Biometric identification: A holistic perspective

Lawrence D. Nadel*
Noblis, Inc., 3150 Fairview Park Drive, Falls Church, VA, USA 22042-4519

ABSTRACT

Significant advances continue to be made in biometric technology. However, the global war on terrorism and our increasingly electronic society have created the societal need for large-scale, interoperable biometric capabilities that challenge the capabilities of current off-the-shelf technology. At the same time, there are concerns that large-scale implementation of biometrics will infringe our civil liberties and offer increased opportunities for identity theft. This paper looks beyond the basic science and engineering of biometric sensors and fundamental matching algorithms and offers approaches for achieving greater performance and acceptability of applications enabled with currently available biometric technologies. The discussion focuses on three primary biometric system aspects: performance and scalability, interoperability, and cost benefit. Significant improvements in system performance and scalability can be achieved through careful consideration of the following elements: biometric data quality, human factors, operational environment, workflow, multibiometric fusion, and integrated performance modeling. Application interoperability hinges upon some of the factors noted above as well as adherence to interface, data, and performance standards. However, there are times when the price of conforming to such standards can be decreased local system performance. The development of biometric performance-based cost benefit models can help determine realistic requirements and acceptable designs.

Keywords: biometrics, performance, scalability, data quality, fusion, model, human factors, standards, cost benefit

1. INTRODUCTION

This intent of this keynote paper is to look beyond the basic science and engineering of biometric sensors and fundamental matching algorithms and present a high level, holistic perspective of the considerations and approaches that can enhance the efficacy and acceptance of biometric identification technology. The discussion will focus on three primary biometric system aspects: performance and scalability, interoperability, and cost benefit.

Prior to the terrorist attacks of September 11, 2001 and the tremendous international growth of electronic information networks, other than large-scale automated fingerprint identification systems (AFIS) used by the law enforcement community, biometric applications generally involved databases containing on the order of hundreds and thousands of individuals. Applications tended to be localized, both organizationally and geographically. Consequently, operational environments were somewhat definable and the biometric characteristics and attitudes of subject populations were more homogeneous and predictable. Interoperability and scalability were not fundamental requirements.

With society becoming more mobile and more "connected," today's biometric applications cut across broad organizational and geographic boundaries. The global war on terrorism and the associated emphasis on homeland security have mandated the capture, processing, and sharing of identity-related information at multiple levels—local, state, national, and international—in government, law enforcement, intelligence, and the military. Similarly, the increasingly global nature of business and commerce requires secure and reliable communication of data, money, and goods between individuals and organizations. Reliable knowledge of the identity of each individual participating in such business transactions is essential. As a result, interoperability and scalability have emerged as key determinants of the success or failure of a biometric-based application. Also, biometric characteristics and attitudes of subject populations are much more diverse, and so these factors must be critically addressed as well.

In the words of the U.S. National Science and Technology Council's (NSTC) Subcommittee on Biometrics, "… use of the technology thus far has mainly consisted of systems designed to meet narrow objectives. To fully meet large-scale identity governance requirements, the use of biometrics technology must be made more robust, scalable and

*nadel@noblis.org; phone 1 703 610-1677; fax 1 703 610-2053; noblis.org

Biometric Technology for Human Identification IV
edited by Salil Prabhakar, Arun A. Ross Proc. of SPIE Vol. 6539
653902, (2006) · 0277-786X/06/$18 · doi: 10.1117/12.724009

interoperable. Meeting these needs will require biometrics technology enhancements, adjustments of commercial business practices and system designs, and development of consensus on social, legal, privacy and policy considerations. Collaboration among the biometrics community— government, industry and academia—on these common challenges is essential."[1]

2. PERFORMANCE AND SCALABILITY

New or evolving large-scale government biometric-related programs that support the global war on terrorism and homeland security (e.g., U.S. Department of Defense Automated Biometric Identification System [ABIS], Federal Bureau of Investigation Next Generation Identification [NGI, currently the Integrated Automated Fingerprint Identification System – IAFIS], U.S. Visitor and Immigrant Status Indicator Technology [US-VISIT]) have demanding performance requirements and continue to grow in scale (e.g., number of transactions, enrolled database size, geographic extent and communications challenges, population diversity). Biometric system scale and performance are inversely related. For example, a system's false non-match rate (FNMR) is linearly proportional to the size of the enrolled database. Therefore, as a system's size increases, sub-system (e.g., matcher) performance must increase if total system performance is to remain constant.

While future advances in the fundamental biometric technologies and continued increases in computing performance (Moore's Law) will contribute to improving biometric system performance in terms of accuracy (e.g., true match rate, false match rate (FMR), FNMR, failure to acquire rate) and speed (e.g., matches per second, image segmentation time, end-to-end system throughput), there are considerable gains to be achieved by using current biometric technology more effectively. Potentially useful approaches are discussed briefly below.

2.1 Using data quality metrics to improve data capture quality and matching performance

Biometric sample *quality* can be described in terms of the following three elements: *character*, based on the inherent characteristics of the biometric source; *fidelity*, the degree of similarity between a biometric sample and its source—this reflects sensor performance as well as any subsequent processing of the sample such as image segmentation and data compression; and *utility*, a sample's contribution to the matching process.[2] Various studies have shown that the accuracy and throughput of a biometric system are directly related to the quality of the reference and probe samples.[3,4] Issues such as how to define and objectively measure quality, and whether or not quality parameters and their use can be standardized or should be matcher dependent are the subject of considerable discussion and research.

Quality metrics determined at the time of sample capture can be used to maximize captured sample quality as follows:

- If a sample does not meet a minimum quality threshold, have the subject provide repeated samples until the quality threshold is attained. If the quality threshold cannot be attained within a predetermined number of attempts, actions that might be taken include the following: (a) retain the best quality sample of those captured, or (b) reject all samples captured and invoke an alternative process—such as collection of additional information associated with the individual or collection of an alternative biometric (in a multi-biometric application), or (c) if the subject is intentionally uncooperative, take appropriate enforcement measures.
- Capture a series of samples, such as a stream of video frames of an individual's face, and retain the highest quality image, fuse the data to obtain a better composite image, or retain and process multiple images.
- Monitoring trends in sample quality over time by location and operator can help determine if capture equipment performance is degrading and if additional operator training or subject instruction might be needed.

Quality metrics determined either at the time of sample capture and/or during system processing can be used in various fashions to improve matching accuracy. Some possible approaches are as follows:

- A higher quality captured sample may replace a lower quality reference sample once the two samples have been deemed mates.
- A local quality metric, such as an indicator of smudges on a fingerprint image, can be used either to disqualify such suspect features from consideration or to lower the features' contribution to the matching decision.
- When performing multi-biometric fusion, the quality of the probe and/or reference image may determine the weight of the sample's match score in a score-level fusion approach, or which of several matchers to use.

- The quality of the probe and/or reference image may be a factor in determining the matcher threshold (to determine match or non-match) that should be used.

Biographic and other textual data associated with an individual is generally collected at the time of subject enrollment; textual data with future encounters is collected subsequently. Elements of this data may be used to support the matching process (e.g., to limit the reference search space and shorten search time, or to support or negate a marginal matcher outcome). The history portrayed by this data may determine what action is to be taken when a biometric match or non-match occurs. Therefore, error checking methods should be employed when this textual data is captured by the system. Error history should be collected for potential use in implementing an error detection and/or correction scheme.

2.2 Addressing applicable human factors with respect to subjects and system operators

Addressing human factors for the subjects of a biometric system can positively impact biometric sample quality and consistency, system accuracy and throughput, and subject satisfaction and willingness to cooperate. Human factors are relevant at multiple levels including: interaction with the capture device, impact of the ambient environment, provision of instructions and guidance, and establishing process flow. Addressing human factors for operators (e.g., a customs and border officer) of operator-assisted systems will help to reduce the extent and frequency of training required and permit operators to interact with the system more efficiently and effectively, thus allowing more time for interaction with subjects.

The human factors of biometric systems is an area that has received limited attention until recently. For example, in support of the US-VISIT Program, the National Institute of Standards and Technology (NIST) studied the usability of a six-inch high 10-print slap capture fingerprint device as a function of counter height.[5] Slap prints were captured with both simultaneous two-thumb impressions and sequential single thumb impressions. Counter heights tested were 26”, 32”, 36” and 42” off the floor. Usability was defined according to the standard ISO 92241-11 with respect to subject *efficiency* (time on task), *effectiveness* (accuracy—represented by the NIST Fingerprint Image Quality [NFIQ] score), and *satisfaction* (subject perceived comfort level). Findings included the following:

- 36” was the most efficient height when a right slap print was part of the capture sequence. Although the speed improvement was relatively small, this can have a cumulative impact when processing a large number of individuals in a queue.
- 26” was the most effective height for a capture sequence involving simultaneous thumbs and a left slap; image quality decreased with increasing counter height Thumb quality was more sensitive to counter height than slaps, and sequential thumb capture more effective than simultaneous thumb capture.
- Subject satisfaction was greatest for the 32” and 36” counter heights.

Conclusions included the following: start the capture sequence with the right hand, capture thumbs sequentially, and do not use a 42” counter height. Additional studies and analyses are in progress.

2.3 Controlling or accommodating the operational environment

Every biometric technology is impacted by one or more aspects of the operational environment with regard to sample capture. In choosing the best biometric for a given application, characteristics of the operational environmental are a key consideration. For example, conventional optical fingerprint sensors will be challenged significantly if operated in bright sunshine. Face and iris recognition systems tend to be particularly sensitive to ambient light conditions, and background lighting may significantly degrade the performance of these systems. In some cases, environmental controls (e.g., temperature, humidity, lighting, noise) are an option. It may be possible to accommodate uncontrollable conditions through judicious sensor placement (e.g., outdoors under a shade or indoors away from a window). The use of a sensor sensitive to a biometric characteristic but relatively insensitive to the offending environment may also be an option. In some applications, image processing may be useful to remove artifacts from captured images.

As given biometric applications expand and data is collected in a wider variety of environments, methods will be needed to detect and compensate for the additional variations in data quality. Likewise, as more and more data is shared between disparate systems, special attention will have to be paid to the capture environment-related characteristics of the data received.

2.4 Designing system workflow to optimize end-to-end throughput and utilization of system resources

As an enabling technology, biometric sample capture and processing is one component of an overall system. Thoughtful sequencing of processes both within the biometric subsystem and between the biometric subsystem and the overall application system can optimize system response time and utilization of system resources. When a rapid response is required, such as when processing a foreign visitor seeking entry into a country, to the extent possible, the most time-intensive processes (e.g., fingerprint-based watch list check) are initiated first so that additional processes (e.g., obtaining associated information such as reason for visiting and intended length of stay, capturing a facial photo) can occur in parallel. Such an approach would minimize processing time as perceived by the subject.

Workflow engineering can also have major impacts on resource utilization. For example, if prior to a fingerprint watch list search fingerprint minutiae extraction is performed on a data capture workstation with rapid and available processing capability then (a) a relatively small minutiae file, rather than a much larger image file, can be transferred to the central fingerprint matcher more rapidly and with less network demand and (b) the central server can devote more of its resources to the matching process by not having to perform minutiae extraction. If the captured image needs to be archived centrally, it could be stored temporarily on the local workstation and queued for transmission when network demands are low. Careful timing and cost analyses must be performed to determine the optimal design.

2.5 Applying multibiometric fusion techniques

The five basic categories of multibiometric fusion are multimodal (e.g., face, finger), multiinstance (e.g., left iris, right iris), multisensor (e.g., optical and capacitive fingerprint sensors; multispectral iris capture), multialgorithm (e.g., two different face matchers), or multipresentation (e.g., two right index fingerprints; multiple facial images from a video stream).[6] Fusion approaches offer creative opportunities to improve system accuracy, user convenience (lower FNMR), security (resistance to spoofing), throughput, and overall system flexibility. Fusion will likely be a valuable approach for addressing some of the performance needs of the large-scale systems noted earlier, where gallery size can easily grow into the hundreds of millions, and subjects and capture environments become more diverse. Research suggests that data quality is the performance-limiting factor when applying multibiometric approaches. The less correlated both the data being fused and the approaches being used by the fusion algorithms, the greater the performance gain to be achieved. [7,8]

Multimode approaches can help accommodate individuals who are unable to provide a particular type of biometric sample such as due to amputation or scarring, or can offer only a subpar presentation of the specific characteristic. Multialgorithm approaches can support more efficient and accurate matching, for example, if the poorest quality data is processed by the most robust but also the most resource-intensive matcher, while the highest quality data is processed by a simpler, faster, less costly matcher. Operational performance can be monitored over time and the system then tuned accordingly. As long as data and interface standards are adhered to, as more capable and less costly hardware and software components become available, individual components can be replaced to improve system performance and operational cost.

2.6 Implementing variable matcher thresholds and network queuing models to accommodate threat and workload dynamics

For a biometric system, FMR and FNMR vary inversely as matcher threshold is varied. Let's say we're designing a system to determine if foreign nationals entering a country at an air port of entry are on a terrorist watch list and match determination needs to be performed within seconds. A biometric check is performed at *primary inspection*; if an individual's biometric matches a biometric reference on the watch list, the individual is escorted to *secondary inspection* to confirm the match and take appropriate action (i.e., release or arrest). A lower FNMR will provide greater security; i.e., it is less likely that a terrorist crossing the border will not be detected. However, a matcher threshold that provides a lower FNMR also increases the FMR; therefore, a greater number of individuals not truly on the watch list will be flagged as likely terrorists, requiring that they undergo a secondary inspection process to determine if they are indeed on the watch list. Too large an FNMR will overload secondary inspection. If the queue in secondary inspection becomes larger than the physical space can accommodate, processing in primary inspection may have to be delayed. The queuing situation can become magnified by unexpected surges in transaction demand, for example, if several planes of passengers arrive simultaneously due to weather delays elsewhere. In such cases, it may be desirable to set the biometric matcher threshold to achieve an acceptably higher FNMR rate to reduce queues in secondary inspection. From a security standpoint, lowering the security level in this fashion may be a controversial decision requiring a well articulated and reasoned approach from the system owners. A thorough understanding and analysis of potential threats is critical in this regard. An integrated biometric performance and network queuing model along with the airline schedule and passenger counts could be used to visualize and determine acceptable matcher operating points and needed staffing.[9]

3. INTEROPERABILITY

Interoperability is significant at a number of levels. Clearly, if biometrics are to support homeland and global security, standardized data formats are required to take biometric data that is captured with one system and enroll and/or search it in another system. At the system level, the use of standards-based hardware and software permits component replacement as more capable and less costly items become available. This will increase system longevity and flexibility and also increase industry competition, which should stimulate increased product quality and decreased product cost. Dependence on single vendors will be minimized and system development and maintenance costs should also decline.

3.1 Adopting applicable standards

Various U.S. national and international standards have either been approved or are currently under development to address aspects such as software interfaces, file and data formats, and performance testing and reporting practices. The principal biometric standards organizations in the U.S. are the American National Standards Institute (ANSI) and International Committee for Information Technology Standards (INCITS) Technical Committee M1. Internationally, the principal standards body is the International Standards Organization (ISO) Joint Technical Committee (JTC) 1/Subcommittee (SC) 37.

In the U.S., the Biometric Application Programmer's Interface (BioAPI) standard specifies the software interface between application software and underlying biometric device-specific software. BioAPI also specifies a Common Biometric Exchange Formats Framework (CBEFF) Biometric Information Record (BIR) format for the storage and transmission of BioAPI-produced data. The CBEFF standard specifies the basic structure of a BIR, which includes the biometric data interchange record along with added metadata (e.g., date of capture, expiration date, whether encrypted and/or digitally signed). Data format standards have been developed for the exchange of fingerprint image, pattern, and minutiae; iris; face; hand geometry; and signature records. Standards have also been developed for performing biometric technology, scenario, and operational tests and reporting the results. Application profiles have been developed to indicate standards that should be adopted for a given type of application (e.g., Biometrics-Based Verification and Identification of Transportation Workers, Biometric-Based Personal Identification for Border Management, Point-of-Sale Biometric-Based Verification and Identification) and how those standards should be explicitly tailored to the application.[10, 11]

Prior to the development of the standards already noted, in 1993, ANSI and NIST developed a standard designed for the communication of biometric information within the law enforcement community, the *Data Format for the Interchange of Fingerprint Information* (ANSI/NIST-CSL 1-1993). In 2000, this standard was updated to *Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information* (ANSI/NIST-ITL 1-2000), which included specifications for mug shots, scars, marks, tattoos, and higher resolution palm and latent fingerprints. A further update of this standard to include additional biometric information, including iris and 10-print slap fingerprint records, has been produced and is expected to receive approval this year, *Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information* (ANSI/NIST-ITL 1-2007).[12] The FBI has implemented the ANSI/NIST standard in its *Electronic Fingerprint Transmission Specification* (EFTS). This year, EFTS will be updated to the *Electronic Biometric Transmission Specification* (EBTS version 8.0), which will keep it synchronized with the ANSI/NIST standard.[13] The U.S. Department of Defense has developed a similar implementation of the FBI standard, also called the EBTS, for communicating with its ABIS system.

It should be noted that INCITS M1 and ISO JTC 1/SC 37 have parallel working groups that have developed U.S. and international standards, respectively. Many of these standards are very similar and discussions are in progress to determine which, if any, of the ISO standards the U.S. should adopt. This would eliminate the extremely likely confusion that could develop from having pairs of similar standards.

With all the benefits that standards can offer, standards are not always a panacea for interoperability. For example, in 2004, NIST conducted the Minutiae Exchange Test (MINEX) to determine the feasibility of using minutiae data (rather than image data) as the medium for exchanging fingerprints between systems.[14] While a number of very interesting conclusions were drawn from this test, the fundamental finding was that vendors' native minutiae representations (i.e., templates) provided superior matching performance when compared with the use of the INCITS 378-2004 minutiae exchange standard. Although the standard does offer a good degree of interoperability, in this particular case, the price of interoperability is lower matcher performance.

3.2 Developing and using standardized test data

One of the challenges to developing and demonstrating the performance of biometric matching algorithms is the lack of standardized test data. Since human subjects are required, biometric data is very time consuming and costly to obtain. Privacy regulations prohibit the use of operational data from being shared and used for product development and testing purposes. Policies and approaches need to be developed to overcome this hurdle. Attempts have been made to develop large corpora of synthetic biometric data; however, to date, such attempts have received limited acceptance.

4. COST BENEFIT

4.1 Modeling system life-cycle costs

One of the reasons that organizations have been reluctant to implement biometric applications has been the inability to demonstrate cost benefit and return on investment. The true benefits of a biometric system are difficult to quantify and are also intangible to a large degree. Cost savings for benefit eligibility systems have been demonstrated at the local level; however, may of these biometric systems have resulted in shifts of abusers to other venues. Crime reduction benefits are virtually impossible to quantify because of the subjective nature of the benefits—how do you assign a dollar value to improving public safety? In addition, some obvious improvements result in increased cost, such as exemplified by the cost of incarceration. Many times, most of the benefits to be gained do not accrue to those who pay the bill.

Cost models are needed that reflect the life-cycle costs to acquire, operate, and maintain the overall system. These costs include the costs to acquire equipment, software, and facilities, as well as their associated maintenance costs. The labor component of the system must also be included. Within the integrated model, it is necessary to include biometric performance characteristics, anticipated workloads, and threat assessments. Models of matcher performance and subject queues can be used to develop a balance between workload, queue build-up, and security (i.e., error rate).

Many of the variables will be inter-related. For example, when using biometrics to perform a watch list check, the more people that are channeled to secondary inspection, the more facility space and agents that will be needed to perform this function.

4.2 Determining realistic performance requirements

Biometric systems are statistical in nature and have an associated error rate. The goal is to achieve as low an error rate as possible. However, the price that one would have to pay to achieve such a degree of perfection might be cost prohibitive. Therefore, when implementing a biometric-based system, one must ask the question "how accurate is realistically good enough?" To answer this question, it may be necessary to conduct a thorough threat analysis including obtaining cost estimates of potential adverse event impacts. Such an analysis will need to look at current security practices critically and collect highly sensitive data such as current manual inspection failure rates, incidents of tailgating and credential passback, and other compromising strategies. Addressing these needs requires strong and cooperative support from management and subject matter experts.

5. CONCLUSIONS

Significant advances continue to be made in biometric technology. However, the global war on terrorism and our increasingly electronic society have created the societal need for large-scale, interoperable biometric capabilities that challenge current off-the-shelf technology. At the same time, there are concerns that large-scale implementation of biometrics will infringe our civil liberties and offer increased opportunities for identity theft. This paper described, from a holistic point of view, a variety of considerations and approaches for achieving greater performance and acceptability of applications enabled with currently available biometric technologies.

REFERENCES

1. National Science and Technology Council Subcommittee on Biometrics, *The National Biometrics Challenge*, Washington, DC, August, 2006. http://www.biometrics.gov/NSTC/pubs/biochallengedoc.pdf
2. Benini, D. (editor), Biometric Sample Quality Standard Draft Revision 7, INCITS M1/06-1001, December 13, 2006. http://www.incits.org/tc_home/m1htm/2006docs/m1061001.pdf
3. National Institute of Standards and Technology, *Online Proceedings of the NIST Biometric Quality Workshop*, March 8-9, 2006 http://www.itl.nist.gov/iad/894.03/quality/workshop/presentations.html
4. Hicklin, A. and R. Khanna., *The Role of Data Quality in Biometric Systems*, Mitretek Systems, February, 2006. http://www.mitretek.org/Role_of_Data_Quality_Final.pdf
5. Theofanos, M., S. Orandi, et al., *Effects of Scanner Height on Fingerprint Capture*, National Institute of Standards and Technology, NISTIR 7382, December, 2006. http://zing.ncsl.nist.gov/biousa/docs/NISTIR-7382-Height%20Study.pdf
6. ISO/IEC JTC 1/SC 37/WG 2, *Multi-Modal and Other Multi-Biometric Fusion*, ISO/IEC JTC 1/SC 37 N1271, ISO/IEC WD3 24722, August 25, 2005. http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263034/2300190/JTC001-SC37-N-1271.pdf?nodeid=4446319&vernum=0
7. Ulery, B., A. Hicklin, et al., *Studies of Biometric Fusion*, National Institute of Standards and Technology, NISTIR 7346, September 2006. http://www.itl.nist.gov/iaui/894.03/pact/ir_7346.pdf
8. Korves, H., L. Nadel, B. Ulery, D. Masi, Multi-biometric Fusion: From Research to Operations, Sigma, Mitretek Systems, Summer 2005, pp. 39-48. http://www.mitretek.org/SigmaSummer2005.pdf
9. Ulery B., D. Masi, H. Korves, and S. McCabe, *The Challenge of Modeling Multibiometric Systems*, Sigma, Mitretek Systems, September 2006, pp. 30-36. http://www.mitretek.org/SigmaSep06_The_Challenge_of_Modeling_Multibiometric_Systems.pdf
10. Podio, Fernando, *National and International Biometric Standards—Status and Adoption*, presented to the Biometric Consortium Conference 2005, September 20, 2005. http://www.biometrics.org/bc2005/Presentations/Conference/2%20Tuesday%20September%2020/Tue_Ballroom%20B/Podio_Standards%20Session%20FINAL.pdf
11. Mayer-Splain, John, *Biometric Standards: A Primer and Update*, presentation to the Mitretek Biometric Identification Cluster Group, May 25, 2006. http://www.mitretek.org/HomelandSecurity/060525_-_The_World_of_Biometric_Standards.pdf
12. ANSI/NIST-ITL 1-2007 web site: http://fingerprint.nist.gov/standard/
13. FBI Biometric Transmission Specification version 8.0 web site: http://204.255.139.206/ebts/
14. NIST Minutiae Interoperability Exchange (MINEX) web site: http://fingerprint.nist.gov/minex04/Home.html