English Language Title: Standards and Biometrics

Author: Bradford J. Wing

U.S. National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL)

Submitted to: Congreso International de Biometría de la República Argentina (CIBRA), “Biometrias II” as an invited contribution.

ABSTRACT

This paper addresses the importance of standards when implementing or using biometric systems. Standards have been developed to ensure that biometric systems can effectively and accurately meet users’ needs such as protecting data integrity, privacy, and security. Examples are given to illustrate the problems addressed by standards in 18 aspects of biometric systems, such as biometric data capture, data transmission, and human factors. The principal standards used in the biometrics community are described and gaps in biometrics standards coverage are identified.

TEXT

1.0 Why have a biometric system?

The basic reason to have a biometric system is to verify the claimed identity of a person or to discover the identity of a person. A biometric system is designed to provide an answer to one of the following questions:

Is the person who he claims to be?

a. Verification (1 to 1 comparison): I have a passport with my facial image stored on the chip contained in the passport (an e-passport), and I claim that the e-passport was issued to me. I can use the ‘facilitated travel inspection lane’ successfully only if a picture taken of me at the kiosk matches the facial information stored in my e-passport.

b. Identification: (1 to many comparison): I am an employee at a factory that uses iris recognition to grant entrance to the facility. I can only enter if my iris image matches one in the database.

Is the person <u>not</u> who he claims <u>not</u> to be?

c. Negative verification: (1 to 1 comparison): I have been accused of a crime and I provide a DNA[1] sample to match against the DNA recovered from a crime scene. I am able to show that I am <u>not</u> the person whose DNA was left at the crime scene if there is no match.

d. Negative identification: (1 to many identification): In a certain nation, all persons that are deported have iris data captured at release. I arrive at the country's airport, have my iris scanned and can enter if my iris does not match one in the deportation database.

Can the person be identified, given the information in the system?

e. Identification: An Alzheimer's[2] patient is found wandering the streets. A fingerprint is taken from the person at a nearby police station, and it is compared against a database of missing persons. The print matches one in the database and the person is identified and returned to the family that had filed the missing person report.

f. Classification: Part of a body is found at a disaster site. A DNA sample is collected from the body and compared to DNA from possible relatives. In this case, the claimed relative is an uncle to two of the victims, and he provided a DNA sample. A match occurs for his mitochondrial DNA[3] to that of both of the victims. This means that the claimed relative and the two victims all have a common maternal ancestor. Mitochondrial DNA is only passed to a child from the mother. In this case, the common maternal ancestor is the grandmother, as shown in Figure 1. Positive identification of the corpse could not be established because the

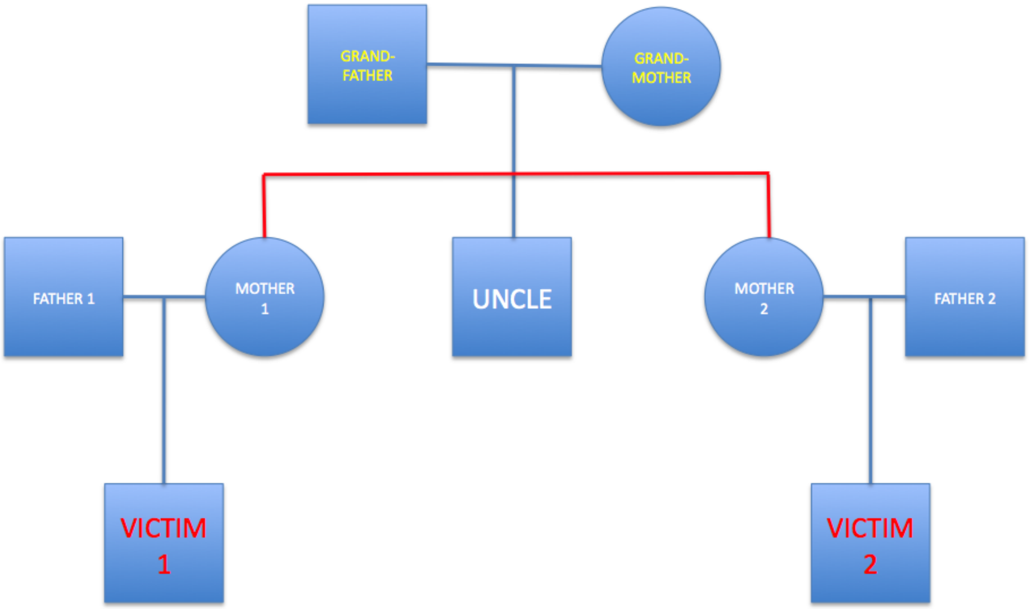
[1] DNA is an acronym for deoxyribonucleic acid. It is a chemical that forms a double helix, which is unique for all persons except identical siblings, for whom it is the same.

[2] Alzheimer's disease is the most common form of dementia. It is incurable.

[3] Mitochondrial DNA are small circular DNA molecules located in structures used to provide energy to the cell (mitochondria). Their small size and abundant nature make them particularly useful when examining small or severely damaged biological material. It can be used to trace maternal lineages as it is only inherited from one's mother.

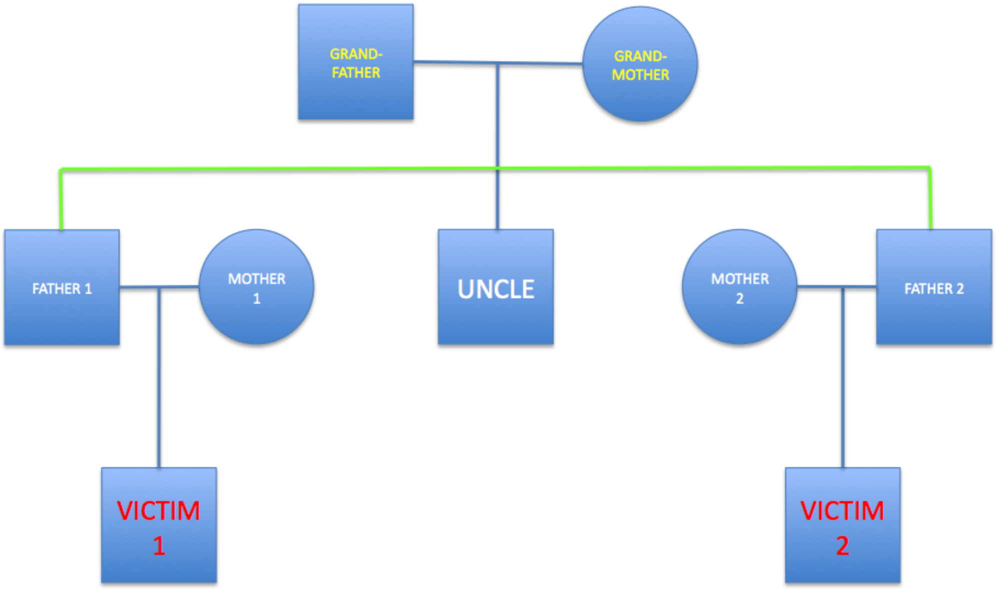
> body could have belonged to either Victim 1 or Victim 2, but the body is classified as being one of the two cousins, to the exclusion of all others.

Note that if the claimed relative (the uncle) had been a brother of the fathers of the victims, as shown in Figure 2, then the mitochondrial DNA test would not have revealed any usable results. If the uncle had been brother to a mother of one victim and father of the second, as in Figure 3, and there was a mitochondrial DNA match of the corpse and the uncle, then positive identification of Victim 1 as the son of Mother 1 could be established.



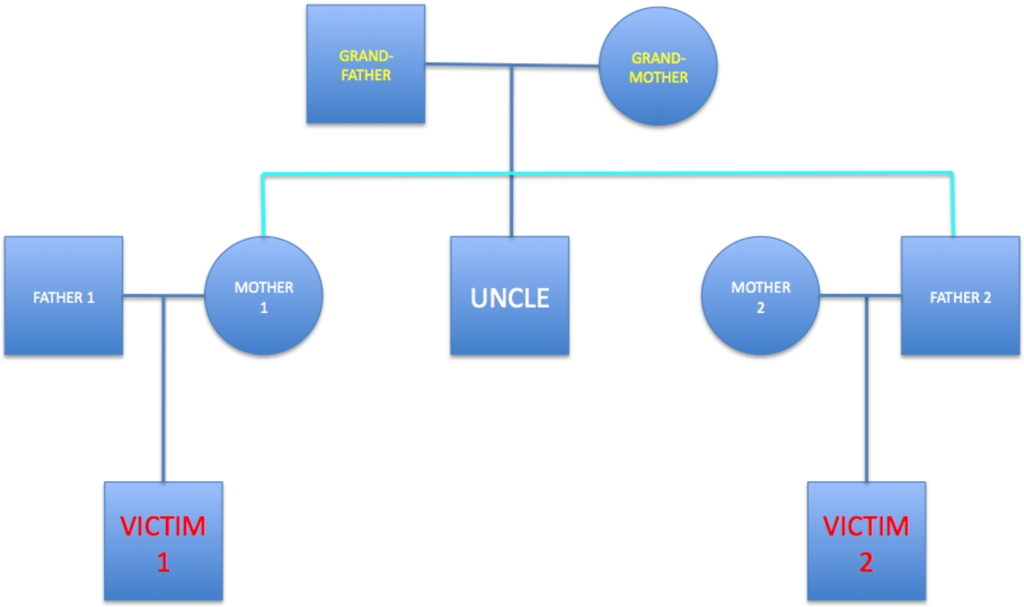
FAMILY TREE A

FIGURE 1



FAMILY TREE B

FIGURE 2



FAMILY TREE C

FIGURE 3

There are many variants on the above uses for biometrics, but they all have in common the fact that people rely upon the system providing a level of assurance that the result is correct.

A deployed system must take into account operational and cost constraints. Operational constraints include policy, legal, data integrity, security and privacy protections, interoperability with other systems, ergonomic considerations, environmental conditions, and many other factors. The data collected, stored, transmitted and used in a biometric system should:

- maintain fidelity to the biometric characteristics of the subject (the person providing the sample);
- describe the collection environment and procedures; and
- describe pertinent facts about the subject.

In addition, the system should:

- have a high degree of reliability, with
    - false match and non-match rates that are within tolerable ranges[4],
    - mean time between failure (MTBF[5]) that is acceptable, and
    - maintenance requirements that are reasonable[6]; and
- appropriately protect the subject's data.

2.0 What is the need for standards?

In order to help ensure that a biometric system is accurate, meets the system owner and user needs, and is able to interface with other systems (where appropriate), standards developing organizations (SDOs)[7] have created standards that can be incorporated into system design and standard operating procedures. Experts in the field, from government, academia, and private industry developed these standards. As a result of implementing standards in a biometric system's design, the system is less likely to be tied to a 'proprietary solution' of a specific vendor. Proprietary

[4] What the tolerable ranges are is a key decision of the system owner.

[5] The MTBF is dependent upon the system owner's definition of a failure.

[6] Some maintenance requirements can involve cleaning a fingerprint platen after every use. Battery replacement for mobile units is part of maintenance, so battery life is an important consideration. The system owner defines 'reasonable.'

[7] Section 4 describes the SDOs and standards that they have developed that are particularly relevant to the biometrics industry.

solutions can result in much higher costs, and possibly result in system failure if the vendor ceases to support the product. Failure to adhere to standards can also seriously degrade the integrity of the system.

'Application profiles' are based upon published standards. An organization tailors the standard to its particular requirements. An optional data field may be required for a particular type of application. Certain options allowed in the standard may be inapplicable to the needs of a particular organization. For instance the US Federal Bureau of Investigation (FBI), the US Department of Defense, the Royal Canadian Mounted Police, the Government of Argentina, INTERPOL, and others have developed application profiles of the standard "Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information" that is commonly called the ANSI/NIST-ITL standard[8].

There are also 'Best Practice Recommendations' (BPR) that describe the most appropriate selection of options and appropriate standards for various types of operational scenarios. An example is "Mobile ID Device Best Practice Recommendation Version 1.0"[9].

Not every step in a biometric system requires a standard. Many things can be addressed by "Standard Operating Procedures" and even common sense. However, there is a strong need for standards for certain parts of biometric systems, due to the severe impact that a failure to use a common format or procedure can have.

An operational (or designed) biometrics system can be discussed by examining it from different perspectives. Not all of the perspectives are relevant to every transaction or each biometric system. The key perspectives are addressed below using examples. They are not listed in order of importance or processing order within a system.

A) Biometric sample collection

Facial recognition algorithms work best with a full-frontal image. There is deterioration in the rate in recognition as the face moves away from the full frontal position. That is why passport facial pictures are required to be a full-frontal pose with a neutral expression, which has been formalized in the standard for international travel documents of the International Civil Aviation

[8] ANSI/NIST-ITL stands for American National Standards Institute / National Institute of Standards and Technology, Information Technology Laboratory. This means that NIST-ITL is accredited by ANSI as an SDO. ANSI/NIST-ITL 1-2011 and its predecessors are available at http://www.nist.gov/itl/iad/ig/ansi_standard/cfm. It is available in English only.

[9] The BPR is available at http://www.nist.gov/itl/iad/ig/mobileid.cfm. It is available in English only.

Organization (ICAO)[10]. Kiosks have been designed to capture full-frontal facial images in facilitated travel installations such as RAPID[11] in Portugal and SmartGate in Australia[12].

B) Associated metadata recordation

When a set of fingerprints is captured from an individual, it is important to label each print to indicate from which finger the image was captured. Large fingerprint systems may compare fingerprints only against those labeled as the same group (such as whorl) for a particular digit (such as index finger of the right hand). If there is no label, the systems may have to compare against all of the fingerprint images that have been stored – a costly and time-consuming process. Thus, standards like ANSI/NIST-ITL 1-2011 have fields that allow the entry of information associated with a fingerprint image, such as the finger position and the method of capture of the print (for example, rolled ink prints or livescan units).

In the 'classification' example described in Section 1.0, the metadata is extremely important. If the uncle were possibly related to the victims as shown in Figure 2, then a mitochondrial DNA would not have been run. An entirely different test (Y-Short Tandem Repeat[13]) would have been used.

C) Retrieval of biometric data to compare against

[10] The ICAO travel document standard, Document 9303, is available at http://www2.icao.int/en/MRTD/Pages/Document9303.aspx. It is available in Arabic, Chinese, English, French, Russian and Spanish.

[11] RAPID is a Portuguese Acronym for the phrase "Automatic Identification of Passengers Holding Travelling Documents"

[12] See Frontex technical report No 1/2010 "BIOPASS II, Automated Biometric Border Crossing Systems Based on Electronic Passports and Facial Recognition: RAPID and SmartGate" It is available at http://www.frontex.europa.eu/gfx/frontex/files/other_documents/biopass_II.pdf.

[13] Short tandem repeats (STR) are short sequences of DNA that are repeated numerous times in direct succession. The number of repeated units may vary widely between individuals and this high degree of variation makes STRs particularly useful for discriminating between people. The Y-chromosome is only in males.

When a biometric sample (called the 'probe' sample) is sent to a large-scale system, the probe may be compared against a subset of the entire database, called the target set. This target set may be selected based upon characteristics of the biometric data as well as its metadata, such as the sex and approximate age of the subject. If the accompanying information is incorrect or incomplete, as described in B) above, the target set may exclude the data associated with the correct identity in the database, causing a match not to be possible.

Some systems retrieve the target set from a 'token' such as an identification card with a chip embedded in it, or an e-passport. The target set in this example consists only of data for one person, the owner of the identifying document. In order to ensure that the token is properly used and that the biometric data on the card is only available to authorized systems, there is typically a control system built into the token. In the case of the identification card, the owner may enter a personal identification number (PIN) that authorizes access to the chip. For an e-passport, the information printed in the 'machine readable zone' on the data page is scanned and used to generate a 'key' to open the chip. Only then can the biometric data be retrieved.

The examples above illustrate different aspects of target set creation. Standards affect biometric systems in different ways.

D) Non-biometric factors affecting the biometric system

This is a very broad topic, and may result in the incorporation of other 'non-biometric' standards into a biometric system's specifications.

As an example, the ICAO standard for travel documents incorporates the ISO standard for optical character recognition, format B (OCR-B)[14]. The information stored using OCR-B printing on the 'information page' of the passport is used to generate a 'key' to open the chip contained in the e-passport in order to read the data stored on it. Without this key, the data cannot be read. This was done to ensure that the data on the chip could not be 'skimmed' by equipment in proximity to the e-passport without the information page being deliberately presented in close range to the authorized e-passport reader.

[14] ISO 1073-2:1976 is available at http://www.iso.org/iso_catalogue/catalogue_detail.htm?csnumber=5568. It is available in English and French.

E) Sample quality analysis

The quality of a biometric sample dramatically affects its usefulness. This applies to both the probe and the target set. If a fingerprint is smudged or if there was not enough pressure applied when it was captured, there may not be enough distinguishing features, such as minutiae, to enable a system to accurately match the sample against other samples. Automated quality analysis of the captured sample can be built into a capture device and provide feedback to the operator. For instance, the US-VISIT program[15] and United States ports-of-entry check the quality of the fingerprint captured at the time of capture. Up to three samples are collected and analyzed automatically by the system, and the best one is used. The operator also has the option to re-take the fingerprint of the traveler if the quality is of a poor level. The quality level of the fingerprint is stored with the fingerprint.

F) Initial data storage

The method and process of data storage, if done improperly, can negate the usefulness of a biometric sample. For instance, when a fingerprint image is taken, it should be stored with at least 19.69 pixels per millimeter, which equates to 500 pixels per inch (ppi). [1000 ppi is recommended for latent prints]. Compression algorithms are used to reduce the original image for more efficient storage and transmission. Certain compression algorithms, such as JPEG[16], were not specifically designed for fingerprints. JPEG forms squares across the image and compresses each square individually. When they are reconstructed, it is possible to introduce 'artifacts,' such a small line segments along the edges of these boxes. That is a real danger for fingerprints, since these artifacts could be interpreted as minutia and may cause a false match to occur or a valid match not to occur. A compression algorithm optimized for 500 ppi fingerprint images, called Wavelet Scalar Quantization (WSQ), is used to store those images. There are specifications for WSQ[17]. Vendors have developed different versions of software that does this compression.

[15] The document "Biometric Standards Requirements for US-VISIT" is available at http://www.dhs.gov/files/programs/gc_1213298547634.shtm.

[16] JPEG is an acronym for the Joint Photographic Experts Group. They created the standard, which is:
"JPEG File Interchange Format, Version 1.02 (JFIF)." It is available at http://www.jpeg.org/public/jfif.pdf.

[17] IAFIS-IC-0110 (V3.1) "WSQ Gray-scale Fingerprint Image Compression Specification, October 4, 2010" is available at https://www.fbibiospecs.org.

Fingerprints are submitted, for instance, to the US FBI from state and local police departments using a variety of implementations of WSQ. NIST validates these algorithms against the specifications. The FBI then publishes a list of approved vendor products for WSQ for use by law enforcement organizations when submitting fingerprints to the FBI.

G) Transmission to another location

The application of biometrics is not confined to one specific location. The capture of a biometric sample can happen at one location, and the matching of it against a database can be performed at a different location. The process of transmission must be clearly specified to maintain the integrity of the data.

For instance, there was a governmental fingerprint system that appeared to be well designed. Upon examination, the overall process was flawed. The original fingerprint image was stored in WSQ. Then it was decompressed, printed, and faxed to another site. At that location, the printed image from the fax machine was compressed in JPEG and transmitted to the central site, where it was decompressed and re-compressed using WSQ. The original sample was stored using WSQ and the final image was also stored in WSQ (so they could claim compliance with the recommended capture and storage compression procedures), but the fingerprint data had effectively been destroyed by the multiple format conversions during the steps of the transmission.

Many forms of compression are 'lossy.' This means that a certain amount of information contained in the original image is lost during compression. When decompressed, the resulting image will not be as detailed as the original image. For fingerprints, this can have extremely negative results.

To address this problem, the ANSI/NIST-ITL 1-2011 standard states: "Images shall be compressed only from an original uncompressed image. If an image has been received in compressed format, it shall not be uncompressed and re-compressed in the same or different format."

H) Comparison of the probe to the target set

The actual comparison of biometric information may be automated, partially automated, or manual. Automated fingerprint matching systems typically rely on a specified set of features within the fingerprint. The need to standardize the encoding of these 'fingerprint minutiae' for use by multiple matchers was recognized very early. In 1986, the first version of what eventually became the ANSI/NIST-ITL standard addressed fingerprint minutiae with the goal of ensuring that law enforcement organizations would be able to send information to one another without extensive re-coding of the data.

However, forensic examiners must rely upon more types of information than where ridges end and divide (bifurcations), which form the basis for minutiae. They must also be able to state their findings in a way that can be understood years later by other examiners. This led to the development of the Extended Feature Set, which is now incorporated into the ANSI/NIST-ITL 1-2011 standard. Forensic examiners can now specify in a fixed manner features such as the location of pores, the number of ridges in an area and other important characteristics. Fingerprint examiners in other locations, and perhaps separated by time, can refer to these features in a way that could have very important results in criminal prosecutions.

I) Biometric sample and metadata storage

In many applications, there is a requirement to use a minimum amount of space. An example is biometric data stored on an identification card used for building access. The data used by iris matchers can be stored in a very efficient manner (in some cases in as little as 3 kilobytes). This has been demonstrated through research conducted at NIST[18]. This analysis also found that one form of compact storage (polar format) resulted in degraded performance. The ISO and ANSI/NIST-ITL standards now both allow the 'crop and mask' format that has been shown to retain fidelity to the original biometric sample yet simultaneously reduce storage requirements. In order to maintain system accuracy, both the ISO and ANSI/NIST-ITL standard do not allow iris data to be stored in the 'polar' format.

J) Reporting and use of comparison results

[18] See http://www.nist.gov/itl/iad/ig/irex.cfm

The output of a biometric system is not necessarily a 'yes' or a 'no.' A probe of a biometric will always have slightly different characteristics than data in the target set, so a 'match' is never exact[19]. In fact, if it is exact, then that means that the probe and the target set data are from the exact same sample, which should raise suspicions about attempts to compromise the system. In many cases, there is only one set of data in the target set that is 'close' in comparison to the probe. In other cases, there may be several sets of data in the target set that are relatively similar to the probe. The presentation of results is generally not covered by standards. It is typically user-specified, based upon the system owner's requirements. For instance, the U.S. Department of State has a facial recognition system[20] used to verify that persons are not 'visa shopping' (applying at multiple consulates under different names in the hope that one application will be approved). The automated system provides a list of the 'best' matches of an applicant against the target set, which is comprised of previous visa applicants. A team of analysts then determines if there is a true or highly likely match.

Other systems, such as access control or computer activation (logical access control) require a yes/no decision. A 'threshold' is set for a match. That is, there have to be enough characteristics in common between the probe and the target set data. If that threshold is met, then access is granted. Since there is always a tradeoff between false match rate and false non-match rate, this threshold may be different for different circumstances.

A nuclear facility will set the threshold such that access cannot be granted unless there is a VERY close match in biometric characteristics. This means that a person will occasionally be denied entrance even though they really are authorized for entry. That is why a backup procedure should always be in place for biometric systems. On the other hand, an amusement park using a biometric verification system for season pass holders does not want to inconvenience its customers. The amusement park will usually set a lower threshold and accept that some transactions could possibly be performed by imposters and recognized as authentic by the biometric system. As biometric systems improve, the same level of true match can be achieved with lower and lower levels of associated possible

[19] It is possible under certain circumstances to have an exact match with DNA.

[20] The Consular Consolidated Database (CCD) Privacy Impact Assessment (PIA) is available at http://www.state.gov/documents/organization/93772.pdf.

false matches. In the amusement park example, this means that the threshold can be increased while still maintaining the same level of service to the customer, and with an even lower level of loss of revenue through unauthorized use of season passes.

The reporting processes and procedures and the setting of thresholds are based upon specific user needs and usually take into account scientific studies on biometric system performance. However, this is not currently seen as an area for standardization efforts.

K) Database analysis

Database analysis is critical in order to maintain a reliable and efficient biometric system. Database analysis encompasses several things, such as review of data associated with the biometric sample, quality analysis of the biometric data, and possible weighting of the matching results based upon those quality values and several issues directly related to the efficiency of the data storage structure and retrieval mechanism.

One aspect of database analysis that is critical is 'database reconciliation.' This can also be referred to as 'establishing ground truth.' For instance, the U.S. Border Patrol can apprehend the same individual multiple times as he or she attempts to illegally enter the U.S. A subject will often give the same name upon subsequent apprehensions since there is a potential for being sent to jail (instead of simply being expelled from the U.S.) if multiple attempts at illegal entry are detected. When fingerprints are taken of the subject, they are compared against a central system (in this example, IDENT). A photograph of the subject is linked to the metadata for the apprehension and to the fingerprint sample. The Border Patrol agent can 'link' two different claimed identities in IDENT based upon the results that are presented – thus establishing that at least two different aliases exist for the same individual.

Note that it is also possible to unlink two apprehension records if it can be shown that that they really do refer to different individuals.

L) Software and hardware reliability

This is an extremely complicated area. Several standards have been developed that apply to both biometric and non-biometric systems.

For instance, in the "Mobile ID Device Best Practice Recommendation Version 1.0" (BPR), there is a section that addresses environmental concerns. In the BPR there is a profile for law enforcement applications and a more stringent profile for military applications. A profile is a set of specifications. The BPR states: "It is the responsibility of the Agency to decide, in the procurement phase of the Mobile ID devices, which profile to request… It is important to choose the right profile since a lower profile could mean that the devices are not able to withstand the operating environment, causing costly failures and decreasing service levels, while choosing too high profile is likely to cause an unnecessary increase in the size, weight and cost of the devices."

For the different profiles listed in the BPR, standards are referenced that address testing of equipment for certain environmental conditions. An example is for the military profile, when testing for survival of mobile biometric devices at different operating temperatures: test using MIL-STD-810F Method 502.4 Procedure II at -20 degrees Celsius and use MIL-STD-810 Method 501.4 Procedure II at 60 degrees Celsius[21].

Categories of testing include operating temperatures, storage temperatures, relative humidity, ingress protection (resistance to water infiltration), and drop resistance / shock tolerance.

M) System performance analysis

System owners want to have the best performing system that they can afford while being suitable to their operating conditions. System performance evaluations can assist the algorithm and biometric system component developers as well as the systems owners. By running algorithms and components in controlled tests, their relative performance can be evaluated.

An example is the Slap Fingerprint Segmentation Evaluation II[22], run by NIST. It is an ongoing evaluation. Participants can submit their algorithms at any time to NIST. The concept is that certain fingerprint capture devices can acquire the images of four fingers at one time on a large platen. Then, the individual fingerprints must be 'segmented.' There can be several issues that complicate the segmentation, such as rotation of the hand on the platen, fingers being very close together, 'ghost' images of prints from residue on the platen, smudged or light

[21] The US Department of Defense test method standards for environmental engineering are available at http://www.dtc.army.mil/navigator.

[22] See http://www.nist.gov/itl/iad/ig/slapsegii.cfm

images of individual fingers, missing fingers, and heat ‘halos’ around the prints.

N) Legal and privacy impact analysis

The expectations and requirements for legal, cultural and privacy protection vary considerably in different jurisdictions. Regulation and SOPs to address these concerns are often written at the jurisdictional level, rather than formalizing the requirements into standards, due to these varying expectations and requirements.

For example, certain travelers, for cultural reasons, may wish to keep their face partially covered. However, their uncovered face image must be printed in the passport, according to ICAO travel document specifications. In order to perform a comparison of the traveler to the image in the passport, many jurisdictions have established special procedures to bring the traveler to a special screening area.

O) Human factors / human interface design

Only recently have standards and best practice documents been developed covering this aspect of biometric systems[23].

This area covers such diverse topics as listed below. These are only a few examples and are not an exhaustive coverage of the types of issues.

- What angle should the angle of the platen on a fingerprint capture device be relative to the subject? At what height should the device be placed?
- What symbols (icons) on biometric devices are most easily interpreted across cultures?
- How can the camera best assist the photographer to ensure that the subject’s face is centered and is at the proper distance from the camera?
- How can mobile fingerprint capture devices be designed so that they do not appear to be weapons to subjects, yet they can be operated using one hand by an officer?

[23] See http://zing.ncsl.nist.gov/biousa/ for several studies in human factors.

P) Interoperability design

This is a major driver behind the development of biometric standards. Isolated biometric systems (for example, access control for a small company) usually do not have a need to send data to other sites. However, as systems become larger, or there is a need to exchange biometric data with other systems. A common data format and understanding of the content of the biometric data ensure its proper use and allow for effective use in another system.

One example is a 'first responder' scenario. At a disaster site, personnel from several different organizations may respond. However, unauthorized persons should not be within the disaster zone. Firefighters from one jurisdiction may have had their fingerprints enrolled in their employment database. Medical practitioners at a local hospital may have had their fingerprints enrolled in the hospital's database. If each system had been designed to store fingerprint data in a standardized format, then a mobile system at the disaster site could be loaded with the fingerprint data of authorized persons. This eliminates the need to submit fingerprint samples of persons accessing the site to multiple systems for verification.

Another example involves INTERPOL. INTERPOL has established a database consisting of fingerprints of persons who are wanted for very serious crimes. The fingerprint data come from a variety of government agencies all over the world. Only because biometric standards are in place and used, can these prints be used by other agencies around the world to determine if they have encountered an individual in the INTERPOL database[24].

Q) Certification of biometric products, system testing laboratories, and testing procedures

When procuring equipment, system owners need to be assured that the equipment will work and will meet requirements. In the procurement process for large systems, the system owner can test the different vendor products in simulated conditions prior to making a purchase decision. However, such extensive testing is often too costly and time-consuming for smaller purchases.

[24] The INTERPOL implementation of the ANSI/NIST-ITL standard is available at http://www.interpol.int/Public/Forensic/fingerprints/RefDoc/ImplementationV5.pdf.

The types of tests and the methods of performing those tests have become a focus for standardization activities. NIST has established the Biometrics Laboratory Accreditation Program[25]. It is designed to verify that those laboratories that perform conformance tests, interoperability testing, technology testing, scenario testing, and operational and usability testing for biometric products follow nationally and internationally recognized biometric testing standards.

R) Security (information assurance, liveness and fraud detection,)

Certain aspects of security, such as information assurance, have several standards applicable to biometrics systems. These include encryption, hashing, digital signatures, and more.

The ICAO established a modified version of public key infrastructure (PKI) for use in e-passports. There is a document-signing certificate that verifies that the data have not been changed since it was written to the chip in the passport; this, however, does not guarantee which organization wrote the data to the chip. A country-signing certificate is also used in e-passports. The key to read the country-signing certificate is shared at the national level. If both certificates are valid, then the information on the chip in the passport can be considered genuine. Other types of checks must be performed to ensure that the printed data on the passport has not been altered.

Research into liveness detection and fraud analysis is underway at several universities and private companies. This involves detecting, for instance whether the biometric sample being captured is from a live subject and from the correct subject. For example, some fingerprint sensors may have heat-detection or vein-detection capabilities to help ensure that the subject is alive and that a severed finger or an artificial finger has not been presented.

Note that certain scenarios do not require or want liveness detection, such as when taking fingerprints from deceased individuals in order to identify a corpse.

3.0 What standards exist and how are they used?

Biometric standards were developed to meet specific needs of communities of users and to reflect the vastly different technological requirements inherent to the biometric modalities, such as DNA and facial recognition.

[25] See http://www.nist.gov/pml/nvlap/nvlap-bio-lap.cfm

Biometric systems may need to also rely upon other standards that were developed for a broad range of applications – such as the Federal Information Processing Standard 180, Secure Hash Standard[26].

The U.S. Government developed a publicly available list of relevant biometric standards. This "Registry of USG Recommended Biometric Standards"[27] has the following sub-registries:

- biometric data collection, storage, and exchange records;
- biometric transmission profiles;
- biometric identity credentialing profiles;
- biometric technical interface standards;
- biometric conformance testing methodology standards;
- biometric performance testing methodology standards.

The principal standards that are used internationally are:

- ANSI/NIST-ITL[28] Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information
    - Focused on law enforcement, military, intelligence, and homeland security applications
    - Application profiles developed for specific uses, such as:
        - FBI / U.S. police agencies
        - U.S. Department of Defense
        - Royal Canadian Mounted Police
        - Terrorist Watchlist Person Data Exchange Package
        - US-VISIT
        - INTERPOL
        - United Kingdom National Policing Improvement Agency
        - German Bundeskriminamt
        - European Union Visa Information System
        - Western Identification Network
    - Covers exemplar and latent friction ridge prints (fingerprint, palmprint, and footprints); images of facial / scar / needle mark / tattoo / iris / other body part and distinguishing characteristics; forensic markups of fingerprints, facial images, and iris images;

[26] SHA-256 hashes are described in this document and are the basis for some of the data fields in the ANSI/NIST-ITL 1-2011 standard. The standard is available at http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf.

[27] It is available at http://www.biometrics.gov/Standards/Default.aspx.

[28] For information, see http://www.nist.gov/itl/iad/ig/ansi_standard.cfm.

        - DNA; associated metadata; and, associated reference information, such as crime scene photographs.
    - Multiple modalities can be included in a single transaction
- ISO/IEC 19794-x (standards) and ISO 29794-x (conformance)[29]
    - Oriented toward civilian applications
    - Large-scale implementations using face, finger, and iris standards, such as
        - The Indian Unique Identification card (UID)[30] and
        - ICAO specifications for e-passports[10].
    - Covers several modalities and formats separately (finger minutiae, image, and spectral and skeletal pattern data; face image; iris image; signature / sign; vascular; hand geometry) for transmission and conformance testing
- CBEFF – Common Biometric Exchange File Format
    - Defines a set of 'header' information for a transmission
    - Allows the incorporation of biometric data and metadata conformant to several standards
- INCITS 381 (fingerprint images), INCITS 378 (fingerprint templates), INCITS 385 (facial images)[31]
    - Developed as US standards prior to the publication of the ISO/IEC 19794-x international standards
    - Used by the U.S. Government for the Personal Identity Verification (PIV) card[32].

4.0 What still needs to be done?

Although standards do exist to address several aspects of biometrics systems, there are still gaps to be filled. Additionally, existing standards need to be updated to reflect the changing requirements of biometrics system

[29] The list of published biometric standards and standards under development in ISO is available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45020

[30] Unique Identification Authority of India, "Biometric Design Standards for UID Applications". It is available at http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf.

[31] INCITS standards are available at http://www.incits.org.

[32] PIV standards and supporting documents are available at: http://csrc.nist.gov/groups/SNS/piv/standards.html.

owners and users as well as to reflect the results of research that has been conducted.

There are three principal forums that are currently developing and maintaining biometrics standards at the international level:

A) ANSI/NIST-ITL working groups

ANSI/NIST-ITL has recently published an updated version (ANSI/NIST-ITL 1-2011). Work is already underway to enhance the standard. Three working groups are now established to address:

- Dental and bitemark analysis;
- Voice recognition; and,
- Conformance testing.

B) ISO /SC37[33] (Subcommittee 37 – Biometrics)

ISO / SC37 has several projects underway. They include:

- Revisions to the existing standards;
- Voice recognition;
- DNA data; and,
- Pictograms, icons and symbols for use with biometric systems.

C) OASIS BIAS Integration TC[34] (Organization for the Advancement of Structured Information Standards, Biometric Identity Assurance Services Integration Technical Committee)

The OASIS BIAS Integration TC is focused upon providing a documented, open framework for deploying and invoking identity assurance capabilities that can be readily accessed through web services. The TC defines and describes methods and bindings that can be used within XML-based transactional web services and service-oriented architecture.

The following list is a sample of the topics under examination that may result in new or updated biometrics standards in one of the forums described above:

[33] Information is available at http://www.iso.org/iso/iso_technical_committee.html?commid=313770.

[34] Information is available at http://www.oasis-open-org/committees/bias.

- touchless fingerprints;
- transformation of a 3-dimensional fingerprint data set to be compared against 2-dimensional databases;
- ear shape;
- gait;
- human odor;
- ocular biometrics: the region around the eye as well as the eye;
- near- and mid-wave infrared facial imaging;
- aging of the subject and of the biometric sample;
- detection of deliberate changes to a biometric characteristic, including
    - plastic surgery of the face or
    - mutilation of fingerprints;
- detection of liveness of the subject;
- anti-spoofing techniques;
- optimization of the design of large-scale biometric systems;
- appropriate use of 'soft biometrics', including
    - height,
    - weight, and
    - skin color;
- multi-modal / multi-sample / multi-instance biometric data fusion;
- data quality analysis, at time of capture and once in the database;
- integration of other processes and procedures with biometrics, including
    - detection of facial micro-movements typical of deceit, and
    - artificial intelligence to assist forensic analysts;
- biometric system design for optimum performance by users and operators (usability and accessibility);
- new communication methods and capabilities; and

- dynamic decision making, including
    - automated or assisted modification of biometric system operational parameters based on current demands upon the system.

CONCLUSION

Standards are only meaningful if they are used. Standards will only be used if they serve a purpose and meet the needs of the biometric system owners and users. This is an ongoing process, but standards should remain stable enough that they can be effectively used over a period of years. Not all systems will be able to adapt to new standards at the same rate.

It is important for biometric system owners, developers, designers and users as well as researchers to reach out to the SDOs and participate in the development process.

For example, ANSI/NIST-ITL operates on the canvass method and is open to all interested parties. ISO / SC37 is organized around national body representation. Each participating national body establishes its own rules for participation, but they may be comprised of industry, government and academic experts. OASIS membership is open to all interested organizations.

It is an ongoing responsibility of SDOs to ensure that they have adequate representation from all interested groups in order to ensure that the standards that they develop are truly reflective of the community's needs and are simultaneously based upon solid scientific research.