, and final release.

The booking station conducts the initial processing of offenders. The booking process includes iris scanning, ink and AFIS (Automated Finger Imaging System) fingerprinting (including whole hand, palm, and side of palms), and photograph. AFIS is a system used by law enforcement to store, search, and retrieve finger and palm prints electronically.

The offender is given a wrist-band with his or her name, picture, DOB, height, weight, and unique offender identification number. The information is written on the bracelet and encapsulated within a

bar code. Each time the offender is to be identified, the information on the bracelet is compared with the result of the iris scan.

The Sheriff's Transfer or Transportation station confirms the identification of general population inmates that leave the building temporarily for court visits in other jurisdictions. The work release station features a dedicated iris scanner for inmates leaving the facility and a dedicated iris scanner for returning to the facility. When an inmate leaves the jail, the system time stamps the exit and the offender must call when arriving and leaving work. The on-duty officer will record the call within the system. The offender must pay rent to the JCSO jail, which is associated to the amount of hourly wage. There are random urine and breath tests to verify they are drug and alcohol free. The computer screen provides the offender ID counter in the upper right corner of the screen with the total number of offenders under the jail's control. Also provided are the number of offenders in the work release program, the number of work release offenders out of the facility, and the number of work release offenders exceeding their time pass. Officers can click an icon and receive the list of individuals and the details about their release commitments. The system sets a time parameter that alerts officers (with a red flashing visual field) when an inmate is overdue.

There is a station within the Inmate Services Unit (ISU) that verifies the inmate before leaving the facility the final time. Prior to iris scanning at the JCSO, officers would review the photo, manually compare a new ink fingerprint with the stored fingerprint, and question the offender before making the final release. According to the JCSO, iris scanning is fast, efficient, and accurate. If an inmate uses another wrist-band, the iris scan will immediately recognize the mismatch.

## **6. THE UNIQUENESS OF IRIS RECOGNITION REVISITED**

The iris is distinctive. It is statistically more accurate than DNA. The iris is stable from age one to death. No two irises, even the left and right irises from the same individual, are alike.

Often, iris recognition technology is referred to as "iris-scanning;" however, no scanning is involved. Iris recognition technology examines the unique patterns of the human iris. A video image of the iris is captured from 3 to 21 inches away (depending on the camera used). This image is used to produce a digitized 512 byte template called an 'IrisCode®.' This process was invented by Dr. John Daugman [5] and patented in 1994.

For authentication, the user presents his/her iris to the system and within seconds the iris is compared to one template or many templates.

Several tests and observations have identified iris recognition technology as one of the most accurate biometric. Iris technology is not intrusive, because the application sensor does not touch the individual. Users prefer the use of the iris over fingerprint mostly because no physical contact is required. The most current test of iris recognition technology is the International Biometric Group's (IBG) Independent Testing of Iris Recognition Technology (ITIRT) [6]. The ITIRT test represents the largest independently-conducted test of iris recognition technology executed to date.

## **7. FUTURE USE OF BIOMETRIC TECHNOLOGY**

It is acceptable for someone who is incarcerated to be enrolled in a biometric system and tracked within a jail process, because of the responsibility imposed on the facility. However, use of biometric systems for day-to-day transactions in a free society may not be accepted. Biometric systems that track individuals purchasing preferences, so retailers can better target their potential customers; will not be viewed favorably by most consumers. Misuse of data, invasion of privacy, and religious convictions are major concerns of a wary public when it comes to biometric usage. On the other hand, tragic events can sometimes spur the willingness of citizens to forego privacy concerns for the protections offered by strong authentication techniques. The question again arises about the misuse, information disclosure, the risk of stolen templates, or system failures (i.e. false rejection or false acceptance) when biometrics are used to identify individuals. System integrity, implementation, and intrusiveness will have to be carefully analyzed before utilizing a biometric to provide authentication for any transaction.

As the need for physical security arises, iris recognition technology, as well as all other biometric technologies, will improve to meet the changing needs of the government and industry. New biometric technologies will arrive creating the need for additional social, legal, and policy issues to be addressed.

## **References**

[1] From an onsite interview with Special Duty Officer James Prichett, JCSO, Golden, CO, August 22, 2005

## References (continued)

[2] From an onsite interview with Sergeant AI Anderson, JCSO, Golden, CO, August 22, 2005

[3] From an onsite interview with Deputy Kimberly Jensen, JCSO, Golden, CO, August 22, 2005

[4] SecuriMetrics, Inc. 757 Arnold Drive, Suite D, Martinez, CA 94553, [www.securimetrics.com](http://www.securimetrics.com), as of September 02, 2005

[5] "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," by John G. Daugman that appeared in the IEEE Transactions on Pattern Analysis and Machine Intelligence VOL 15, NO 11, November 1993

[6] "Independent Testing of Iris Recognition Technology Final Report," May 2005 by the International Biometric Group (<http://www.biometricgroup.com/>) delivered to the Department of Homeland Security

### **About the authors:**

Kimberly Woods, Information Center Specialist, WVHTC Foundation Technology Management Group  
Kimberly currently tests and evaluates biometrics products for the Department of Defense.  
Bachelor of Science in Forensic Identification (Biometric Systems) – 2003, West Virginia University  
Bachelor of Science in Computer Engineering – 2002, West Virginia University

Thomas McLaughlin, Project Manager, WVHTC Foundation  
Public Safety & Homeland Security Group – Office of Law Enforcement Technology Commercialization  
Tom has previous work experience with the National Security Agency as an information system security engineer and the Northrop Grumman Corporation as a design and field engineer. Tom currently assists the Department of Justice/National Institute of Justice with the commercialization of emerging technologies for law enforcement.  
Master of Science in Electrical Engineering – 1999, Johns Hopkins University  
Bachelor of Science in Electrical Engineering – 1987, West Virginia University