TechBrief

FHWA Contact: Phil Forjan, HCS-20, (202) 366-6817

Biometric Identification Standards Research

The vision of the Office of Motor Carriers is to help move people, goods, and commercial motor vehicles on our Nation's highways in the most efficient, economical, and crash-free manner possible. The OMC research and technology program focuses on improving safety in interstate commercial motor vehicle operations and serves a trucking and motor coach industry that carries more than 40 percent of all intercity freight.

Studies are conducted in the following areas: commercial driver human factors, health, and performance needs; new and emerging driver and vehicle technologies; safety-related data collection and analysis needs; and performance-based changes to the Federal Motor Carrier Safety Regulations.

The OMC's technology research promotes safety by identifying, collecting, and communicating information about technological advances.

Office of Motor Carrier Research and Standards
400 Seventh Street, SW
HCS-30; Room 3107
Washington, DC 20590

Introduction

The Commercial Motor Vehicle Safety Act of 1986 was enacted to remove unsafe and unqualified commercial motor vehicle (CMV) drivers from the nation's highways by establishing a "one-driver, one-license, one-record" policy. This policy made it illegal for CMV drivers to have more than one commercial driver's license (CDL) and led to the development of the Commercial Driver's License Information System (CDLIS). This system contains identification information on CMV drivers, and provides States with the ability to check if a person already has a CDL before issuing a license to that applicant.

In 1988, Congress passed the Truck and Bus Safety and Regulatory Reform Act, which required the Federal Highway Administration to develop minimum uniform standards for a biometric identification system for CMV drivers. The establishment of a biometric identifier for CMV drivers would ensure the positive identification of drivers and would further prevent the issuance of multiple CDLs to one driver.

A 1990 Federal Highway Administration (FHWA) study that evaluated biometric technologies concluded that fingerprinting and retinal scanning were the two most promising technologies. Upon conclusion of the study, the FHWA determined that more time was needed for biometric technologies to develop in order to meet specified requirements and be beneficial to the CDL program. The present study began in October 1995.

A "biometric" technology is an automatic method for the identification, or identity verification, of an individual based on physiological or behavioral characteristics. Biometric *systems* function to identify individuals by matching a specific personal characteristic, the biometric identifier, with one previously recorded. General biometric systems consist of the five sub-systems shown in **figure 1**: data collection, transmission, signal processing, storage, and decisions.

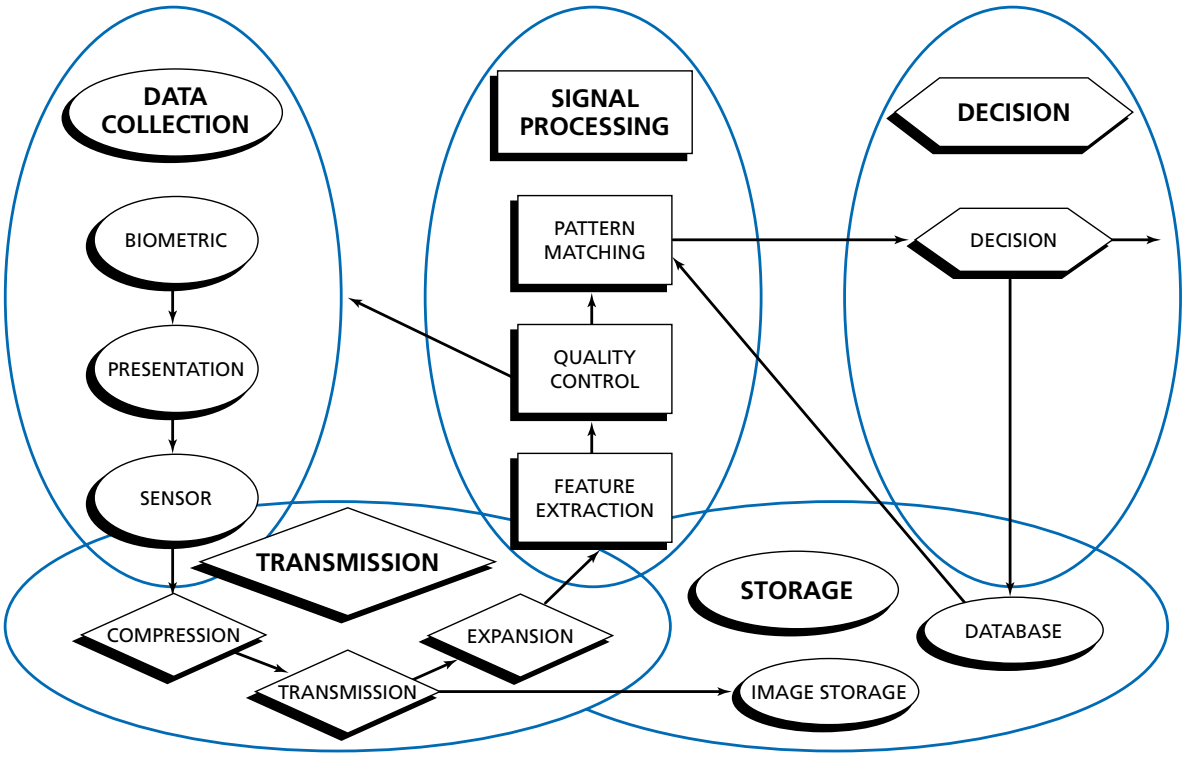
Purpose

The primary objective of this study was to make recommendations to the Secretary of Transportation for the establishment of minimum uniform standards for a biometric identification system to ensure identification of CMV drivers. Researchers sought to review the current status of biometric technologies to determine their ability to meet the needs of the CDL program and to determine the cost-effectiveness of the most promising technologies and systems for large scale applications.

Technology Selection

This study considered all commercially available biometric systems, including signature verification, voice recognition, finger and palm prints, iris and retinal scans, facial images, and even body odor systems.

Figure 1.
The General Biometric System



In determining candidate biometric technologies, researchers first needed to establish a fair and rational set of criteria. The American Association of Motor Vehicle Administrators (AAMVA) created a Biometrics Working Group to review this project and to establish functional requirements for a biometric identification system. After revision, the requirements included:

- The system will capture the biometric identifier from each applicant without increasing the actual time a customer is in a Department of Motor Vehicles office by more than 30 seconds.
- The identifier must be an accurate, relatively unalterable, unique physical characteristic that can be captured, recognized or verified, and stored — and must be verifiable over an indefinite period of time.
- The method of capturing the biometric identifier will be unobtrusive to the applicant. The method will be socially acceptable and will not endanger the health, safety, or welfare of any applicant.

Because the AAMVA functional requirements alone were insufficient to narrow the field of potential technologies, researchers then set up the following criteria:

- Vendors must claim that the technology supports all of the required applications. The technology must aid in the prevention, detection, and deterrence of the possession of multiple licenses by a single driver, and also in the use of a fraudulent CDL by a driver.
- The technology must have been used previously in a similar large-scale application for which an independent performance/cost audit is available indicating that the revised AAMVA working group functional requirements can be met.
- The technology must be available from multiple vendors supporting a single image collection, compression and storage standard.

Researchers determined that fingerprinting is the only biometric technology that can currently meet the above criteria, and that no other technology would meet the criteria within the next 5 to 10 years. Based on the material reviewed, researchers believe that an automatic fingerprint identification system (AFIS) could be designed to approximately meet all of the revised functional requirements. Current AFIS systems are computationally the fastest of all existing biometric technologies.

Methodology

Automatic Fingerprint Identification System Performance

In order to establish parameter values to predict AFIS performance on a large scale, researchers considered five important non-independent parameters that govern the performance of an AFIS.

- The system penetration rate is the expected percentage of the fingerprint database that may be compared to a single print.
- The bin error rate is the probability that a search for a print in the database will be unsuccessful because the sample and template prints were placed in different "bins".
- The single comparison false match rate is the probability that two non-matching prints will be matched incorrectly.
- The single comparison false non-match rate is the probability that two matching prints will not be matched when compared.
- The single comparison match rate is the number of "one to one" comparisons per second that can be made by the hardware of a single sample print to templates received from that database.

Mathematical models were developed to predict each of these parameters. Researchers then conducted the Republic of the Philippines Social Security System Identification Card Project AFIS benchmark test in May 1997. Four vendors participated in this test, which measured penetration rate, bin error rate, and single comparison false match and false non-match rates for each vendor. Single comparison match rate was not measured because each vendor was already required to produce a specified number of comparisons.

System Architecture

Researchers also constructed three approaches to the creation of a nationwide biometric system for identifying drivers: the centralized system; the distributed system with centralized communication; and the distributed system with direct communication.

The Federal-level centralized system is the most straightforward. It would establish a national system, much like CDLIS, that would electronically hold the records of all licensed commercial drivers. A commercial driver applying for a new license or a renewal would have copies of his/her fingerprints sent to the central site to be scanned against the existing database. To be effective, all states would be required to participate.

The State-level distributed system with centralized communication would have each state maintain and control its own commercial driver AFIS system. When a driver applies for a license, the fingerprint image would be sent to a centralized communication site, which would distribute the image to the independent systems in all other jurisdictions.

The State-level distributed system with direct communication is identical, except that fingerprint images would be sent directly by states to other participating jurisdictions.

Findings

With the data collected from the Philippine AFIS benchmark test, researchers predicted throughput and error rates for a centralized fingerprint system used in conjunction with CDLIS. Using mathematical models, researchers forecasted that a single-print system could not meet the revised functional requirements.

A single-print AFIS system collects only one fingerprint from each subject. Considering the bin error rate and the single comparison false non-match rate, the probability for a false non-match in this case would be 11 percent. This is only slightly higher than the functional requirement mandating no more than a 10 percent false non-match rate in the identification mode, but considerably higher than the requirement of no more than 1 percent in the verification mode. Further, the system false match rate in the identification mode against 8.5 million enrolled prints becomes 99 percent, compared to the requirement of less than one ten-thousandth of one percent (one in one million).

A two finger system, which collects prints from two different fingers of each subject, can approximately meet the functional requirements in both verification and identification modes.

In addition, this study included a procedure for a detailed cost-benefit analysis. Researchers concluded that there are no technical barriers to the implementation of either a Federal- or State-level biometric system, but that a Federal, centralized system for identifying commercial drivers is the most cost-effective approach.

Standards Development

Standards are required if a biometric identification system is to operate among States or on a national

Researcher
This study was performed by James L. Wayman, Biometric Identification Research Director, College of Engineering, San Jose State University. Contract No. DTFH61-95-C-00165.

Distribution
This Tech Brief is being distributed according to a standard distribution. Direct distribution is being made to the Resouce Centers and Divisions.

Availability
The study final report is available from the National Technical Information Service, Telephone: (703) 605-6000.

Key Words
biometric identifier, minimum uniform standards, functional requirements, automatic fingerprint identification system (AFIS), two-finger system, image quality, data compression, data format standards, unique identifier.

U.S. Department of Transportation
Federal Highway Administration

December 1998
Publication No. FHWA-MCRT-99-003

level. Regardless of the final system architecture, four standards are required and a fifth would be helpful:

- a standard biometric identifier;
- an image quality standard;
- a data compression standard;
- a data format standard; and
- a feature set standard.

This study recommends that fingerprinting be adopted as the standard biometric identifier, and that a two-print system be used. As far as determining which fingers to print, there is no standard. Researchers recommend that thumbs or index fingers be used, but the final decision should be made by the AAMVA Committee of States.

This study also recommends that image quality, data compression, and data format standards be adapted from existing standards developed by the Federal Bureau of Investigation, the American National Standards Institute, and the National Institute of Standards and Technology. These standards are included as appendices in the final study report.

The development of standard features for fingerprint comparison is a controversial subject. Vendors largely oppose standards, because of the loss of a perceived competitive advantage that would follow uniformity. The study recommends that AAMVA express interest in monitoring any feature set standard development.

The 1998 Transportation Equity Act for the 21st Century calls for a unique identifier for CMV drivers, which may be, but is not limited to, a biometric identifier. This research will aid States that choose to implement a biometric identification system for CDL drivers, as the report provides specific minimum standards for the use of fingerprinting to identify drivers, and the cost-effectiveness of implementing such a system.