EXPLORING BIOMETRIC VALIDATION APPROACHES IN THE AGE OF COVID-19

Presented by:
Abdul Rahman, Ph.D.

HDIAC Homeland Defense & Security Information Analysis Center

4695 Millennium Drive
Belcamp, MD 21017-1505
dsiac.org

Office: 443.360.4600
Fax: 410.272.6763
Email: contact@dsiac.org

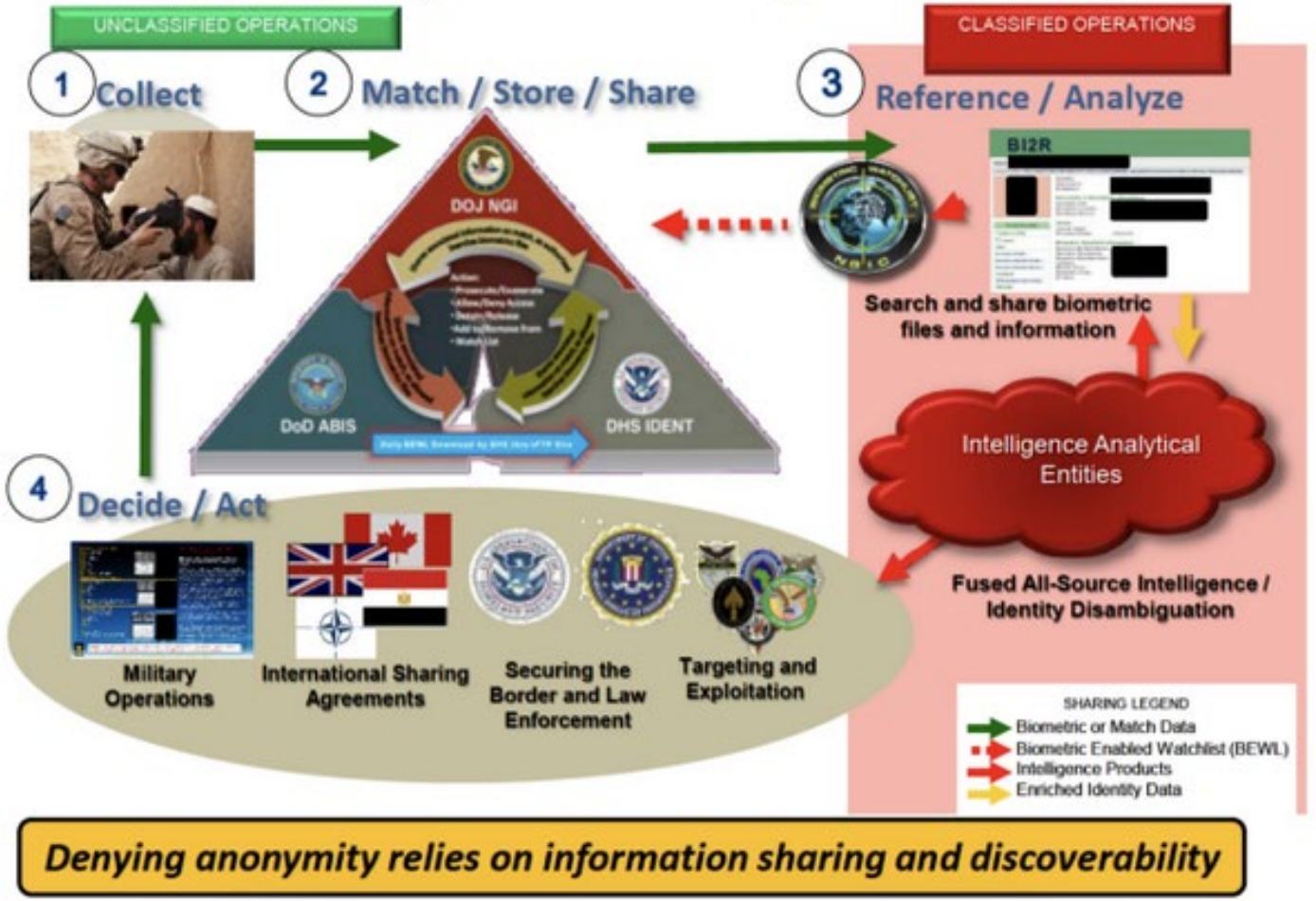
Overview

- Biometric systems use the observed biological or behavioral traits of individuals to create unique identifiers for use in comparison against biometric templates.
- The joint ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) standardized vocabulary for biometrics defines a *biometric characteristic* as "a biological and behavioral characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition."
- The most common biometric modalities in use today include the face, fingerprint, DNA, gait, palmprint, and iris.
- The field also encompass traits like voice signature, shape of the periocular region (around the eyes), vascular or vein patterns, cardiac rhythm, and skin texture.
- While traditional systems are uni-modal, multi-modal data fusion holds promise to significantly improve existing recognition and identification tasks.

Biometrics and National Security

- Biometric recognition technologies are used widely across the federal government, primarily by the DoD, DHS, and DOJ.
- Biometrics are a critical resource for forward-deployed U.S. forces as well as homeland defense operations.
- Accurate recognition and identification allows warfighters to fix (and track) the identity of an individual regardless of disguises, occlusions (masks), or expression.
- This is particularly beneficial in low-illumination, long-distance, or low-quality sample capture environments.

Current DoD Biometrics and Identity Intelligence Cycle and Challenges



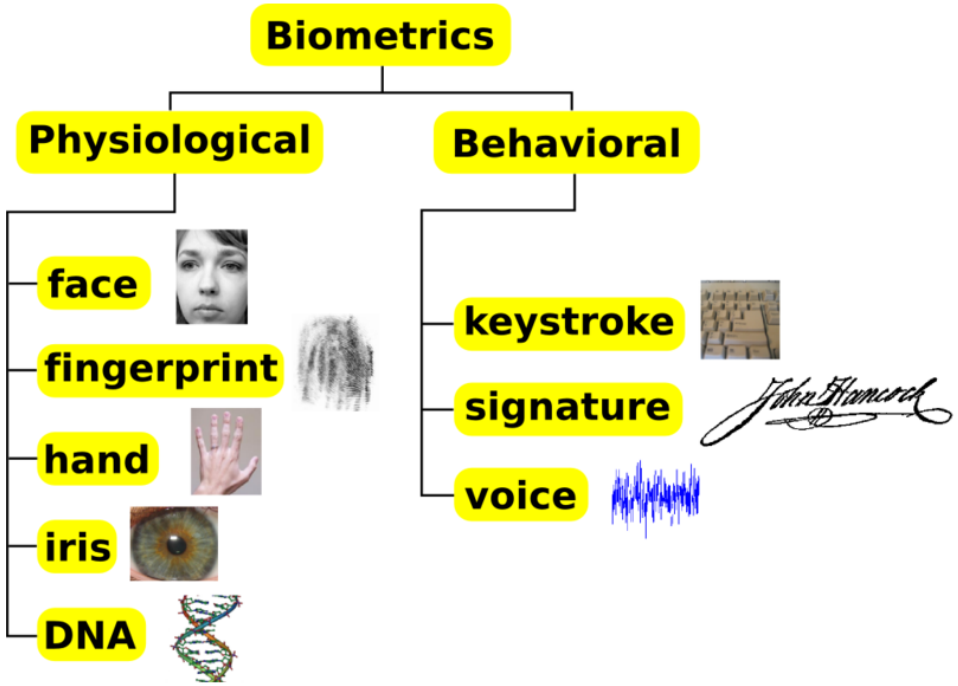
Source: Glenn Krizay, "Leveraging Biometrics within the National Defense Strategy – Draft," June 2019.

TRADITIONAL BIOMETRIC VALIDATION

7 Characteristics of a Biometric Trait

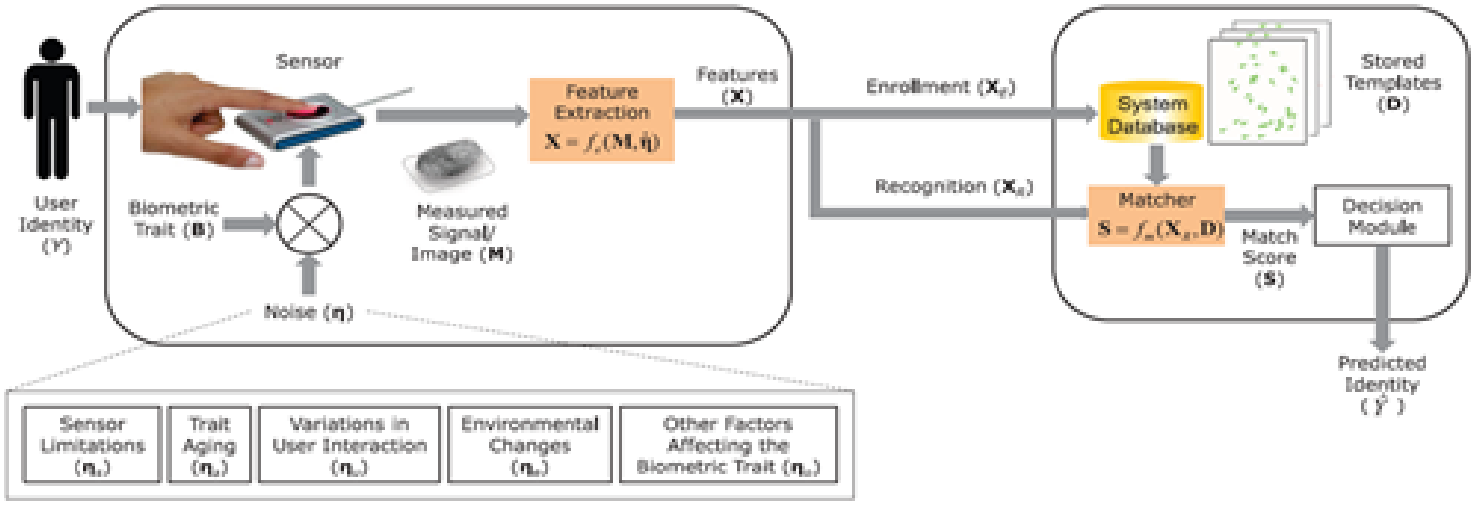
A usable biometric trait for identification or recognition displays seven fundamental qualities:

1. *universality* (qualities per user)
2. *uniqueness* (a subject's distinguishing features)
3. *permanence* (its inability or unlikelihood to change over time)
4. *measurability* (ease of acquisition of the biometric data sample)
5. *performance* (functional and robust properties of the trait)
6. *acceptability* (acceptability by the system user)
7. *circumvention* (the ability to spoof or deceive the recognition system)



Source: Wikimedia Commons, 2007. https://commons.wikimedia.org/wiki/Category:Biometrics#/media/File:Biometrics_traits_classification.png

Architecture of a Biometric System



Source: Jain, Anil & Nandakumar, Karthik & Ross, Arun. (2016). 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. Pattern Recognition Letters. 79. 10.1016/j.patrec.2015.12.013.

- Enrollment and recognition are the two stages central to most biometric systems.
- A biometric feature set is a representation of extracted features that are quality checked prior to storage in the template database.
- These feature sets are processed during enrollment, leading to a usable digital representation of the extracted traits. Recognition is facilitated through the comparison of acquired biometric capture data against previously stored templates to return a match if one exists.

Uni-Modal Biometrics

- Traditional biometric verification and identification systems are uni-modal: matching a fingerprint, face image, etc., in isolation.
- Uni-modal facial recognition systems are widespread and typically return a high positive rate of identification due to large enrollment datasets, mature feature extraction and matching techniques, and its reliance on passive recognition.
- The COVID-19 pandemic has challenged this: wearing a mask occludes ~70% of the face and use with sunglasses or face shields can further stymie feature extraction.

Uni-Modal Biometrics

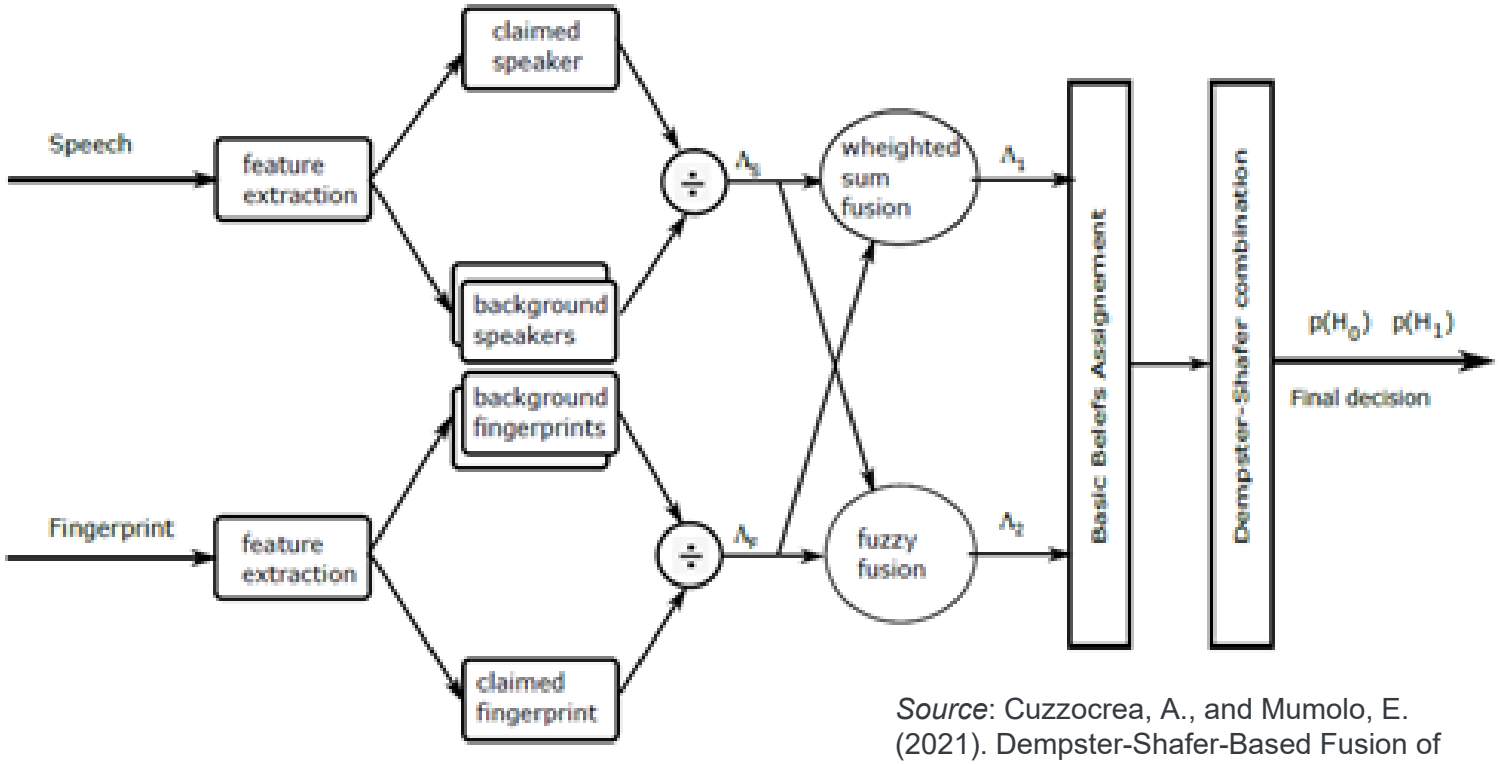
- In July 2020, NIST assessed the efficacy of pre-COVID facial recognition algorithms on faces with digitally applied masks.
  - The most accurate pre-COVID algorithms had a false non-match rate (FNMR, assuming false match rate of 0.00001) of 0.03% of unmasked persons using border crossing images. When using masked images, their FNMR rose to about 5%.
  - Other leading pre-COVID algorithms returned false non-match rates as high as 50%.
  - NIST also found that mask coverage of the nose, the shape and size of a mask, and its color also affected FNMR rates.

Digital application of mask shapes to photos by the National Institute of Standards and Technology

Source: NIST, Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms, July 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf

Multi-Modal Biometric Systems

- Multi-modal systems combine multiple biometric characteristics.
- This is the most relevant type of data fusion for next-generation sensing and control systems, as it can leverage two or more biometric modalities.
- Examples are the face, finger, hand, legs, iris, voice, etc., yielding face recognition, fingerprints, hand geometry, gait, iris scan, and voice recognition.

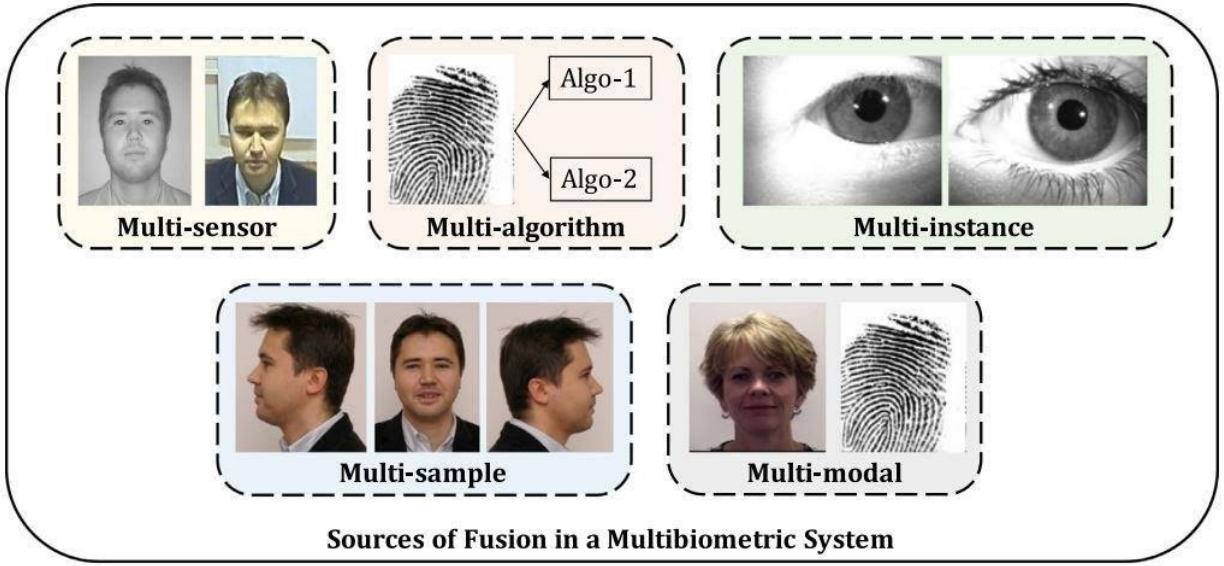


Source: Cuzzocrea, A., and Mumolo, E. (2021). Dempster-Shafer-Based Fusion of Multi-Modal Biometrics for Supporting Identity Verification Effectively and Efficiently, *2021 IEEE 2nd International Conference on Human-Machine Systems (ICHMS)*, 1-8.

DATA FUSION IN BIOMETRIC VALIDATION

Data Fusion in Advanced Biometrics

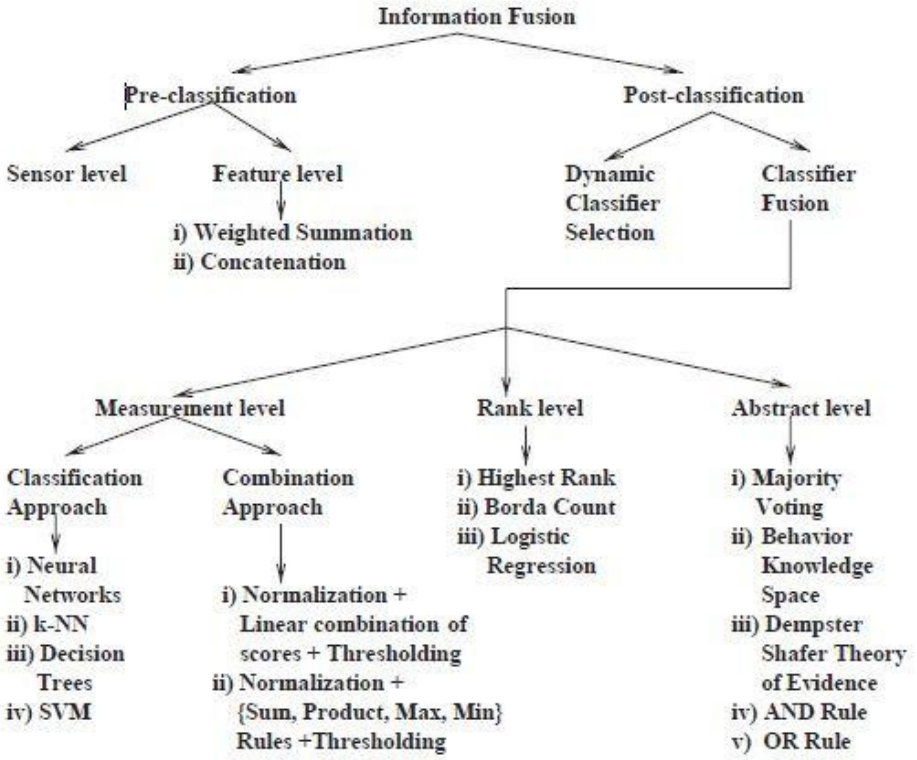
- Recent advances beyond uni-modal recognition and identification are termed *multibiometric*.
- Sources of fusion include:
  - *Multi-sensor*
  - *Multi-algorithm*
  - *Multi-instance*
  - *Multi-sample*
  - *Multi-modal*



Source: Singh, R., Ross, A., & Singh, M. (2019). A Comprehensive Overview of Biometric Fusion. *Information Fusion 52*, 187-205.

Data Fusion in Advanced Biometrics

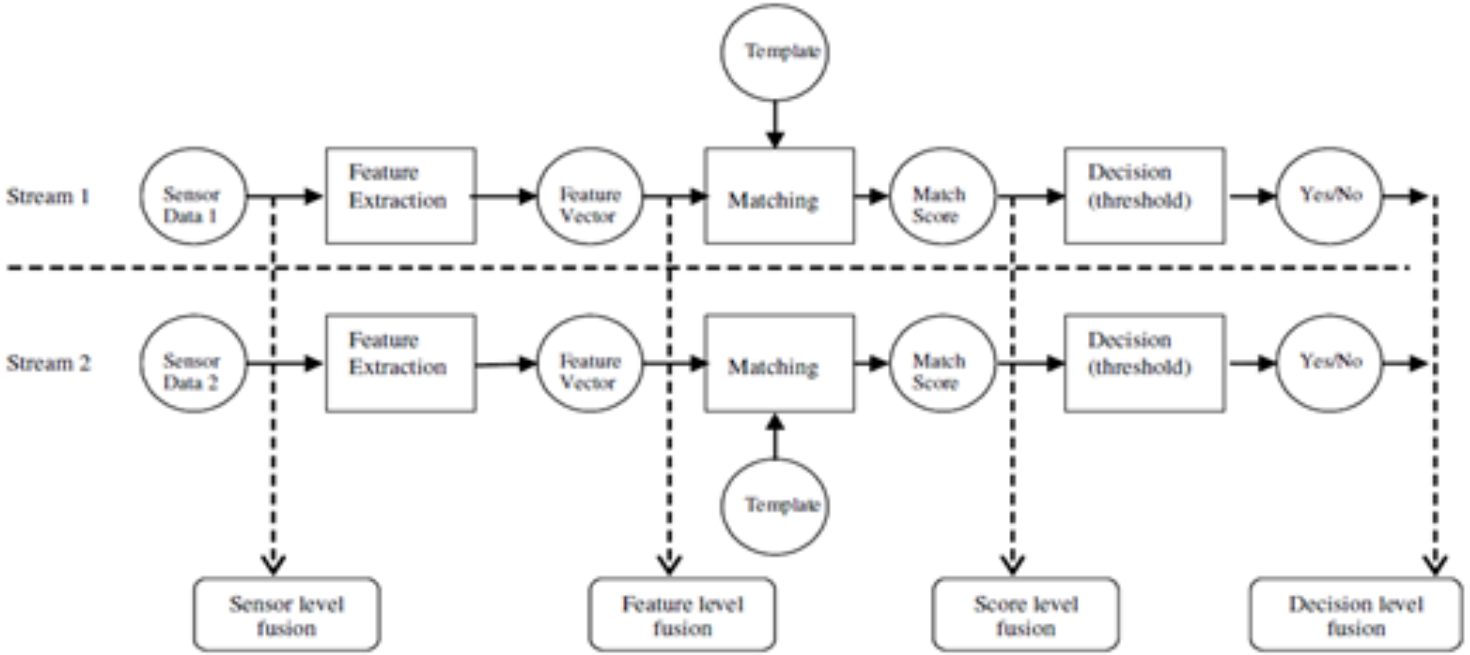
- Data fusion can also occur at the analytical level rather than at the source collection level alone:
  - *Sensor-level*
  - *Feature-level*
  - *Score-level*
  - *Rank-level*
  - *Decision-level*



Source: Jain, A., Qian, J.-Z., & Ross, A. (2001). Information Fusion in Biometrics. *Proc. of 3rd Int'l Conference on Audio- and Video-Based Person Authentication*, (pp. 354-359), Sweden.

Data Fusion Levels

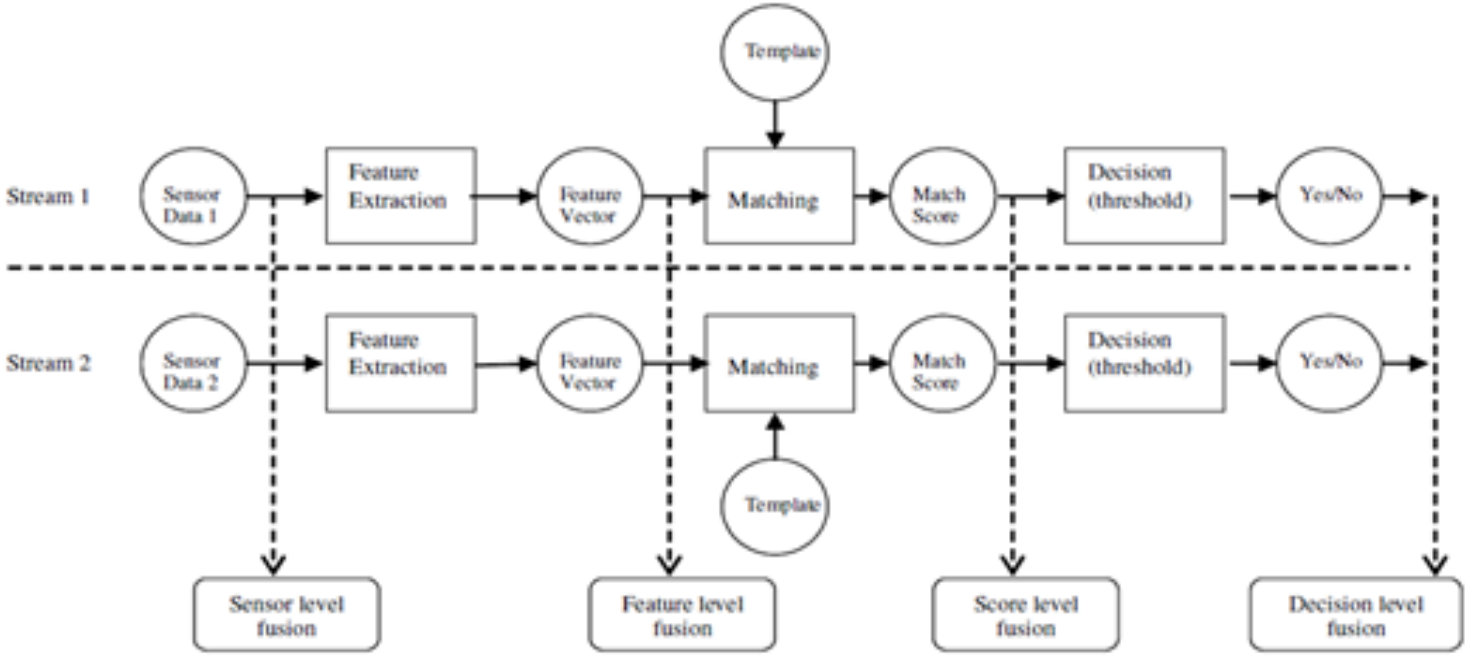
- Rank-level: in rank-level fusion, the classifier (matcher) compares each enrolled biometric trait against all the identities stored in the database.
- Decision-level: decision-level fusion (also referred to as the abstract level) fuses together information taken from different sources after each has been classified individually; it then makes the final decision based on methods such as the "AND" and "OR" rules, using weighted voting. This is a later-stage approach for fusing data for each biometric and is the least powerful.



Source: Alsaade, F. (2008). Score Level Fusion for Multimodal Biometrics. Ph.D. Thesis, University of Hertfordshire, Hatfield, UK.

Data Fusion Levels

- Feature-level fusion: feature-level fusion uses feature vectors originating from multiple biometric sources or feature vectors from the same source using multiple feature extraction. Feature vectors are fused together to create a new single feature that represents an individual [9]. This is done via appropriate feature normalization, transformation, and reduction schemes.



Source: Alsaade, F. (2008). Score Level Fusion for Multimodal Biometrics. Ph.D. Thesis, University of Hertfordshire, Hatfield, UK.

Artificial Intelligence (AI) & Machine Learning (ML)

- Combining multibiometric approaches with AI and ML tools provides the best approach to increase verification accuracy.
- AI/ML algorithms can increase speed as well as accuracy.
- Current top algorithm-type candidates include Gaussian Mixture Models, Artificial Neural Networks, Fuzzy Expert Systems, and Support Vector Machines.
- Future improvements will require more data, more data sources, and more types of data sources on which to train AI-ML algorithms.

Deep Learning (DL) and Data Fusion for Biometrics

- The application of DL methods to biometrics data fusion holds promise to overcome the limitations of traditional uni-modal methods.
- Prior DL approaches have relied on weight combination, or feature concatenation, which constructs representation layers for recognition stages.
- Due to the difficulty of fusing multiple modalities for recognition based on inherent modality inconsistencies and technical fusion obstacles, these methods are generally understood to be inefficient.
- A path to overcoming these challenges is provided through the utility of convolutional neural networks (CNNs), which enable highly improved recognition via multi-fusion network layers that drive robust and informative model learning.
- Furthermore, the broad applicability of these DL methods to modality fusion supports more compact and discriminative feature representations.
- This, in turn, facilitates improved predictive power in multi-biometric systems.

Summary

- DL models that employ multiple layers require large volumes of data in order to significantly outperform traditional analytical methods based on convex optimizations (e.g., linear and kernel methods).
- For DoD operations, long distances between network nodes can add latency or delays in communication beyond the optimal.
- Upstream fusion of data from multiple sensor types and modalities improves target detection and classification by forming data vectors, prior to degradation due to statistical algorithms applied to data.
- Next-generation, multi-modal biometric data fusion efforts that use multi-stream, multi-sensor, and multi-modal sources may be best fused upstream and through the application of DL methods to produce a biometric recognition system that integrates all available identity operations information.

Questions?

EXPLORING BIOMETRIC VALIDATION APPROACHES IN THE AGE OF COVID-19

Presented by:
ABDUL RAHMAN

4695 Millennium Drive
Belcamp, MD 21017-1505
dsiac.org

Office: 443.360.4600
Fax: 410.272.6763
Email: contact@dsiac.org

HDIAC Homeland Defense & Security Information Analysis Center