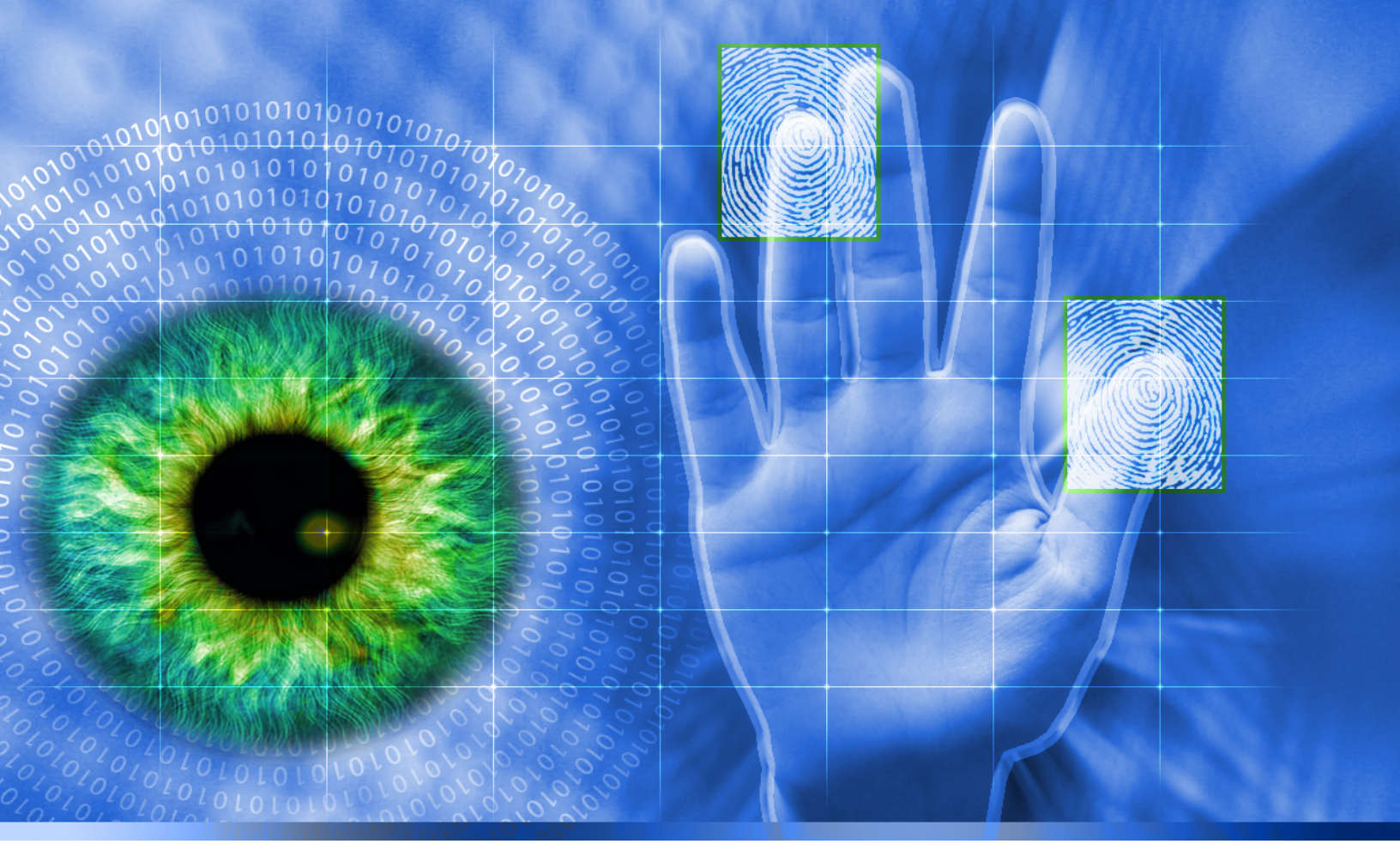

*System Assessment and Validation for Emergency Responders (SAVER)*

# Biometric Systems Application Note

*June 2015*

Homeland Security
Science and Technology

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

***Prepared by Space and Naval Warfare Systems Center Atlantic***

The *Biometric Systems Application Note* was funded under Interagency Agreement No. HSHQPM-13-X-00024 from the U.S. Department of Homeland Security, Science and Technology Directorate.



The cover photo image was provided by Space and Naval Warfare Systems Center Atlantic.

# FOREWORD

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercially available equipment and systems, and develops knowledge products that provide relevant equipment information to the emergency responder community. The SAVER Program mission includes:

- Conducting impartial, practitioner-relevant, operationally oriented assessments and validations of emergency responder equipment; and
- Providing information, in the form of knowledge products, that enables decision-makers and responders to better select, procure, use, and maintain emergency response equipment.

SAVER Program knowledge products provide information on equipment that falls under the categories listed in the DHS Authorized Equipment List (AEL), focusing primarily on two main questions for the responder community: "What equipment is available?" and "How does it perform?" These knowledge products are shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. As a SAVER Program Technical Agent, the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Atlantic has been tasked to provide expertise and analysis on key subject areas, including communications, sensors, security, weapon detection, and surveillance, among others. In support of this tasking, SPAWARSYSCEN Atlantic conducted research on biometric systems and their use by emergency responders. Biometric systems technology falls under AEL reference number 05AU-00-BIOM titled Device, Biometric User Authentication.

Visit the SAVER website on First Responder.gov (http:www.firstresponder.gov/SAVER) for more information on the SAVER Program or to view additional reports on biometrics or other technologies.

## POINTS OF CONTACT

**SAVER Program**
**U.S. Department of Homeland Security**
**Science & Technology Directorate**
FRG Stop 0203
245 Murray Lane
Washington, DC 20528-0215

E-mail: saver@hq.dhs.gov
Website: http://www.firstresponder.gov/SAVER

**Space and Naval Warfare Systems Center Atlantic**
Advanced Technology and Assessments Branch
P.O. Box 190022
North Charleston, SC 29419-9022

E-mail: ssc_lant_saver_program.fcm@navy.mil

# TABLE OF CONTENTS

## LIST OF FIGURES

# 1. INTRODUCTION

Biometrics measure the physical and behavioral characteristics of individuals and assigns a unique identity through automated methods. Physical characteristics include the anatomical components and physiological functioning of the human body, while behavioral characteristics describe the way an individual reacts or moves within the environment. Biometric systems can be classified according to the human characteristic being measured. These classifications are also known as biometric modalities. The modalities most commonly used in law enforcement are fingerprint and facial recognition.

Public safety and emergency response agencies are rapidly implementing biometric systems to improve operations such as verifying inmate identities, investigating crime scenes, and maintaining security at sporting events and incident command posts. Among the many benefits biometric systems provide are enhanced safety for emergency responders and increased security of the nation's borders.

This application note presents information on biometrics technology, standards and specifications, and databases, as well as discussions of current applications of the technology. It is intended to assist those seeking to implement this technology. The content in this document was gathered from October 2013 to April 2014 from Internet searches, industry publications, and interviews with subject matter experts.

# 2. TECHNOLOGY OVERVIEW

Biometric systems are highly complex and involve a variety of components and processes. Biometric system concepts, underlying technology, and how the technology functions are described below.

## 2.1 Verification and Identification

Biometric systems can be used for verification or identification. Verification, sometimes referred to as one-to-one matching, determines if a person is whom he or she claims to be. This process involves capturing a person's biometric data and matching it against an existing record for that person. Typical applications of these types of systems include controlling access to a secure facility or granting permission to use a secure computer system.

Alternatively, identification determines who an individual is through a process referred to as one-to-many matching. With these systems, a record of a person may be known to exist in the database (i.e., closed-set identification) or may not be known to exist in the database (i.e., open-set identification). His or her biometric data is compared against all existing records in a database in order to find a match. For example, law enforcement could use this type of system to identify an individual who does not have a driver's license at a traffic stop.

Biometric systems automate the verification and identification processes by capturing characteristics of individuals, extracting measurable features, and comparing the data against enrolled biometric records.

## 2.2 Enrollment

Enrollment is the process by which the biometric data of individuals is captured and stored so that it can later be used for matching. A verification system, for example, could require the creation of a relatively small enrollment database for all personnel authorized access to a particular facility. In contrast, an effective identification system may require a much larger biometric database. The entire collection of fingerprints maintained by the Federal Bureau of Investigation (FBI) would be one example.

Biometric data is captured by Federal, state, local, and tribal authorities during activities such as criminal investigations, criminal booking, and security clearance processing and then electronically transmitted to the enrollment database for matching. The data would be enrolled in the database as long as it meets stringent quality criteria. Once an enrollment database is established and made accessible, biometric systems can use algorithms to compare new data inputs to existing records and find matches.

## 2.3 Biometric Modalities

Biometric systems can perform capture and recognition of a single characteristic, or they can be multi-modal, addressing two or more characteristics. They may be intrusive, requiring the individual to have direct contact with the capture device, or non-intrusive in which the biometric data is captured from a distance. An overview of biometric modalities is provided below.

### 2.3.1 Physiological/Anatomical Modalities

**Fingerprints**

Fingerprints are the biometric modality most commonly used in law enforcement. Fingerprints can contain as many as 70 to 75 unique characteristics, or print pattern features, such as details in the ridge endings and bifurcations (where a ridge splits into two ridges). Fingerprints can be flat or rolled. A flat fingerprint image, as shown in Figure 2-1, is taken by touching a single finger to a platen, or paper card, without any rolling motion. A fingerprint enrollment record may include one or more flat fingerprints. A slap image is taken by simultaneously pressing the four fingers of one hand onto the platen or card. Slaps are typically captured using the "4-4-2 method" whereby the individual's right and left four fingers are captured first, then flat impressions are taken of both thumbs. Prints can also be rolled, in which the finger is rolled from one edge of the nail to the other on the platen or card. Rolled fingerprints are required primarily to support human examiners in latent print matching. Livescan fingerprints are taken by a sensor with the subject present, and latent fingerprints are taken from surfaces that an individual has touched.

**Figure 2-1. Flat Fingerprint**

*Image courtesy of SAVER*

**Face**

Facial recognition systems are gaining popularity in law enforcement applications. Facial recognition is a non-intrusive biometric technology since it does not require individuals to come into contact with the equipment. Both two-dimensional (2-D) and three-dimensional (3-D) systems exist. In 2-D facial recognition, the face is photographed and specific facial parameters

are analyzed to find a match. These facial parameters could include the distance between the eyes, the length and location of the nose, and the width of the mouth, as shown in Figure 2-2. Face matching accuracy using 2-D technology is often affected by factors such as lighting, pose, facial expression, facial hair, and/or makeup.

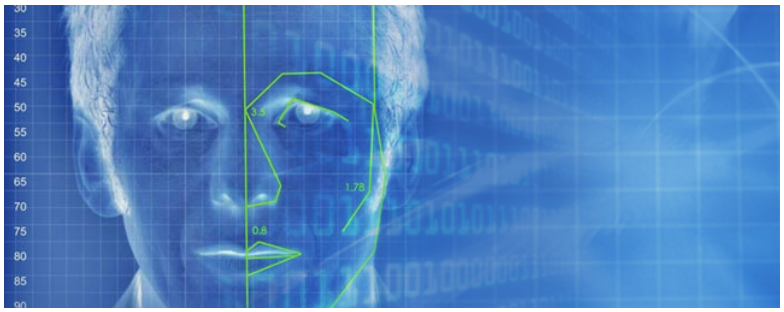

**Figure 2-2. Facial Features**

*Image courtesy of SAVER*

In 3-D facial recognition, a 3-D head/face model is created using one or more specialized cameras. The information is compressed into a 3-D biometric template that contains a unique "shape signature" of the face, and analyzed by an algorithm. This technique can result in a system that is more robust to changes in pose, illumination, and expression.

The FBI is currently working to add a facial recognition matcher to their national database. For more information on this technology, see the *Three-Dimensional Facial Recognition TechNote* and the *Facial Recognition Application Note*, which are available for download on the SAVER website at http://www.firstresponder.gov/SAVER.

## Iris

Iris recognition is also gaining traction in law enforcement. This technology involves taking a picture of the iris, which is the colored portion of the eye surrounding the pupil. Iris recognition is considered non-intrusive since it is simply an image. Near-infrared light is used to bring out the tissue structure of the iris regardless of the eye color and produce a clear, high-contrast image of the iris. The intricate structural patterns are then analyzed using algorithms.

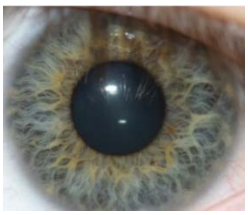

**Figure 2-3. Human Iris**

*Image courtesy of Matthew Goldthwaite/Wikimedia Commons/GDFL*

Over 250 characteristics can be obtained from the iris, an internal organ which is protected by the cornea from damage and wear. These two facts serve to make it an effective characteristic for biometric identification.

## DNA

DNA, the hereditary material in humans, has been used in forensics for many years. Cheek, or "buccal," swab samples can be collected using an FBI-issued kit and sent to the FBI for analysis. The Department of Defense (DoD), Department of Homeland Security (DHS), and FBI are conducting an initiative called "Rapid DNA." This effort focuses on developing and integrating commercial products that can fully automate the creation of a DNA profile from a buccal swab

within 2 hours. Rapid DNA includes the goal of initiating biometric enrollment and identity matching while a suspect is in police custody during the booking process.

**Palm Print**

In palm print recognition, an image is taken from the side and underside of the hand, and the analysis and recognition processes are similar to those of the fingerprint modality. Some palm print recognition systems scan the entire palm while others segment the palm into smaller areas for optimal matching accuracy. The FBI is currently working to add palm print recognition to their national biometric database.

**Hand Geometry**

Hand geometry is a recognition technology that uses the structure, shape, and proportions of the hand to aid in verifying an individual's identity. The human hand is not unique; therefore, hand geometry cannot be used effectively for identification in a large dataset. However, it can be paired with other forms of identification, such as a personal identification number or badge, as part of an access control system. During the capture process, the individual places their palm on the surface of a specialized reader. Characteristics such as length and width of the fingers, width of the palm, and finger curve are measured and used to create a template for one-to-one matching.

**Retina**

This recognition technology images the retina at the back of the eye and compares the pattern of blood vessels with existing data in an enrollment database. A specialized retinal scanner casts a beam of low-energy infrared light into the individual's eye and captures an image. The retinal blood vessels absorb the light more readily than the surrounding tissue, and the resulting pattern of variations is converted into a biometric template. It should be noted that retina images are declining in use for recognition systems. The medical community has found that they can be used to diagnose certain medical conditions. This has led to privacy concerns.

**Ear Shape**

Ear shape is a characteristic that is under research for its applicability to biometric identification. Ears can be distinguished by many points such as the overall shape (e.g., rectangular, triangular) of the ear, the contour of the helix (outer edge of the ear), and whether the lobule, or earlobe, is detached or attached to the head. Ear shape does not change significantly over an individual's lifetime and is not affected by factors such as expression as in facial recognition. Additionally, it is a non-intrusive biometric.

**Facial Thermography**

A thermogram is a visual display of various temperatures distributed on an object. Facial thermography, in particular, detects the unique patterns of heat emitted from a person's face and captures them with an infrared camera. Research has shown that virtually every individual's facial thermography is unique, making this characteristic applicable to biometric identification.

**Veins**

Veins, also called vascular pattern recognition, identify individuals using near-infrared light to detect the patterns of the blood vessels in a finger, on the palm, or on the back of the hand. As in retinal scanning, the difference in the amount of light absorbed by the blood vessels and other

tissue is captured as an image by the scanner. Characteristics such as vessel branching points are extracted from the image and used to create the biometric template. This characteristic is unique to each individual and is stable and unchanging.

### 2.3.2 Behavioral Modalities

**Speaker Recognition**

Also called voice recognition, speaker recognition measures voice patterns produced by the physical structure of the vocal tract combined with behavioral characteristics of the individual when speaking. Samples are captured over time and changes are analyzed. This modality is different from speech recognition, which recognizes words as they are articulated and is not considered a biometric technology.

**Keystroke Dynamics**

Keystroke dynamics is a biometric modality that measures a person's typing patterns and rhythm and uses them for recognition.

**Gait/Body**

Gait/body technology recognizes individuals by their distinctive walk. Motion characteristics are derived from a sequence of images captured with a camera or data produced by the accelerometer in a smart phone. These characteristics are processed to produce a template that can be used for identification. The characteristics can be obscured by obstructions such as loose-fitting clothing.

### 2.3.3 Soft Biometrics

Some soft biometric characteristics can be combined with biometric modalities to enhance verification and identification capabilities, especially in the field of forensics. These include eye color, dental information, height, weight, as well as scars, marks, and tattoos.

## 2.4 Biometric System Framework and Components

Biometric systems have a great deal of variation in the system framework and how biometric samples are processed. The basic system framework can be separated into five primary functions: capture, conversion, storage, comparison, and decision. Each of these functions uses one or more system components including sensors, scanners, cameras, software and algorithms, computers, and displays. Figure 2-4 and the sections that follow provide a simplified description of these biometric system functions and components.

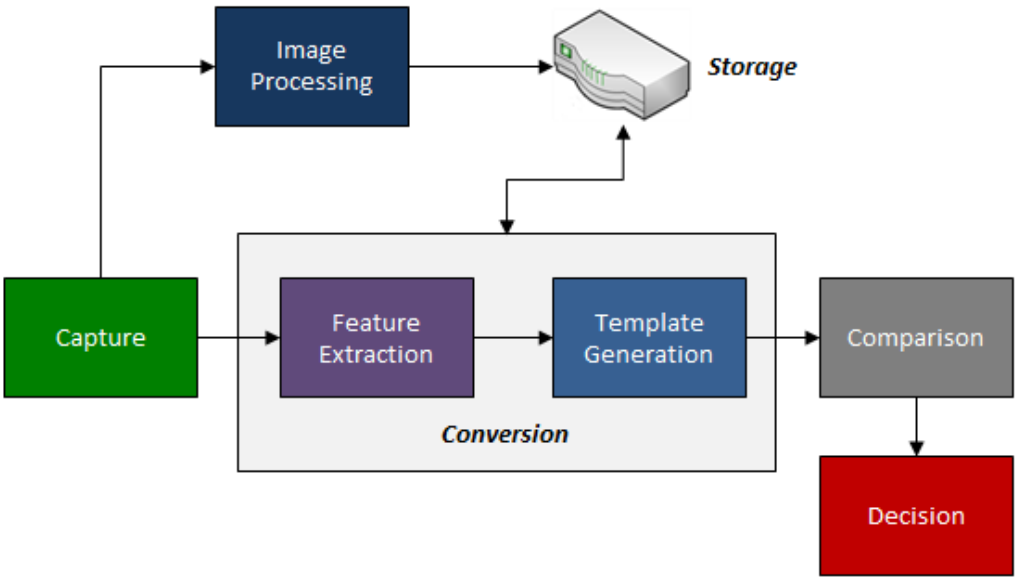


**Figure 2-4. Biometric System Processes**

*Image courtesy of Scientific Research Corporation*

## Capture

A sensor, such as the one shown in Figure 2-5, is used to capture a biometric sample from an individual as part of the capture step. Examples of capture activities include taking a digital photograph of a face, capturing fingerprints on an optical platen or sensor pad, and photographing an iris. The sensor converts the data to a digital format to prepare it for conversion. Biometric systems typically capture multiple samples in order to produce the most accurate record. For example, a facial recognition system may require several images in varying degrees of light or at different angles.

**Figure 2-5. Fingerprint Sensor**

*Image courtesy of SAVER*

## Conversion

The conversion process varies with the modality and system architecture. Signal processing algorithms perform quality control on the captured biometric sample. An example of a quality control activity is normalizing a facial image (e.g., changing color to black and white, adjusting for lighting and orientation differences). A subsequent step called feature extraction may take place, as depicted in Figure 2-6. Here, the system focuses on certain aspects of the biometric sample that make it unique, such as the ridge patterns in a fingerprint or the areas around the eyes, nose, and mouth. These distinctive features are extracted from the biometric sample, and an algorithm then converts them into a biometric template. Another variation in conversion is the processing of an image, such as a fingerprint. The captured image, typically a large file, may

be compressed using a specific algorithm to preserve quality during transmission. The resulting record, which is now called a biometric reference, is stored in a biometric database. A person's biometric reference may include their identification information as well as biometric samples, images, and templates. The actual content of a biometric reference is system specific and customized to the system's intended use.

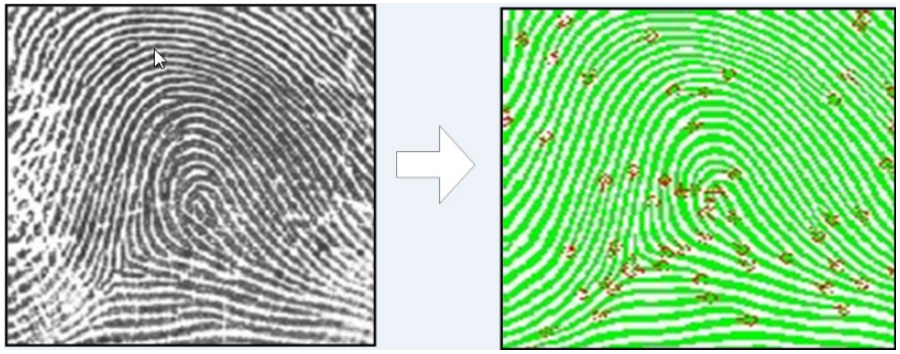

**Figure 2-6. Fingerprint Feature Extraction**

*Image courtesy of SAVER*

## Storage

A biometric database can be hosted on a server, or some other form of storage, and is used to maintain the biometric references. On mobile biometric systems, the biometric references may be stored on the mobile device itself. Some systems allow individual template storage on a personal identification smart card, such as a personal identity verification (PIV) card.

## Comparison

During the comparison phase, the newly processed templates are passed to a matching algorithm. This algorithm compares them to existing templates in the biometric references, estimating the extent of the similarity or, in some cases, the differences between them. In fingerprint comparison, for example, two types of matching are employed. Minutiae-based matching analyzes "minutiae points," such as the location and direction of the ridge endings and splits along the ridge paths of a fingerprint. Pattern matching simply analyzes the similarities between two fingerprint images. Typically, the algorithm produces a match score, which is used in the decision process.

## Decision

The decision process uses results produced by the matching algorithm to make a system-level decision. If the numeric score from the previous step is above a specified threshold, the biometric sample and references are deemed a match. The threshold for biometric systems is often adjustable to allow an organization to balance the tradeoff between False Acceptance and False Rejection (see Section 2.5 below). Even though biometric systems are highly accurate, there is still a margin of error that may produce more than one biometric reference as potential identification matches. This step may be fully automated or human-assisted. In some instances, results are displayed on a screen and may include additional data obtained through the biometric system's access to law enforcement records management systems, driver's license databases, or mug shot repositories, among others.

## 2.5 Performance

The performance of biometric systems depends on a number of factors. First, matching accuracy may be higher when the system used to capture the data in the enrollment database is the same one used to capture the new sample. For instance, systems implemented by a single vendor may have a good matching success rate because the same equipment and algorithms are used for both enrollment and new sample capture. Another factor that has a direct impact on the matching performance of the system is the quality of the captured biometric sample. The specific sensor or camera used, the operational environment, and operator skill level all affect matching performance. A few examples of the sample quality are:

- An unusable fingerprint image may be taken by a biometric system user with insufficient training and experience. Mistakes can include inconsistent pressure of the finger on the sensor plate or sliding the finger across the plate.
- A poor quality fingerprint sample can be caused by the poor quality of friction ridges present on the finger.
- A poor quality facial sample can be caused by inadequate lighting levels, poor focus, or varying facial expressions.
- An iris sample can be affected by the quality of the camera and proper iris position.

Many metrics are used to evaluate performance of a biometric system. Organizations must determine the importance of each of these metrics and adjust the system's sensitivity levels accordingly. Two of the primary verification metrics are:

- False Acceptance Rate (FAR) is the probability, expressed as a percentage, that a new biometric sample is incorrectly matched to a non-matching reference (i.e., another person's existing biometric reference). In a verification system, this means an unauthorized person would be granted access.
- False Rejection Rate (FRR) is the probability that the system fails to detect a match of a new biometric sample to a matching reference. In a verification system, this means an authorized person would be denied access.

Two of the primary identification metrics are:

- False-Negative Identification Rate (FNIR) is the percentage of matching attempts in which an enrolled user's correct biometric record is not among the returned matches. In an identification system, this means that input from an enrolled person is falsely declared as not belonging to any person enrolled in the system.
- False-Positive Identification Rate (FPIR or FPR) is the percentage of matching attempts in which an incorrect match is returned for users not enrolled in the system. In an identification system, this means that input from a person not enrolled in the database is falsely declared a match with one or more existing references.

Other metrics include the tradeoff between the FAR/FNIR and the FRR/FPIR, the percentage of biometric inputs that are rejected from the enrollment process, and the percentage of times the biometric system fails to accept an input when presented accurately. Speed and throughput are also important factors to consider.

### 2.6 Privacy

The use of biometric systems raises a number of privacy concerns. These include the concern that a biometric system, such as a facial recognition system, may be used to track a person's activities and that biometric data may be improperly used for forensic purposes. Other issues include the ability of facial recognition systems to capture images of individuals' faces without their knowledge or consent, and the risk that biometric systems can be breached compromising an individual's biometric data.

## 3. BIOMETRICS RESOURCES

The U.S. government strives to promote interoperability and collaboration between joint, interagency, intergovernmental, and multinational entities using biometrics. Provided below is a summary of Federal agencies and their ongoing work in the biometrics field, existing standards and specifications, and large-scale operational search engines and databases.

### 3.1 National Institute of Standards and Technology (NIST)

NIST performs biometrics research in the areas of: measurement; evaluation and standards for fingerprint matching and electronic transmission; criminal justice information systems; face recognition; iris recognition; and multi-modal biometrics. The organization works to develop a common set of standards, protocols, and access methods for interoperability of biometric systems in use throughout the Federal government.

Standard or Specification: ANSI/NIST-ITL 1-2011 Update: 2013

NIST developed a standard that defines the requirements for the electronic exchange of fingerprint, palm print, facial/mug shot, and other biometric data used in the verification and identification of subjects. The standard is called the American National Standards Institute (ANSI)/NIST Information Technology Laboratory (ITL) 1-2011 Update: 2013, NIST Special Publication 500-290, "Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information." The goal of the standard is to specify a common format for the exchange of biometric data across jurisdictional lines and between dissimilar systems made by different manufacturers.

### 3.2 National Institute of Justice (NIJ)

NIJ has a biometrics program that is active in collaborating with other Federal agencies in biometrics research, development, test, and evaluation efforts that benefit state and local law enforcement.

### 3.3 Federal Bureau of Investigation (FBI)

The FBI's Biometric Center of Excellence (BCOE) is the focal point for biometric collaboration and expertise for law enforcement and intelligence communities. The BCOE identifies operational needs for biometric technology with a focus on handheld biometric devices, standards, and interoperability. The BCOE tests and evaluates technologies, implements and oversees pilot and demonstration programs, and develops technology guidelines.

Standard or Specification: EBTS

The FBI's Electronic Biometric Transmission Specification (EBTS) Version 10.0 governs transmission of biometric images, as well as identification and arrest data, to the FBI by Federal, state, local, and international agencies. The FBI EBTS is based on the ANSI/NIST-ITL 2011 standard.

Databases: IAFIS, RISC, NGI, and NDIS

The Integrated Automated Fingerprint Identification System (IAFIS) is a national fingerprint system maintained by the FBI's Criminal Justice Information System (CJIS) Division. The system provides automated tenprint and latent fingerprint search capabilities, electronic biometric reference storage, and electronic exchange of fingerprints. It is accessible and provides responses 24 hours per day, 365 days per year and contains fingerprint references of over 115 million individuals. IAFIS also contains criminal history information, including mug shots; descriptions of scars, marks, and tattoos; physical characteristics; and aliases.

The Repository of Individuals of Special Concern (RISC) is a subset of IAFIS containing records on wanted persons, individuals in the sex offender registry, known or suspected terrorists, and other persons of special interest. RISC provides rapid search capabilities to law enforcement and partnering agencies.

The Next Generation Identification (NGI) project is a multi-year effort by the FBI to expand its biometric identification capabilities in order to:

- Expand the server capacity of the IAFIS;
- Add matching capabilities in other modalities such as face, iris, and palm prints;
- Improve its identification processes; and
- Ultimately replace IAFIS.

In a national press release dated September 15, 2014, the FBI announced full operational capability of NGI.

The Combined DNA Index System, or CODIS, is the FBI's program dedicated to supporting criminal justice DNA databases. CODIS includes the National DNA Index System (NDIS) containing DNA profiles submitted by Federal, state, and local forensic laboratories. The database contains over 10.8 million offender profiles, 1.8 million arrestee profiles, and 542 thousand forensic profiles.

## 3.4 Department of Homeland Security (DHS), Science and Technology Directorate (S&T)

DHS S&T performs research and development of biometric technology with the goal of promoting interoperability and effectiveness of systems designed to strengthen security of the homeland. Its efforts in the biometrics field have been focused on developing, integrating, testing, and transitioning biometric systems to operational Federal, state, local, and tribal end users. The directorate is leading efforts to develop a compact, lightweight, "four finger slap" sensor to capture multiple fingerprints at once on a mobile device (current systems only allow one or two prints at a time). The directorate is also leading development of systems that can integrate multi-modal biometric capabilities into a single device.

## 3.5 DHS Office of Biometric Identity Management (OBIM)

The mission of DHS OBIM, formerly U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT), is to help reinforce U.S. immigration and border security through the use of biometric technology. Their biometric specification and large-scale database are used by many DoD, Federal, state, and local entities to screen international travelers.

Standard or Specification: IDENT IXM

The Automated Biometric Identification System Exchange Messages Specification (IDENT IXM) is a standards-based messaging format for interfacing with US-VISIT/IDENT systems. The specification is based on the ANSI/NIST-ITL 1-2011 standard and is used by external entities seeking to create a client application that will interface with US-VISIT/IDENT messaging services.

Database: IDENT

DHS IDENT, the biometric reference data repository and comparison service portion of the US-VISIT program, is a DHS-wide system for storage and processing of biometric information for applications, including national security, law enforcement, border security, immigration control, and intelligence. Biometric reference data in the database consists of fingerprints, date of birth, place of birth, gender, and name. IDENT contains over 146 million biometric records.

## 3.6 Department of Defense

The Defense Forensics and Biometrics Agency (DFBA) is the DoD agency leading development and implementation of biometrics for combatant commands, services, and agencies, as well as increasing joint service interoperability. DFBA operates and maintains a DoD biometric database and watchlist service to support the national security strategy.

Standard or Specification: EBTS

The DoD EBTS 3.0 (2011) governs transmission of biometric reference data between DoD biometric systems and to systems operated by external agencies, coalition members, international partners, and governments. The DoD EBTS is based on the ANSI/NIST-ITL 2011 standard. A companion guide has been published called Implementation Guidance for Electronic Biometric Transmission Specification (DoD EBTS) targeted to biometric vendors, manufacturers, software/hardware developers, and implementers.

Database: Automated Biometric Identification System (ABIS)

ABIS is the central and authoritative multi-modal biometric database system for the DoD. The system provides search and retrieval services and interfaces with DoD information-sharing entities, including intelligence systems and other biometric repositories across the Federal government.

DoD also maintains the Biometric Enabled Watchlist (BEWL). BEWL is a DoD-wide service providing biometric matching and fusion with intelligence systems in order to return results quickly on persons of interest. It relies on the ANSI/NIST-ITL 1-2011 standard.

## 3.7 Biometrics.gov

Biometrics.gov (http://www.biometrics.gov) and its companion website, The Biometric Consortium (http://www.biometrics.org), are central sources of biometric-related information

and activities for the Federal government. These websites promote collaboration and information-sharing between government; commercial entities; state and regional organizations; international organizations; and the public.

### 3.8 ISO/IEC JTC 1/SC 37

The International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee (ISO/IEC JTC) 1/Subcommittee (SC) 37's responsibilities include the development of a family of standards on biometric data interchange technologies to support interoperability among applications and systems.

## 4. APPLICATIONS

Applications of biometric systems in public safety and law enforcement are widespread and varied. Automated fingerprint recognition has been in use for many years. Mobile identification devices are used more prevalently now for operations such as criminal arrests and booking, crime scene investigations, traffic stops, and border control. In these sometimes volatile situations, positive identification can be obtained almost instantly, increasing officer and community safety and speeding up the apprehension of suspects.

Facial and iris recognition systems are used for criminal booking, inmate identity verification, and criminal investigations. Biometrics technology can be used for access control for buildings, systems, and networks. The sections below describe some of these applications and provide examples of jurisdictions, counties, regions, and states that have implemented noteworthy biometric recognition systems.

### 4.1 Local, State, and Regional Biometric Systems

Local, state, and regional law enforcement agencies may implement their own biometric systems that share a common suite of hardware and software. The shared enrollment database is used for identification processing first; if no potential matches are found, the jurisdiction may send the biometric reference to Federal biometric databases for further analysis. Although these implementations are generally successful, system interoperability can be a challenge. New system implementations are more stringent with the application of Federal standards and best practices and adherence to a vendor agnostic (or open) approach that promotes interoperability and compatibility across systems and platforms.

Examples of local, state, and regional biometric systems in use today include the following:

Texas Department of Public Safety

The Texas Department of Public Safety has implemented an Automated Fingerprint Identification System (AFIS) that maintains biometric fingerprint records of all persons previously arrested in the state. In addition to livescan units used at police stations for arrests throughout the state, mobile fingerprint devices have been deployed to over 50 law enforcement agencies to capture live and latent prints for rapid identification. Fingerprint captures are transmitted to the AFIS with results returned in near real time.

Los Angeles County

The Los Angeles County Regional Identification System (LACRIS) is a biometric system that processes over 30,000 fingerprint and palm print comparisons and identifications monthly for area law enforcement agencies. The system provides matching against the California Identification System, called Cal-ID, and updates arrest records based on identification. Templates are also transmitted to the FBI's IAFIS for matching. The county has added mobile fingerprint recognition capability to facilitate rapid identification of suspects at booking and latent print enrollment and analysis.

Washington, D.C. Metropolitan Area

The Washington, D.C. Metropolitan area's AFIS, called the Northern Virginia Regional Identification System (NOVARIS), encompasses individual local systems in northern Virginia, Montgomery, and Prince George's Counties in Maryland and Washington, D.C. Housed and maintained by Fairfax County, Virginia, the system allows cross-jurisdictional data sharing and provides increased processing speed. It offers multi-modal capabilities including palm print; livescan and latent fingerprint; and face recognition. The region has also added mobile fingerprinting capabilities through the use of handheld devices.

Florida

The Pinellas County, Florida, Sheriff's Office has implemented a facial recognition system with a large database of enrolled images first built in 2001. This database of over 30 million facial images, reported to be the largest facial image database in the nation, facilitates rapid identification capability for corrections processing, mobile arrests/booking, and investigations. Over 193 Federal, state, and local law enforcement agencies are served by this system. They include more than 35 sheriff's offices contributing mug shot data for facial searching. Additional partnering agencies contributing their facial data include the Florida Department of Corrections, Washington, D.C. Metropolitan area (through a connection with NOVARIS), the Drug Enforcement Administration, Florida Sex Predators & Offenders, Missing and Endangered Persons Information Clearinghouse, and the Florida Department of Highway Safety and Motor Vehicles. Agencies capture facial images using digital cameras to take photos of suspects' faces for on-scene identification. The images are uploaded wirelessly using a camera docking station or by connecting the camera to a laptop in the patrol vehicle. Results are typically returned within 30 seconds and are displayed as a rank ordered gallery of potential matches with associated demographic information from the arrest record.

Western States

The Western Identification Network provides biometric enrollment and matching for nine western states—Alaska, California, Idaho, Montana, Nevada, Oregon, Utah, Washington, and Wyoming. This was the first multi-state automated fingerprint identification system with search access to over 29 million fingerprint records and 500,000 palm print records. The network accommodates extended searches to Cal-ID, operated by the California Department of Justice's Bureau of Identification, and the FBI's IAFIS.

## 4.2 Inmate Enrollment/Management

Biometric systems provide an effective means of verifying the identity of inmates housed in a detention facility. For example, agencies can use these systems to overcome situations in which new inmates refuse to identify themselves or provide a false identity. Agencies can also use biometrics to verify inmate identity prior to release. Fingerprint, iris, and facial recognition systems that enable biometric enrollment as part of in processing have already been implemented at many detention facilities. Biometric reference data is captured and matched against existing biometric references in the database to ensure each inmate's identity is correctly verified before a release, transfer to another facility, or other movement out of the facility. The sections below describe implementations of such systems by law enforcement agencies.

Pinal County, Arizona, Sheriff's Office

The Sheriff's Office of Pinal County, Arizona, implemented an iris recognition system to enroll and identify inmates of the detention center as well as convicted sex offenders undergoing registration at the facility. This particular system, called the Inmate Recognition and Identification System (IRIS), has been implemented in over 500 jurisdictions across 47 states. The system hosts a national database of over 400,000 biometric iris records and shares it with member agencies. Enrollment at the detention center occurs as offenders undergo booking or sex offender registration. Sheriff's deputies take photographs of the offender's eye, capturing its unique features in a non-intrusive manner, and transmit the resulting template to the national database. The system can then compare the captured iris template to existing biometric references stored in the national database and get results back quickly, typically in less than 8 seconds. These results include candidate matches and criminal information on the subjects. In Pinal County, almost 20,000 biometric records have been created during enrollment of inmates and convicted sex offenders.

Tarrant County, Texas, Police Department

Tarrant County, Texas, Sheriff's Office implemented an iris recognition system to enroll inmates at the county jail. At the time of booking, each individual's irises are imaged using a handheld camera. The image is processed and entered into the local iris database along with basic information about the inmate, creating a biometric reference. Matching takes place against more than 230,000 unique iris records stored in the database and results are returned within minutes.

## 4.3 Access Control

Biometric systems are effective in establishing and verifying the identity of individuals who are authorized access to a restricted facility, system, or area. Traditional authentication methods, such as access cards and personal identification numbers or codes, can be augmented with a biometric system, as shown in Figure 4-1, that uses unique individual characteristics to accurately verify identity. Emergency responder agencies may implement biometric access control systems to prevent unauthorized access to a variety of sites, including Emergency Operations Centers (EOC), emergency incident scenes, and critical infrastructure such as water treatment plants.

**Figure 4-1. Biometric Access Control**

*Image courtesy of Annagen, LLC dba Netrepid/CC-BY-SA-3.0/Wikimedia Commons*

Florida Division of Emergency Management

The Florida Division of Emergency Management has implemented a biometric access control system for their EOC. The fingerprint template and personal information of individuals authorized access into the EOC are stored on a personal identity verification card. Several doors are equipped with devices that are used to scan an individual's card, capture a fingerprint image, and convert it to a fingerprint template. The system checks the validity of the card and determines if the captured fingerprint template matches the fingerprint template contained in the card's barcode.

## 4.4 Border Security

Agencies can use biometric recognition systems to help secure the nation's borders by identifying individuals entering the U.S. illegally. Aliens committing crimes and held in local detention centers can also potentially be identified at booking, leading to reduced instances of booking under fraudulent identities. The following are examples of agencies using biometrics for border security.

Immigration and Customs Enforcement (ICE)

ICE uses mobile biometric capabilities in many jurisdictions across the country to rapidly identify aliens who have been arrested for a crime and placed into law enforcement custody. Typically, a local law enforcement agency with a criminal alien in custody submits an immigration query to ICE based on biographical data such as name and date of birth. These identifiers can be easily falsified. A biometric system that shares data with Federal, state, and local biometric databases; however, can be used to determine the identity and immigration status of an individual and lead agents to criminal information logged in other systems under aliases. Fingerprints sent by jurisdictions to the FBI are checked against records both in IAFIS and DHS' IDENT, thereby increasing identification rates and aiding ICE in enforcing immigration laws.

As part of the Biometric Identification Transnational Migration Alert Program (BITMAP) project, ICE is also seeking to use biometrics beyond the nation's physical borders in

collaboration with DoD. Multi-modal biometric identification devices are deployed to agents to capture data on individuals such as special-interest aliens in foreign immigration detention centers and gang members in foreign prisons. The data can then be used to conduct screenings, gather intelligence, and initiate investigations before the alien reaches the United States. This is the first system to search and enroll against all three major biometric databases: IDENT, ABIS, and IAFIS.

U.S. Coast Guard

The U.S. Coast Guard, responsible for protection of the United States' 95,000 mile maritime border, is using mobile biometric technology to identify individuals attempting to enter the U.S. illegally. The target for the implementation initially was the Mona Passage between Puerto Rico and the Dominican Republic, where 40 percent of illegal aliens enter the United States. The U.S. Coast Guard uses mobile identification devices to capture fingerprints and facial images of individuals and then transmit the records via satellite for comparison against biometric data in the DHS IDENT database. Results are typically returned within 2 minutes. Using this technology, the U.S. Coast Guard can quickly obtain criminal histories on these individuals, many of whom have previously entered the United States illegally and may have committed serious crimes while on American soil.

## 4.5 Criminal Investigation

Law enforcement agencies use biometric recognition systems to obtain positive and timely identification of criminal suspects. The following are examples of specific applications.

Stockton, California, Police Department

The Stockton, California, Police Department introduced mobile fingerprint devices as part of a pilot project with DHS to capture latent fingerprints at crime scenes, identify persons of interest in near real time, and reduce the time required to develop leads. The system uses a local AFIS with over 400,000 fingerprints from arrestees and serves over 10 agencies in San Joaquin County, California, that are all connected through a common biometric system. The system provides additional connectivity to numerous other counties and local government agencies and is integrated with local mug shot and records management systems. The mobile fingerprint devices transmit images securely over the commercial cellular network to mobile computers in the patrol vehicles, which then send data to the local AFIS for enrollment and matching. Capture and transmission of latent prints for matching is a new capability. Results are returned in less than 1 minute.

Pinal County, Arizona, Sheriff's Office

The Sheriff's Office of Pinal County, Arizona, expanded its biometrics program in 2012 by implementing mobile multi-modal biometric devices for patrol deputies, detectives, and SWAT members. The devices are used to capture unique fingerprint, iris, and facial biometric data from suspects at the scene, such as at a routine traffic stop or border crossing, in order to verify their identity and gather criminal background information quickly. The county is using smartphones and tablets equipped with a biometric module to capture biometric samples. The devices transmit the biometric data to a large database and receive results within seconds, increasing officer and public safety, situational awareness, and timely investigations.

# 5. CONCLUSION

Biometric systems provide reliable verification and identification capabilities to Federal, state, local, and tribal emergency responder agencies. These systems capture and match physiological, anatomical, and behavioral characteristics that are distinctive and unique to each individual. Fingerprint, face, iris, and DNA are the most common modalities in use in law enforcement. Many other modalities are in use as well, such as ear shape, vein, and voice recognition, while others are still under research and development.

Biometric systems are very technologically complex, but there are five primary processes supported by the sensors, software, and computers that make up these systems. These include capture, conversion, storage, comparison, and decision. Biometric databases house the biometric data, or biometric references, against which biometric samples are compared.

Emergency responder applications of biometric systems include forensics, inmate enrollment and verification, border security, criminal investigations, access control, and crime scene evidence collection. Rapid identification using biometric systems provides many benefits, including enhanced safety for emergency responders, a safer community, and increased security of the nation's borders.