Overview of Fingerprints and Biometrics at NIST

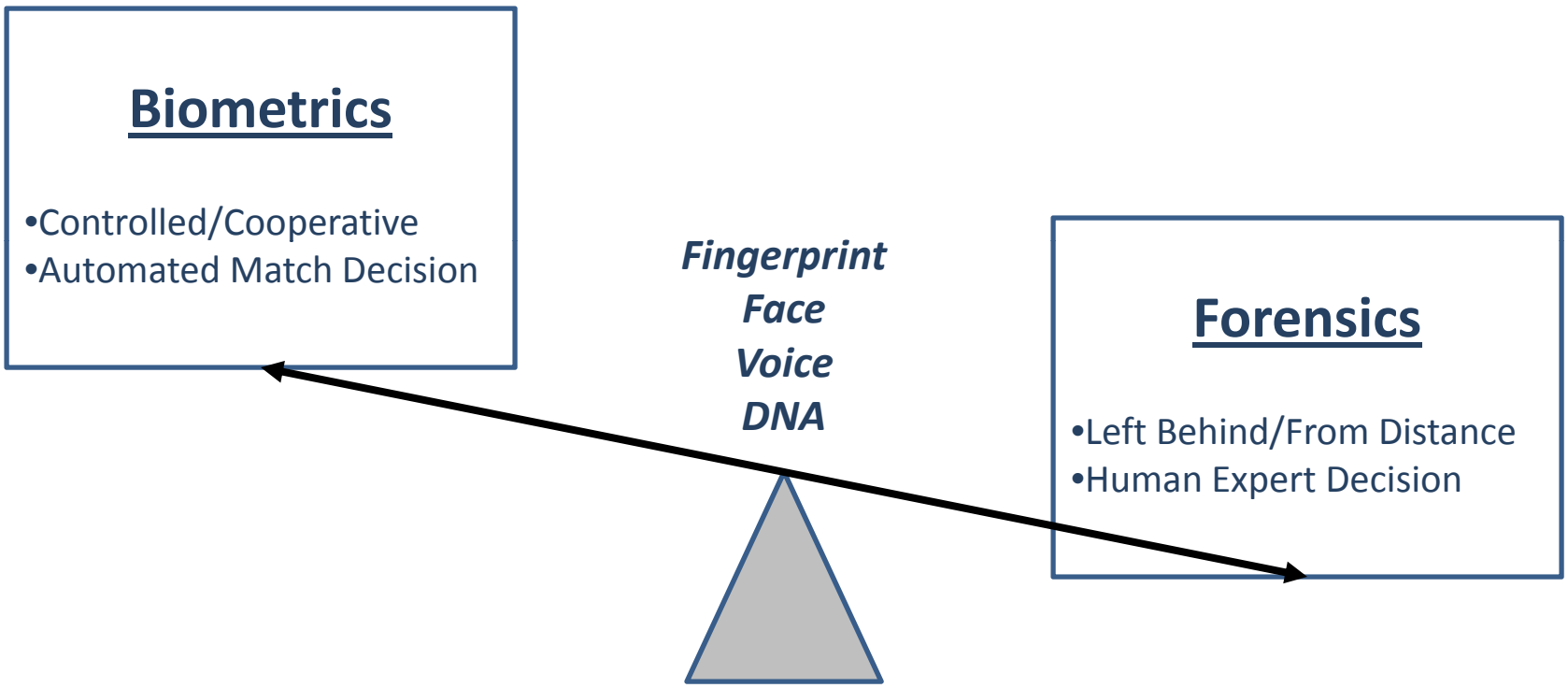
Forensics@NIST 2012

November 30, 2012

Michael Garris

Image Group Leader

ITL/Information Access Division


Biometrics
•Controlled/Cooperative
•Automated Match Decision
Fingerprint
Face
Voice
DNA
Forensics
•Left Behind/From Distance
•Human Expert Decision

Forensics@NIST 2012
Session: Fingerprints & Biometrics
November 30, 2012

Overview of Fingerprint and Biometric Activities at NIST

Mike Garris
ITL/Information Access Division
Image Group Leader

I. Welcome to the Last Session of the Symposium

A. In this session we will be discussing a variety of Research, Standards Development, and Evaluation activities related to fingerprints and biometrics that are taking place in various groups in the Information Technology Laboratory

B. I have been asked to moderate this session and to start it off with a brief overview

C. You might be wondering why talk about Biometrics at a Forensic Science Symposium?

1. I see the connection of fingerprints to forensics, but why the broader topic of biometrics?

II. How is Biometrics Related to Forensics?

A. **A Biometric** – a *measurable* anatomical, physiological, or behavioral characteristic that can be used for automated recognition

B. **Forensic Identification** is the application of forensic science and technology to identify specific objects (such as people) from the trace evidence left behind at a crime scene or the scene of an accident

C. If the trace evidence left behind includes a "biometric" then it could be used for "forensic identification"

1. Common examples are fingerprints and DNA left behind at a scene

2. But in our digital world, trace evidence may likely contain a photo, video, or voice recording thus linking face and speaker recognition technologies also to forensics identification

D. Two significant distinctions between biometrics and forensics

1. Biometric samples are typically collected under controlled / cooperative conditions while forensics data is "left behind" or observed from a distant sensor

2. The level of automation is also different – biometrics rely on an automated match decision while forensics rely on human expert decision

3. These factors can be thought of as two ends on a scale, and as an application or case moves from one end of the scale to the other, forensics begins to morph into something that looks much like biometrics and vice versa

III. A Brief History of Biometrics at NIST and in ITL

A. I am the 3rd generation manager of biometrics work that began at NIST in the Mid 60's

1. NIST researchers at the time partnered with the FBI to develop the first electronic fingerprint matching technologies
2. In the 80's ITL pioneered the very first biometric standard (a data format standard). Today the "ANSI/NIST-ITL Standard" is used around the world to support data exchange for Law Enforcement, Border Security, and it is rapidly expanding to support Forensics
3. Upon the tragic events of 9-11, and with our decades of expertise in fingerprint technologies and standards, Congress called upon ITL through mandates of the USA PATRIOT ACT and Enhanced Border Security and VISA Entry Reform Act to lead the testing and establishment of biometric standards to enhance national security
4. Today NIST is a world leader in developing and promoting biometric standards and conducting biometric technology evaluations; and we expect the momentum of this impact to continue to carry over into forensics

IV. How can we apply what we do in biometrics to forensics?

A. Take image-based biometrics as an example – specifically fingerprints

1. Develop and promote Open Standards
   a) Data Format Standards –
      (1) For exchanging the fingerprint image, image attributes, feature templates (minutia data), subject's biographic descriptors, and encounter data (e.g. date, time, & location)
   b) Conformance Test Suites
      (1) The existence of a data format standard alone is not enough to guarantee an implementation meets the technical requirements specified in a standard
      (2) Conformance Testing measures whether an implementation faithfully implements the standard to see if it functions appropriately by presenting a suite of correct and incorrect data cases
   c) Performance Testing Standards
      (1) What methods, metrics, and with what level of uncertainty will performance results (such as throughput and accuracy) be reported
      (2) I would like to point out that measuring and understanding the error rates of forensic applications was a key topic of study called for in the 2009 NAS Forensics Science Report

2. Technology Evaluations & Challenge Problems

    a) Help spur competition and innovation by benchmarking the state-of-the-art and exploring the art-of-the-possible

    b) We are currently running a 1-to-Many fingerprint evaluation involving the participation of 21 different organizations including all major vendors. There are 80 different algorithm submissions being tested on enrollment galleries as large 5 million subjects (50 million fingerprints)

3. Research in Data Quality Metrics, Usability, & Interoperability

4. Bi-products from this work includes

    a) Standard Reference Datasets

        (1) Provides researchers with sample data needed to develop new pattern recognition technologies

    b) Baseline Recognition Technologies

B. This expertise in Image-Based Biometrics can be transferred to Pattern-Based Forensics

1. Work has already begun with OLES to support a standards and evaluation project in Ballistics and Firearm Tool Marks

2. We are making great progress with creating a standard data package for Dental Records and Bitemarks

3. Our Latent Fingerprint Matching work is expanding into Palmprints

V. This Session's Line-Up

A. Research, standards, and evaluation projects in Fingerprints, Face, & Voice

B. So without further delay I would like to start our next talk