U.S. Navy Biometrics: An Overview

Anh N. Duong
USN Biometrics Lead
OPNAV N3/5 & NCIS Science Advisor
anh.duong@navy.mil

February 2008

Why Biometrics?

- **Military operations**
  - **Physical Security / Force Protection**
  - **Real-time tactical & strategic decisions during battlefield & interdiction operations**
  - **Disaster / humanitarian relief**

- **Business Functions**
  - **Physical and logical access controls**
  - **Privilege management**
    - **Health care, benefits, finance, time and attendance, etc.**

Required Capabilities

- Efficiently enroll, verify and identify individuals encountered in the conduct of operations
- Rapidly compare identity info to watchlists
- Rapidly record various types of information associated with an individual
- Rapidly recall, update and manage ‘trusted’ information associated with individuals
- Rapidly assess credibility of witness/INTEL source
- Share information
- Operate in austere, expeditionary environments
- Operate remotely/non-intrusively against non-cooperative subjects

Navy Thrusts

- **Navy Ashore**
  - Entry Control Point (OPNAV N4/CNIC, NAVFAC & SPAWAR)
- **Navy Afloat**
  - EMIO Capabilities Enhancement (OPNAV N6, PMW-160 & SPAWAR)
  - Identity Dominance System (OPNAV N8, PMS-480 & NSWC)
- **Navy Law Enforcement/Counter Intel/Intel**
  - Forensics (NCIS)
  - Exploitation (ONI)
- **Navy RDT&E**
  - Face Recognition Technology (ONR)
  - Fusion (ONR)
  - Biometrics to Human Networks (ONR)
  - Forensics (N-PSEAG)

Navy Ashore Thrusts

Entry Control Point

- Deployment of biometrics-enabled entry control will be based on Required Operational Capabilities (ROC) priorities

- Awaiting OSD policy. Main issues:
  - ❖ Databases
  - ❖ Interface hardware & software
  - ❖ Local vs. central data storage
  - ❖ Trusted travelers

- Physical Security Equipment Action Group (PSEAG) is building a Joint common interface via which all Services can access required government databases, using COTS at entry points

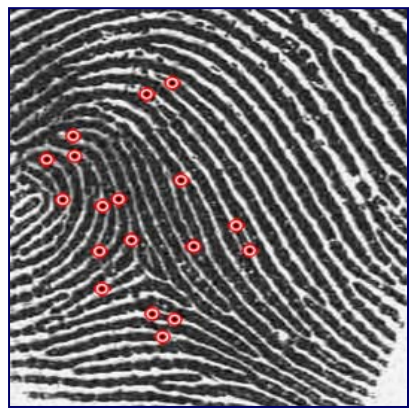
Navy Afloat Thrusts

Maritime Interdiction Operation (MIO)

- Stop-Gap solution acquired via Rapid Deployment Capability
- NAVCENT issued policy for Biometrics collection
- Long-term requirements described in the Identity Dominance System CDD
- Wireless Shipboard System being developed
  - For communication between boarded vessel and Navy ship

Navy Forensics Thrusts

- **Team DON (USN/USMC/NCIS) is creating and deploying Joint Expeditionary Forensics Facilities for CENTCOM**
  - **Latent Print**
  - **Firearms**
  - **DNA**



Naval RDT&E Thrusts

- **Office of Naval Research (basic & applied research)**
  - **Pattern Recognition**
    - **Face Recognition Technology**
  - **Human Activity Recognition**
    - **Biometrics from Intelligent Video Surveillance**
    - **Human ID at Distance, including Maritime Domain**
    - **Face biometrics from video**
  - **Face/activity recognition to Human Networks**
  - **Night biometric technologies**

- **Navy Physical Security Equipment Action Group (advanced development, prototype and demonstration)**
  - **Mobile and modular forensics lab design**
  - **Forensics training kits for war fighters (in partnership with TSWG Forensics & Training Subgroups)**
  - **Battlefield Evidence Information Management System (BEIMS)**

Future Needs

- Continued improvement in face recognition for outdoor, night and non-cooperative subjects
- Data fusion of multi-biometrics (face, iris, hand, motion)
- Biometric-quality face data from surveillance video
  - Automatically correct images to optimize matching algorithms
- Face and iris biometrics at greater ranges
  - Correct for air turbulence, moisture and motion blur
  - Nominal 300 M face, 20 M iris
- Biometrics to Actionable Intelligence
  - Accurate classification of human networks enabled by the fusion of data from all possible identity specific technologies
    - Biometrics
    - Tagging, tracking and location
    - Symbols of choice (email address, phone number, address, name...)