Homeland Defense & Security Information Analysis Center

HDIAC Biometrics Webinar

Identifying Priorities for R&D in Biometric Technologies
April 28, 2015

Erik J. Bowman
Technical Fellow, NGIS &
Chief Engineer DoD ABIS Program

Homeland Defense & Security Information Analysis Center (HDIAC)
(865) 535-0088
www.hdiac.org

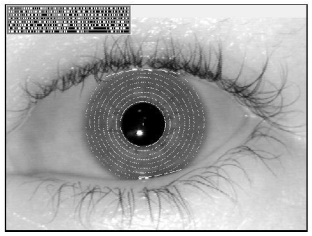
DoDIACs
Department of Defense Information Analysis Centers

Agenda

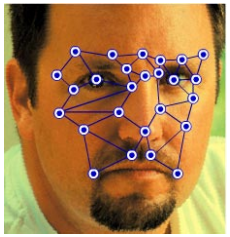
1. Biometrics – A Primer on how the industry defines itself
2. Biometrics Transaction Processing – 100,000 Foot View
3. Industry Trends & Research Problems

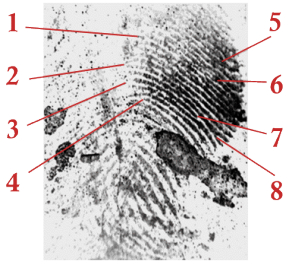
What are Biometrics?

Automated methods of identifying or verifying an individual based on physiological or behavioral characteristics



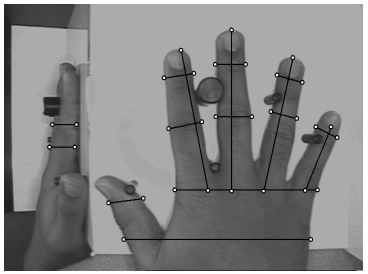
Iris



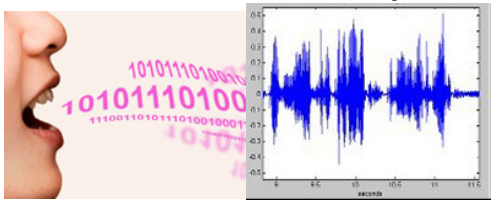


Latent Fingerprint

Fingerprint



Hand Geometry



Voice

Automated Methods

- Anything a machine can perform by itself without human intervention

- We perform automated biometric identification every day
  - Recognizing the voice, face, or interesting behaviors of your friends (or enemies)

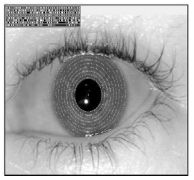
Biometric Systems try to automate what humans do every day.

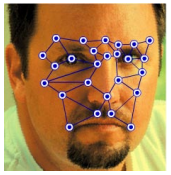
Identifying or Verifying

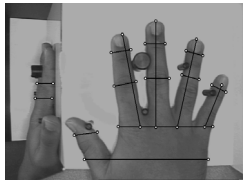
- Identification
  - "Have I seen you before?"
  - Trying to find a needle in a haystack
  - 1: Many search type
  - Applications include: National Identification, Border Crossing …
- Verification
  - "Are you who you claim to be?"
  - Allowing a person logical or physical access to a resource
  - 1:1 search type
  - Application include: Physical Access Control, Logical Access Control, Time and Attendance

Physiological or Behavioral

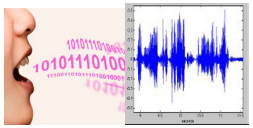
- Physiological Traits *typically* don't change over time
  - Fingerprint
  - Palm
  - Face
  - Iris
  - Hand Geometry

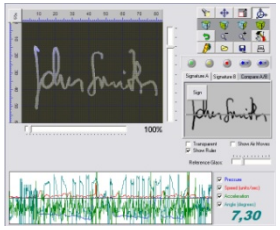


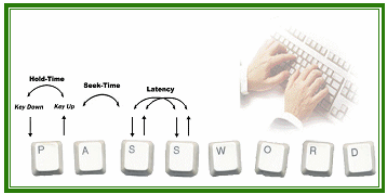




- Behavioral Traits tend to change frequently
  - Voice
  - Signature / Handwriting
  - Gate
  - Keystroke Dynamics



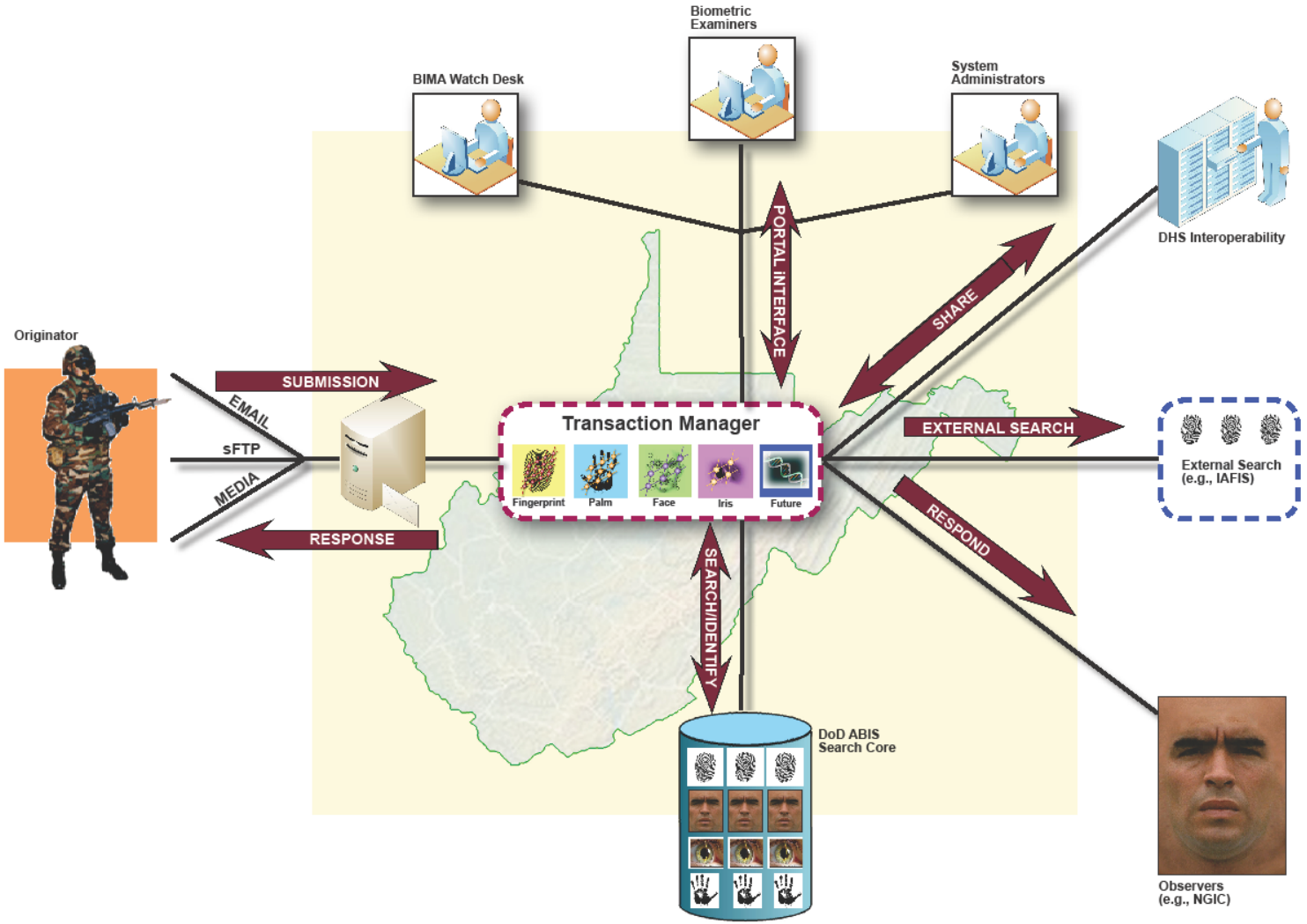




Biometric Processing

(100K Level View)

Biometric Transaction Operational View



Essential Customer Functions

Ingest	Pre-Processing	Search	Post-Processing	Response
Receive input	Add privacy act disclaimer to search request data (ASL/RFP field) if biometric subject is US person	Send search to IAFIS	Aggregate COTS search results	Determine response TOT
Determine submission type	Validate and repair search request data	Determine search core search requests for individual modalities	Compute fusion score	Determine response recipients
Authenticate submitter	Store submission data • Store biographic and contextual data • Store biometric image and/or template data	Send search requests to COTS search engine	Determine automated decision	Determine output format(s) for response recipients
Verify application profile domain and version on AP white list	Generate external submission	Store biometric image and/or template data	Request manual review	Strip protected encounters from list of matching encounters
Verify TOT is authorized for submitter	Perform bulk delete		Send yellow notification to submitter	Generate response
Reject search request if biometric subject is US person and submitter is not authorized to submit US person			Store final decisions (includes dispositions made by examiners and automated matches by search core)	Send response
Reject duplicate submissions			Update identity structure	
Validate TCN			Check for watch list hits	
Send submission receipt			Generate enrollment keys and enroll templates in COTS search cores, if biometrics are to be retained	
Assign priority to search request				
Create submission DB record				
Create transaction				

Large Scale Biometric Programs

1. DoD ABIS – (Non-Cooperative Mission all 1:N)
   - ~12 Records, 15K Transactions Per Day
2. UK NPIA - IDENT1 (Forensic Mission all 1:N and 1:1)
   - ~ 15M Records, 47K Transaction Per Day
3. DHS - IDENT (Cooperative Mission – 1:1 and 1:N)
   - ~200M Records, > 200K Transactions Per Day
4. UKBA - IABS (Cooperative Mission – 1:1 and 1:N)
   - 12M Records, 10K Transactions Per Day
5. FBI - NGI (Cooperative Mission – 1:1 and 1:N)
   - 33M Criminal + 33M Civilian Records, 120K Transactions Per day
6. UID – India (Cooperative Mission – 1:1 and 1:N)
   - 200M Records enrolled of 600M, minimal 1:N searching as enrollment is key
7. DoS Face Recognition – (Cooperative Mission – 1:1 and 1:N)
   - 200M Records, 40K Transactions Per Day

Industry Trends & Research Problems

Industry Trends

- Business
  - Mergers and Acquisitions are likely to continue within the industry…barriers to entry will become cumbersome for small players
  - Consolidation of State AFIS markets being led by Vendors (NEC)
  - COTS providers becoming medium systems integrators
  - Medium scale biometric programs abroad (Australia/New Zealand, UK)
  - COTS biometrics research and development turning to Cloud (NEC, MorphoTrust)
  - Financial industry will continue to push biometric usage
  - Mobile giants will continue to implement multiple biometric modalities
  - National identity schemes will continue

- Technology
  - Traditional DNA is here now
  - Alternatives to RAPID DNA coming out universities
  - Multimodal biometric fusion will become more important to large-scale systems
  - Voice biometrics (speaker identification) are on the rise
  - Identification of individuals in non-ideal environments (indoor, outdoor, pose angles)
    - Face/Gait/Voice recognition in video surveillance
  - Cloud-based solutions versus High Performance Computing

Research Questions

- How do we drive down the total cost of ownership of a biometric system?
- How do we increase the accuracy of our system?
- How do disparate systems share data to create actionable intelligence?

Academic Research (CITeR)

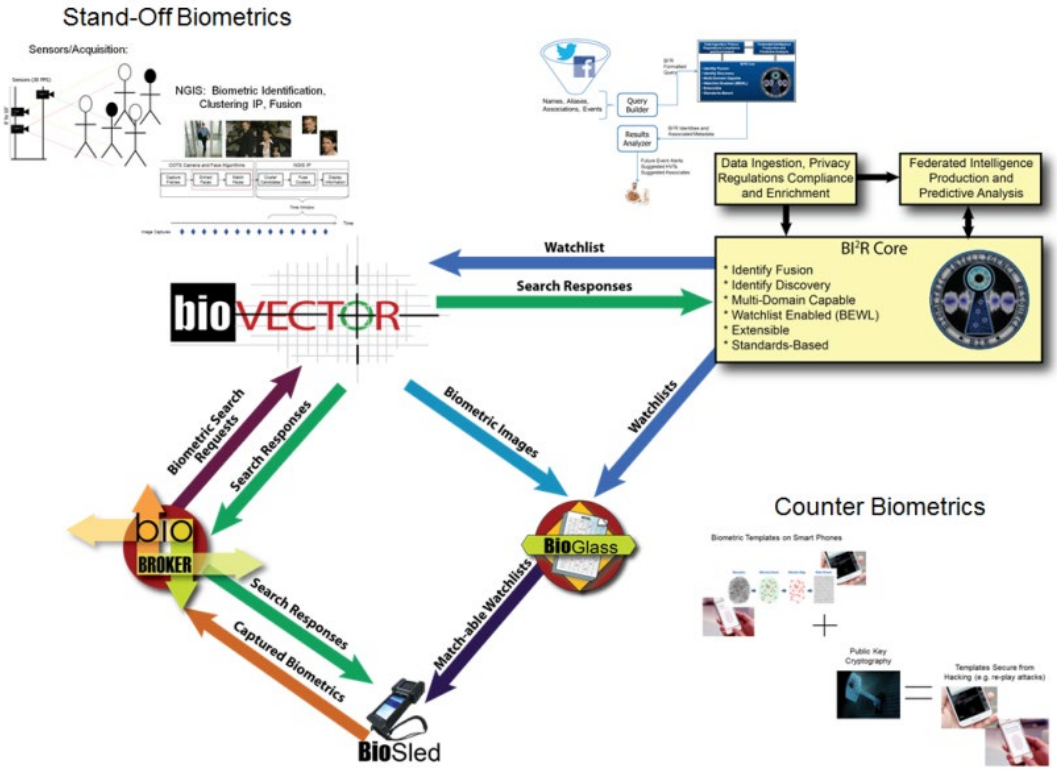
- 20 funded research projects being studied by leading universities

- Topics include:
  1. Liveness detection for fingerprints
  2. Credibility and Deception detection
  3. Cancellable biometrics
  4. Heterogeneous face recognition (still to video)
  5. Cross device, cross distance matching face with mobile devices
  6. Active and long term user authentication
  7. Writer identification and verification
  8. Fingerprint identification: a longitudinal study
  9. Touch DNA
  10. Fusing biometric and biographic information

Commercial Research Priorities

- Mission thread focused
- Very large-scale processing
- Multimodal biometric collection and matching
- Stand-off biometric capture and matching
- Increasing accuracy as datasets get larger
- Cloud

Collect, Store, Match, Analyze, Act



- Customer proven core capabilities offered by BioSled, BioVector, the BI2R Core, BioBroker, and BioGlass
- These proven capabilities will be bolstered with further IR&D in Stand-off capture/match, Counter Biometrics, BI2R in a cloud and on a mobile device (e.g. BioSled), and data sharing will complete the entire lifecycle of the identity dominance chain
- This results in NGIS being able to offer the complete life cycle for identity dominance
- These capabilities provide definitive answers to the following two questions:
  - Do I know who you are?
  - Can I determine intent?

Mobile

- Samsung Galaxy S5 Android Smart Phone
- Fingerprint: Integrated Biometrics Sherlock
  - FBI Appendix F Certified, FAP 45
- Iris: IriTech IriShield
  - Dual Iris, SAP 30
- Face: Samsung Galaxy S5 Camera
  - 14 megapixel, SAP 52

High powered, standards-based biometric device aimed at usability and affordability

Stand Off Biometrics "Recognizing Faces in a Crowd"

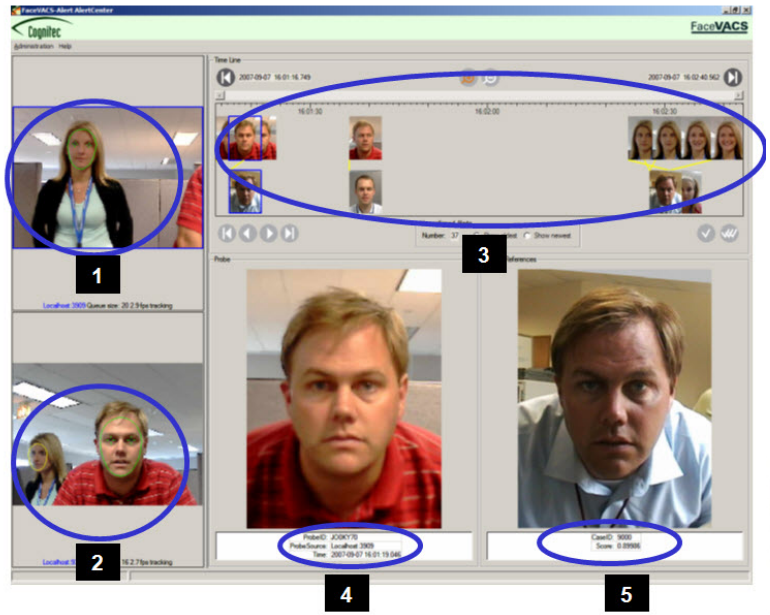
Number 1
- IP Camera input 1
- Subject A - green outline indicates face and eyes have been located

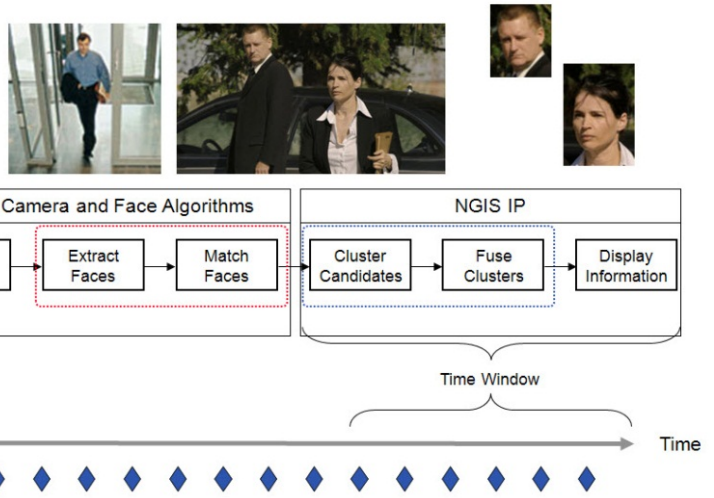
Number 2
- IP Camera input 2
- Subject B - green outline indicates face and eyes have been located
- Note the background Subject A with a yellow circle indicating a head has been found

Number 3
- Multiple Probe images that are alerts from the video feeds are tracked along a timeline against gallery images providing detail on when the alert happened

Number 4
- Detail on the probe image (including camera and timestamp) are shown here

Number 5
- Detail on the gallery image against which the probe is matched are shown here. In this case a match score of 0.89986 is shown

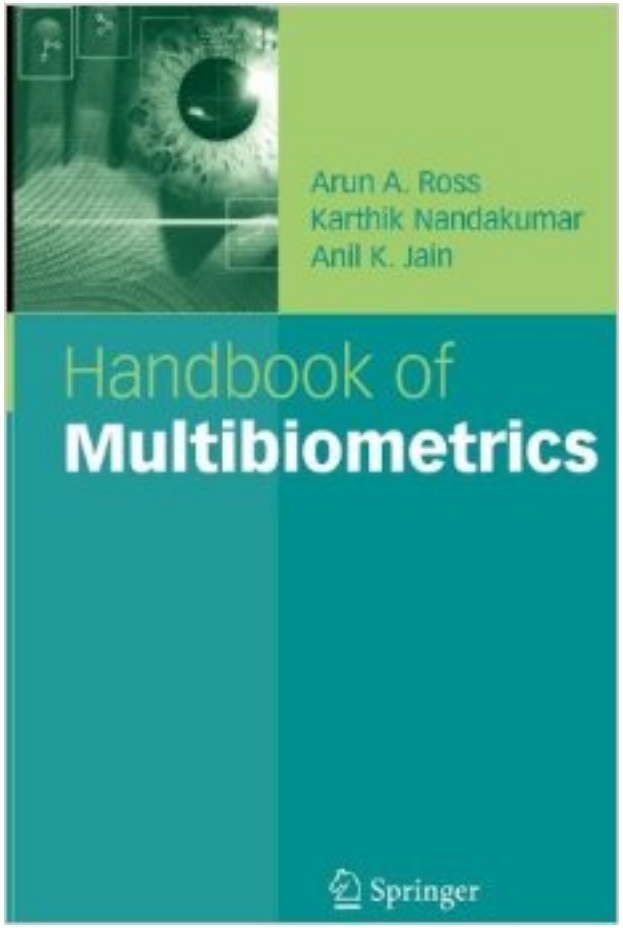




Finding faces in crowd involves COTS biometric matching software and NGIS intellectual property to reduce the false alarm rate

Multimodal Fusion

- Fusion is a technique for combining information from multiple sources in order to increase accuracy
- Fusion is critical for biometric systems of the future with steadily larger databases
  - Accuracy declines as database size grows
  - Without increased accuracy, larger database sizes lead to greater demand for human verification of results that are not sufficiently certain
- For multiple biometrics such as fingerprints, face, and iris, a fusion algorithm is needed to combine results from separate matching algorithms for each modality



Comparison of Fusion Strategies

Strategy	Description	Advantages	Disadvantages
Feature Level	Combining multiple sources to extract features more accurately	Improved feature extraction	Not mature, an academic research area at best
Sensor Level	Raw data from the sensor is combined, e.g., multiple fingerprint impressions	Improved accuracy, especially for latent prints	Not yet available in products and requires multiple samples
Score Level	Scores from multiple matchers are mathematically combined	Proven effective in IDENT1 and some COTS products	Scores from multiple vendors or modalities are not generally comparable
Rank Level	Candidates are combined using relative position in the candidate list, not match score	Makes few assumptions about meaning of scores so is theoretically more sound than score level	Does not use score information so does not give an indication of confidence of result
Multi-Strategy	Twp or more strategies are combined, e.g., score level for some types of biometrics, rank level for others	Goal is to improve accuracy beyond what a single strategy can do	Ad hoc and hence hard to create a general approach

Cloud and Biometric Processing

- Clearly advantageous in terms of computing resources

- Security questions remain open
  - In an infrastructure as a service who is responsible for securing the data?

Contact HDIAC

Mr. Stuart Stough
HDIAC Director
Oak Ridge, TN
sstough@hdiac.org
(865) 813-1067

Website: www.hdiac.org
E-mail: info@hdiac.org
Phone: (865) 535-0088

Department of Defense Information Analysis Centers