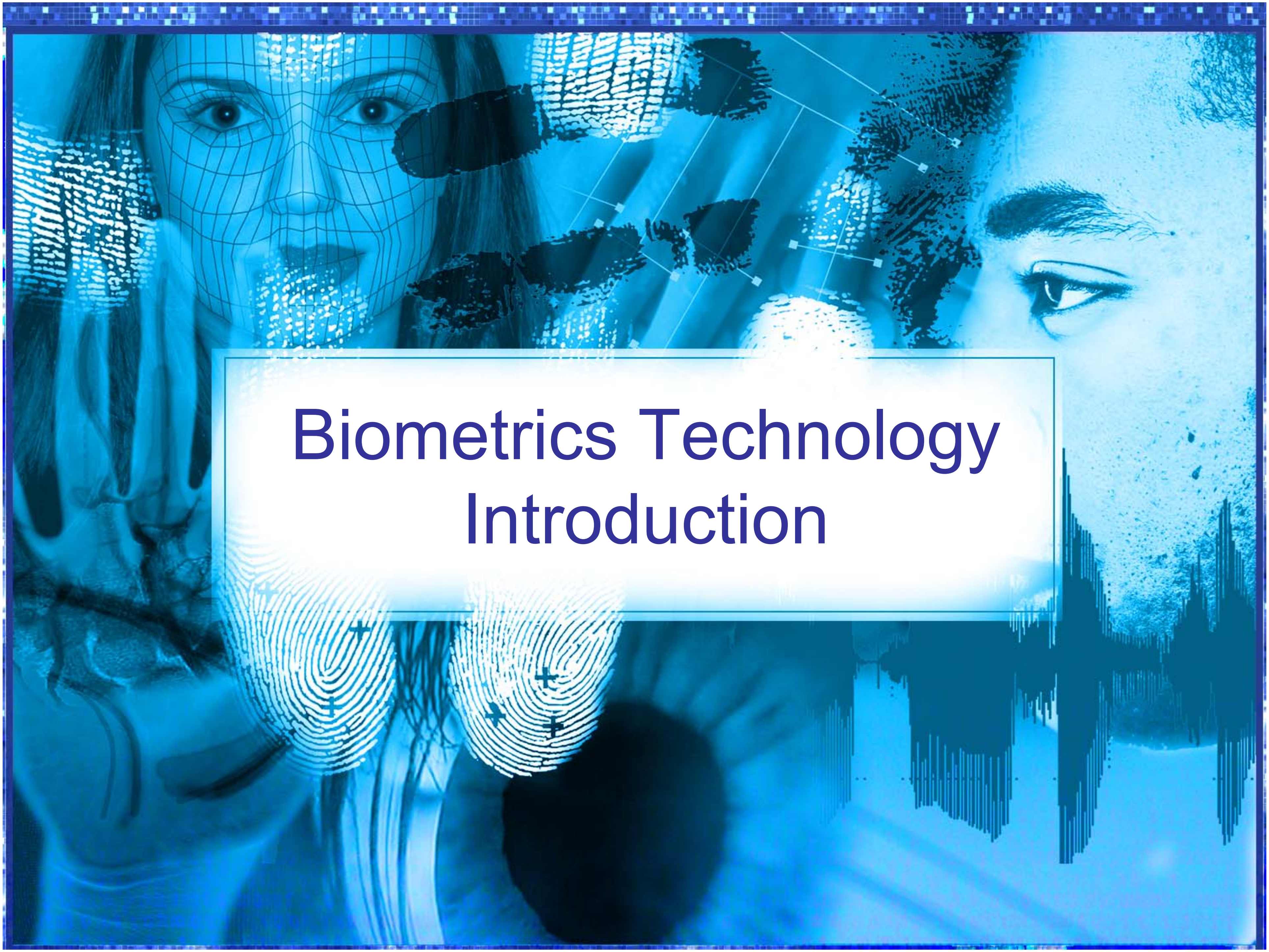


Biometrics Technology Introduction

Biometrics

General term used alternatively to describe a characteristic or a process

As a Characteristic it is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition

As a Process it encompasses automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics

Recognition

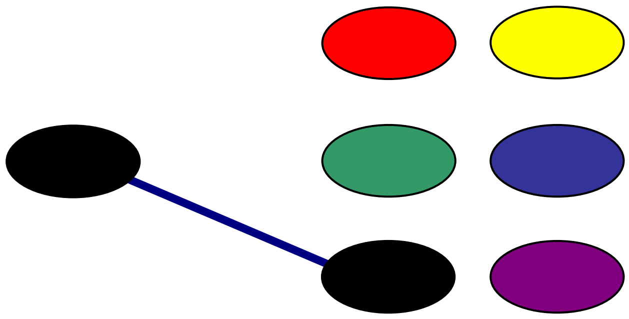
- Used in the description of biometric systems (e.g. face recognition or iris recognition) relating to their fundamental function
- Generic term; does not necessarily imply verification closed-set identification or open-set identification (watchlist)

Verification

- Task where the biometric system attempts to confirm an individual’s claimed identity by comparing a submitted sample to one or more previously enrolled templates

Identification

- Task where the biometric system searches a database for a reference matching a submitted biometric sample
- A biometric is collected and compared to all the templates in a database
- Closed-set identification: the person is known to exist in the database
- Open-set identification: the person is not guaranteed to exist in the database. System determines if the person is in the database



1: Many Identification

Biometric Term

Biometric Predecessors

- Handprints may “have…acted as a nonforgeable signature” of its originator at least 31,000 years old
- Evidence suggests fingerprints were used as a person’s mark as early as 500 B.C.
- Early Chinese merchants used fingerprints to settle business transactions
- Chinese used fingerprints and footprints to differentiate children
- Early Egyptian uses:
  - Traders were identified by their physical descriptors
  - Differentiate between trusted traders of known reputation and previous successful transactions, and those new to the market

Timeline

1858	First systematic capture of hand images for identification purposes is recorded
1870	Bertillon develops anthropometrics to identify individuals
1892	Galton develops a classification system for fingerprints
1896	Henry develops a fingerprint classification system
1936	Concept of using the iris pattern for identification is proposed
1960s	Face recognition becomes semi-automated
1960	First model of acoustic speech production is created
1965	Automated signature recognition research begins
1969	FBI pushes to make fingerprint recognition an automated process
1974	First commercial hand geometry systems become available
1986	Exchange of fingerprint minutiae data standard is published
1988	First semi-automated facial recognition system is deployed
1992	Biometric Consortium is established within US Government
1997	First commercial, generic biometric interoperability standard is published
1999	FBI's IAFIS major components become operational
2002	M1 Technical Committee on Biometrics is formed
2003	Formal US Government coordination of biometric activities begins
2004	US-VISIT program becomes operational
2004	DOD implements ABIS
2005	US patent on iris recognition concept expires

Standards

- Help users deploy and maintain their systems in an easier manner
- Promote longevity
- Enable interoperability
- National and international efforts developing standards for:
  - Technical interfaces
  - Data interchange formats
  - Testing and reporting
  - Societal issues

True Biometric System

Use automated comparisons of electronic data to calculate a match

- Template data to conduct the match:
  - Smaller amount of data extracted from the detailed sample
  - Differential between the template and the sample is conceptually similar to the potential gap between probable match and actual identicalness

Education and contingencies:

- Create organizational awareness
- Prepare for unforeseen situations

Privacy protection:

- Participant awareness
- Organizational sophistication
- Decision-making process

The technology itself may have certain limits; the integration of awareness should not

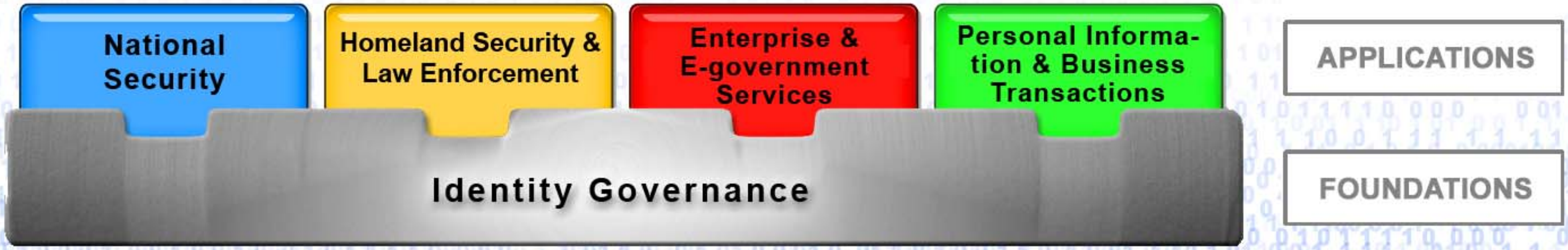
How Biometrics are Used

National Security - automated methods capable of rapidly determining an individual’s true identity, previously used identities and past activities

Homeland Security & Law Enforcement - technologies to secure the U.S. while facilitating legitimate trade and movement of people and to identify criminals in the civilian law enforcement environment

Enterprise & E-government Services - Administration of people, processes and technologies

Personal Information & Business Transactions - business plans that meet customer demands for service at any time, from any location and through multiple communication devices



National Security

Homeland Security & Law Enforcement

Enterprise & E-government Services

Personal Information & Business Transactions

Identity Governance

APPLICATIONS

FOUNDATIONS

Levels of Authentication

Something you have:

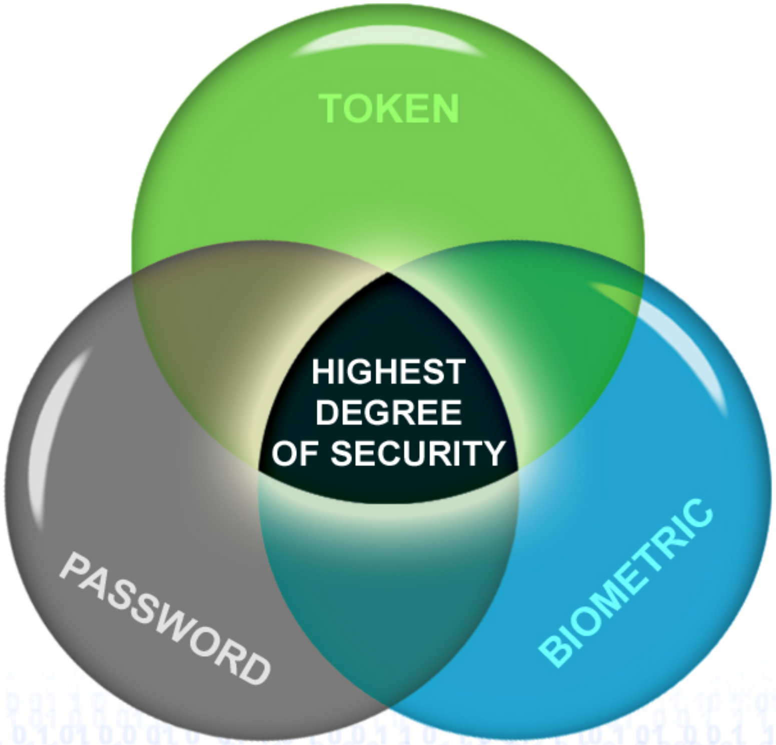
- Token
  - **Key**
  - **Card or badge**

Something you know:

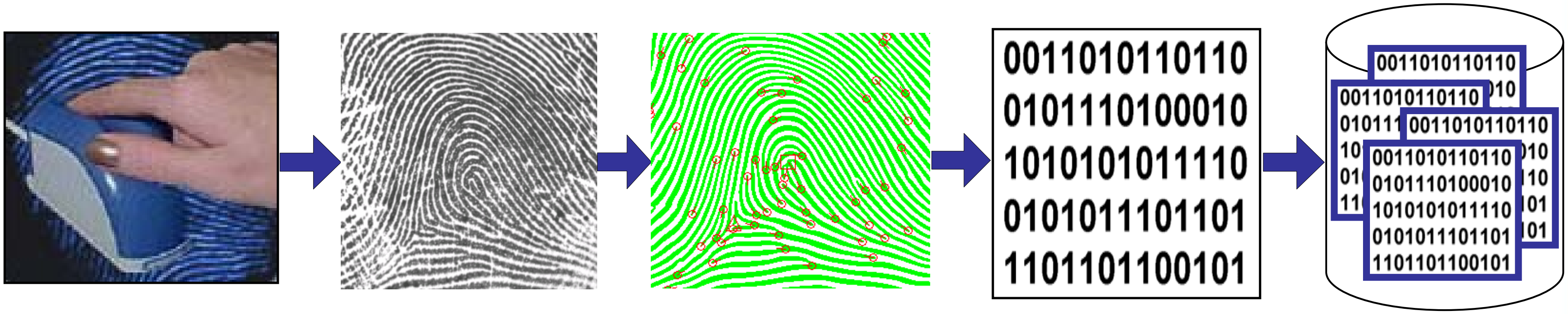
- Password
- PIN
- A memory “unique” to you

Something you are:

- Biometric
  - **Physiological**
  - **Behavioral**



How Biometrics Work



Biometric Presentation

Capture & Preprocessing

Feature Extraction

Template Creation

Storage

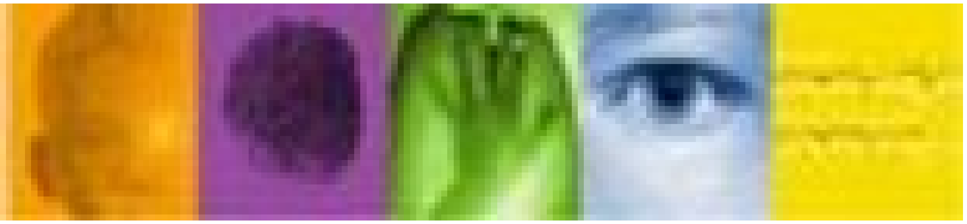
Enrollment Process

Biometric Implementation Factors

- Location
- Security Risks
- Task (identification or verification)
- Expected number of users
- User circumstances
- Existing data

The effectiveness of an implementation is dependent on how and where the technology is used

Biometric Modalities



Common Biometric Modalities:

- Fingerprint
- Face
- Iris
- Voice
- Signature
- Hand geometry

Other modalities:

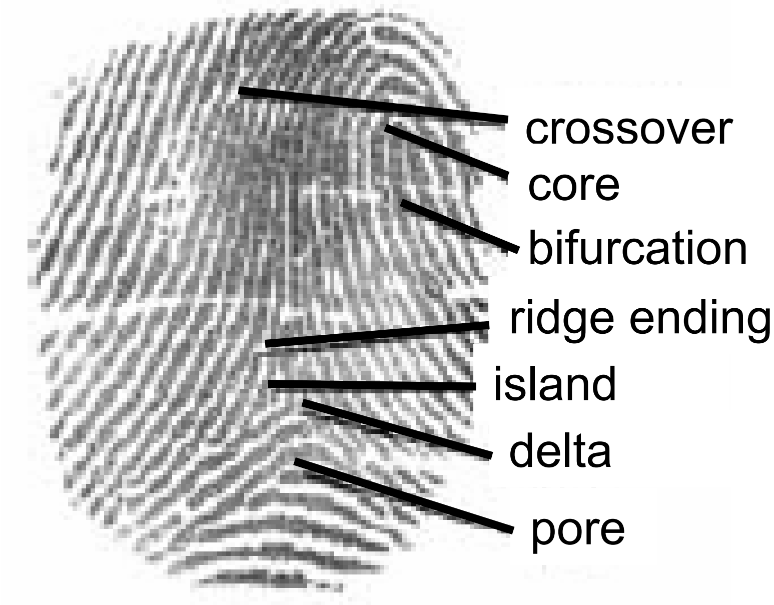
- Gait
- Vascular
- Retina
- Facial Thermography

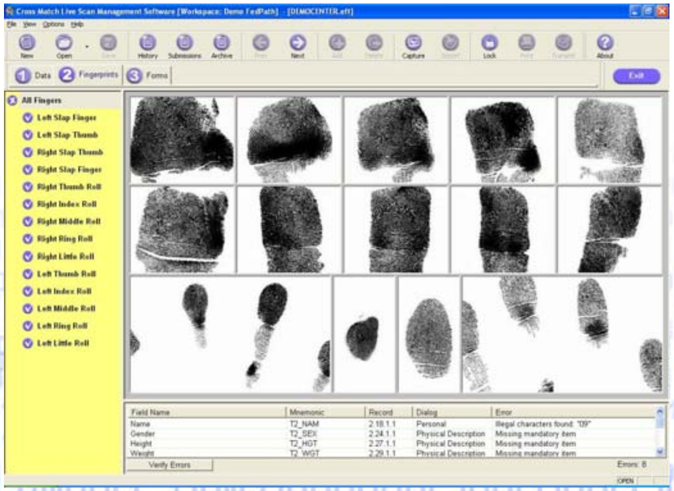
Biometric System Components

- **Sensor** - collects data and converts the information to a digital format
- **Signal processing algorithms** - perform quality control activities and develop the biometric template
- **Data storage** - keeps information that new biometric templates will be compared to
- **Matching algorithm** - compares the new biometric template to one or more templates in data storage
- **Decision process** - uses the results from the matching component to make a system-level decision (either automated or human-assisted)

Fingerprint Recognition

- Manual fingerprint recognition studies began in the late 1800s and early 1900s
- Automated biometric identification techniques introduced in the 1980s and 1990s
- Fingerprints have uneven surface of ridges and valleys that form a person’s unique pattern
- Ridge patterns on the finger’s top joint command primary interest




Cross Match Live Scan Management Software [Workspace: Demo FedPath] - [DEMOCENTER.eft]

Field Name	Mnemonic	Record	Dialog	Error
Name	T2_NAM	2.18.1.1	Personal	Illegal characters found: "09"
Gender	T2_SEX	2.24.1.1	Physical Description	Missing mandatory item
Height	T2_HGT	2.27.1.1	Physical Description	Missing mandatory item
Weight	T2_WGT	2.29.1.1	Physical Description	Missing mandatory item

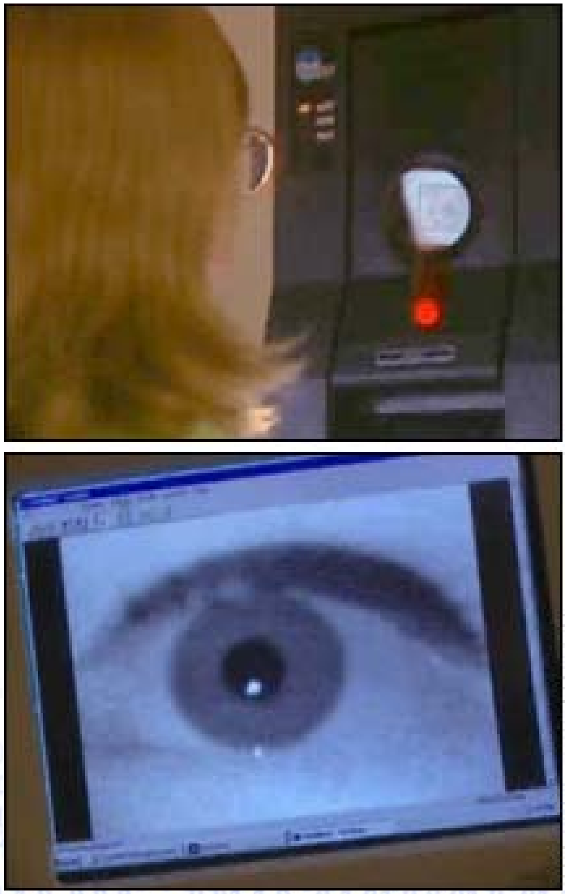
Errors: 8

Face Recognition

- Humans easily recognize familiar faces
- Humans struggle at recognizing unfamiliar individuals
- Machine vision research began in 1960s
  - Use automated methods for recognizing individuals via their facial characteristics
  - No agreed-upon methods for automated face recognition as there are for fingerprints
- Facial image types:
  - Low resolution 2D images
  - High resolution 2D and 3D shows the potential to greatly improve face recognition accuracy

Iris Recognition

- Iris recognition concept dates to 1936
- Major advancements began late 1980s
- First algorithm patent issued 1994 for iris recognition automatically
- Iris image process:
  - Illuminate iris with near-infrared light
  - Takes illuminated picture of the iris without causing any discomfort to the individual



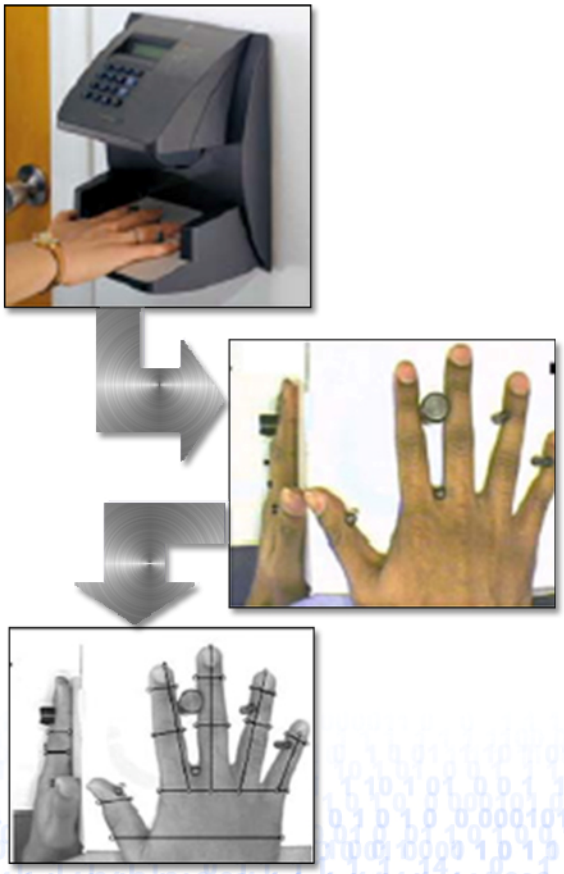
(COURTESY IRISCAN)

Hand/Finger Geometry

One of the first successful commercial biometric products

Verification Process:

- User enters a PIN to claim an identity
- Places hand on the system, which takes a picture of the hand
- Using mirrors, picture shows top and side hand views
- Measures digits of the hand and compares to those collected at enrollment



Other Recognition Methods

- Speaker recognition…Influenced by physical structure of vocal tract and behavioral characteristics
- Dynamic Signature…Measures the speed and pressure when signing name (not what the signature looks like)
- Keystroke dynamics…Measures the typing patterns
- Retina recognition…Images back of the eye and compares blood vessels with existing data
- Gait/Body recognition…Measures how someone appears when walking
- Facial Thermography…Measures how heat dissipates off the face

Individual Privacy Claims

Privacy Torts…Civil injuries for which individuals may be compensated

In 1960, William Prosser surveyed roughly 300 legal cases and consolidated the various claims filed by individuals into four separate causes of action:

1. Intrusion upon the individual’s private affairs
2. Public disclosure of embarrassing private facts about the individual
3. Publicity (wide-scale publication) that places the individual in a “false light” in the public view
4. Appropriation of the individual’s name or likeness.

Where there is biometric information there is personal information. Conduct a privacy assessment to analyze effect.

Privacy Assessment

Decisional: Individual's authority to make decisions that affect the individual's life and body and that of the individual's family members such as end of life issues

Spatial: Relates to physical spaces like the home, the bedroom, etc. Focuses on who may enter or observe the objects and/or the activities that occur in the particular place.

Intentional: Intimate activities or characteristics that are publicly visible. Focuses on the individual's authority to bar further communication of the observable event or feature; e.g., claims against repeating conversations that occurred in public but were directed to specific individuals and publishing photographs of unintended nudity, etc.

Informational: Use of information that relates to an individual. Focuses on the individual's authority to control how that information is used (by whom and for what purpose) and the responsibility of other individuals and organizations to include the individual in decision-making processes that drive subsequent use.

Privacy assessment should identify each aspect, individually and holistically

Why Biometrics?

- Most definitive, real-time tool available today
- Can be combined with other tools to form more secure, easier to use verification solutions
- Recognizes individuals definitively
- Based on physiological and behavioral characteristics

Biometric technologies offer enhanced security and convenience over traditionally used identity governance tools

Content Development

These Slides were originally developed by the NSTC Subcommittee on Biometrics and modeled after information in the documents from their Introduction to Biometrics page at www.biometrics.gov.

The Subcommittee requests that those using these slides reference the original text documents to ensure viewers have access to technically correct information.

Reference