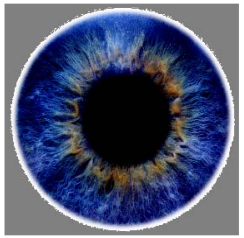
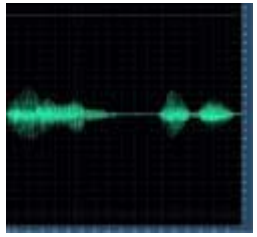
Biometrics
Technology and Standards
Overview

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

Biometric Terms

Verification occurs when the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates

Identification the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database.

- Identification is "closed-set" if the person is known to exist in the database
- In "open-set" identification, the person is not guaranteed to exist in the database. The system must determine if the person is in the database

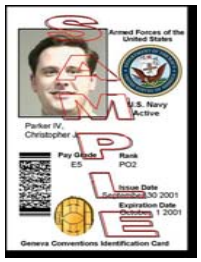
Recognition is a generic term and does not necessarily imply either verification or identification. All biometric systems perform "recognition"

A "watchlist" task is an example of "open-set" identification

Levels of Authentication

Something you have:

- Token
  - Key
  - Card or badge



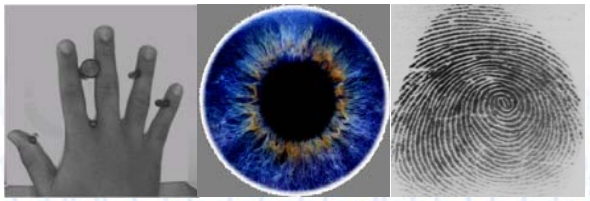
Something you know:

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

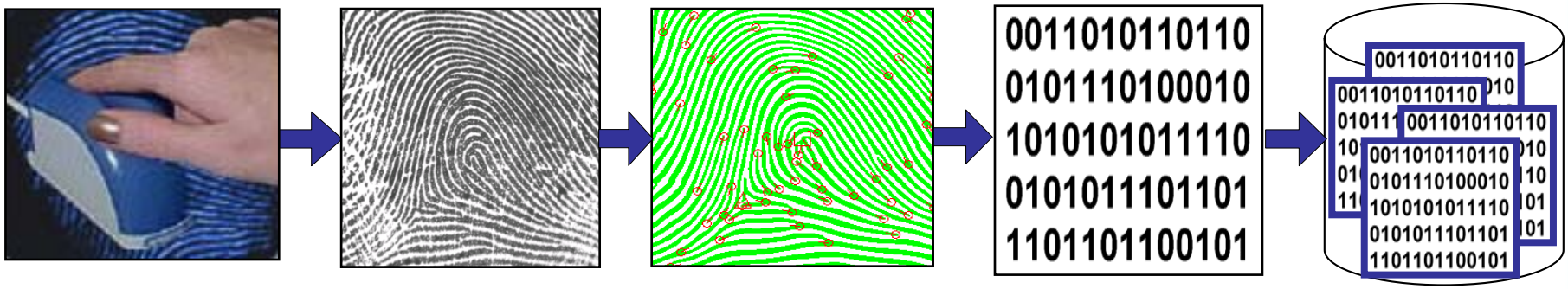
SUPERBOWL45!#
30761

Something you are:

- Biometric



How Biometrics Work



Biometric Presentation

Capture & Preprocessing

Feature Extraction

Template Creation

Storage

Enrollment Process

Paradigm Shift

The Case for Biometrics

- More Secure
- Definitive Recognition
- Less Vulnerable
- Freezing / fixing identity: $x = x$

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

Biometric Modalities

- Dynamic Signature
- Facial Recognition
- Fingerprint
- Hand Geometry
- Iris
- Palm Print
- Speaker Recognition
- Vascular

Dynamic Signature Recognition

* This graphic is for flow & doesn't represent a biometric activity

Dynamic Signature History

1965…first signature recognition system developed

1970s…research continues on the use of static or geometric characteristics (what the signature looks like) rather than dynamic characteristics (how the signature was made)

1970s…interest surges in dynamic characteristics with the availability of better acquisition systems accomplished through the use of touch sensitive technologies

1977…patent was awarded for a “personal identification apparatus” that was able to acquire dynamic pressure information

Dynamic Signature Technology

- Uses the anatomic and behavioral characteristics that an individual exhibits when signing his or her name (or other phrase)
- It is not a graphic image of the signature (common in locations where merchants are capturing signatures for transaction authorizations)
- Dynamically captured data:
  - Direction
  - Stroke
  - Pressure
  - Shape
- Individual's signature can enable handwriting to be a reliable indicator of an individual's identity

Dynamic Signature Characteristics

- Velocity
- Acceleration
- Timing
- Pressure
- Direction
- All analyzed in the X, Y, and Z directions:
  - **X and Y positions are used to show the changes in velocity in the respective directions (indicated by the white and yellow lines)**
  - **Z direction (red line) is used to indicate changes in pressure with respect to time**

Face Recognition

* This graphic is for flow & doesn't represent a biometric activity

Face Recognition History

1960s…the first semi-automated system developed:

Administrator located features (such as eyes, ears, nose, and mouth) on the photographs before it calculated distances and ratios to a common reference point

1970s…Goldstein, Harmon, and Lesk used 21 specific subjective markers such as hair color and lip thickness to automate the recognition

1988…Kirby and Sirovich applied principle component analysis

1991…Turk and Pentland discovered use of eigenfaces techniques

1993-1997…FacE REcognition Technology (FERET) Evaluation, sponsored by the Defense Advanced Research Products Agency

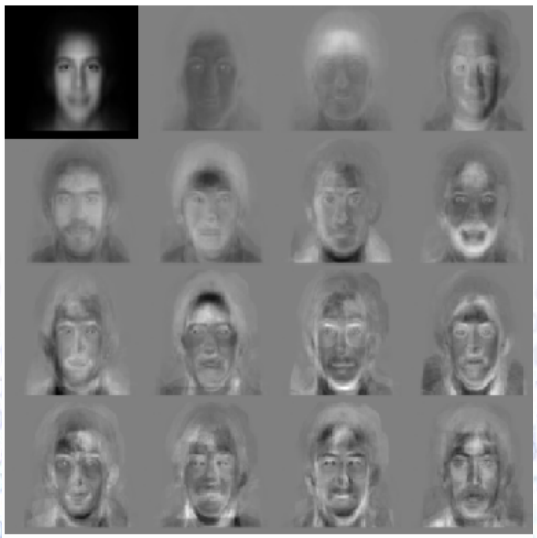
2000, 2002 and 2006…Face Recognition Vendor Tests (FRVT)

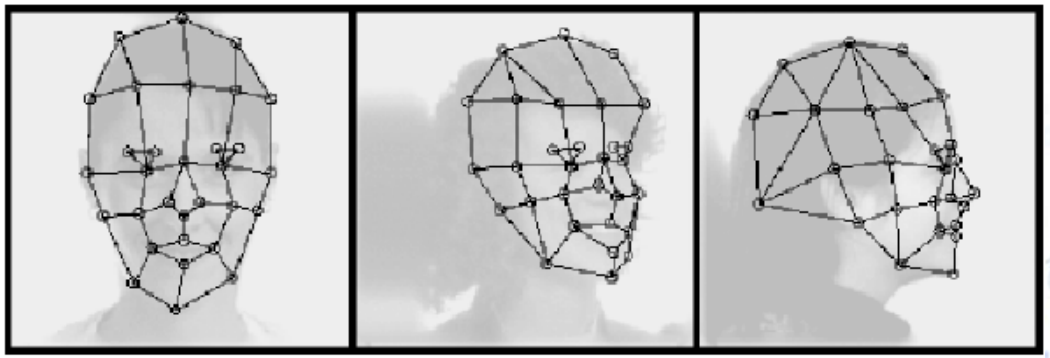
2001…NFL Super Bowl trial captured surveillance images and compared them to a database of digital mugshots

2006…***Face Recognition Grand Challenge***

Face Recognition Approaches

- **Geometric** (feature based)
- **Photometric** (view based)
- **Algorithms:**
  - Principal Components Analysis (PCA)
  - Linear Discriminant Analysis (LDA)
  - Elastic Bunch Graph Matching (EBGM)





Principal Components Analysis (PCA)

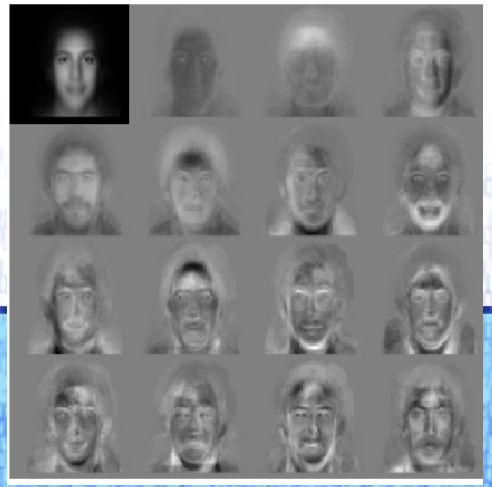
Eigenfaces (orthogonal [uncorrelated] components)

Pioneered by Kirby and Sirivich in 1988

Technique:

- Probe and gallery images are same size and normalized to line up subject's eyes and mouth in images
- PCA reduces dimension of data by compression basics and reveals the most effective low dimensional structure of facial patterns
- Dimension reduction removes useless information and precisely decomposes face structure into eigenfaces
- Each face image may be represented as a weighted sum (feature vector) of the eigenfaces, stored in a 1D array
- A probe image is compared against a gallery image by measuring the distance between their respective feature vectors

Technique reduces data needed to identify individual to 1/1000th of the data presented



PCA approach typically requires the full frontal face to be presented each time; otherwise the image results in poor performance

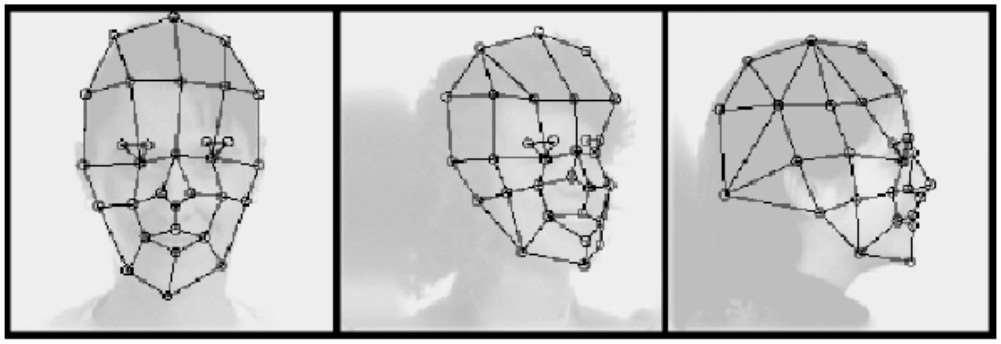
Linear Discriminant Analysis

- Statistical approach for classifying samples of unknown classes based on training samples with known classes
- Aims to maximize between-class (i.e., across users) variance and minimize within-class (i.e., within user) variance.

Elastic Bunch Graph Matching

Real face images have many nonlinear characteristics:

- Variations in illumination (outdoor lighting vs. indoor fluorescents)
- Pose (standing straight vs. leaning over)
- Expression (smile vs. frown)



Technique:

- Gabor wavelet transform creates a dynamic link architecture that projects the face onto an elastic grid.
- Gabor jet is a node on the elastic grid, notated by circles on the image, which describes the image behavior around a given pixel. It is the result of a convolution of the image with a Gabor filter, which is used to detect shapes and to extract features using image processing
- Recognition is based on the similarity of the Gabor filter response at each Gabor node
- This biologically-based method using Gabor filters is a process executed in the visual cortex of higher mammals
- This method requires accurate landmark localization, which can sometimes be achieved by combining PCA and LDA methods

Fingerprint Technology

* This graphic is for flow & doesn't represent a biometric activity

Fingerprint History

Late 19th century… Sir Francis Galton defined points/characteristics to identify fingerprints.

1960s… Fingerprint identification began transition to automation

1969… Federal Bureau of Investigation (FBI) pushed to automate fingerprint identification process

1975… FBI funded development of fingerprint scanners for automated classifiers and minutiae extraction technology

1970-1980s… NIST led developments in automatic methods of digitizing inked fingerprints and the effects of image compression on image quality, classification, extraction of minutiae, and matching.

1980s… M40 algorithm, FBI's first operational matching algorithm

1981… five Automated Fingerprint Identification Systems (AFIS) deployed

1994… Integrated Automated Fingerprint Identification System (IAFIS):

1999… Lockheed Martin selected to build the AFIS segment of the FBI's IAFIS project and the major IAFIS components were operational by 1999

2003… Fingerprint Vendor Technology Evaluation (FpVTE) initiated to evaluate the accuracy of fingerprint recognition systems.

Fingerprint Technology

Appears as a series of dark lines and white space:

- Dark lines represent the high, peaking portion of friction ridge skin
- White space is the valleys between these ridges and is the low, shallow portion of the friction ridge skin
- Based on the minutiae, or the location and direction of the ridge endings and bifurcations (splits) along a ridge path.

Information collected from a fingerprint's friction ridge impression:

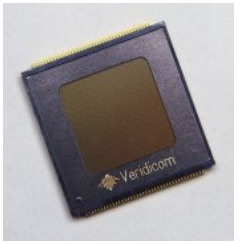
- Flow of the friction ridges (Level 1 Detail)
- Presence or absence of features along the individual friction ridge paths and their sequence (Level 2 Detail)
- Intricate detail of a single ridge (Level 3 Detail)
- Recognition is usually based on Levels 1 and 2 of detail or just on Level 3

AFIS technology exploits some of these fingerprint features:

- Interprets flow of the overall ridges to assign a fingerprint classification
- Extracts minutiae detail – a subset of the total amount of information available yet enough information to effectively search a large repository of fingerprints

Fingerprint Hardware

- Optical sensors take an image of the fingerprint, and are the most common sensor today
- Capacitive sensors determine each pixel value based on the capacitance measured, made possible because an area of air (valley) has significantly less capacitance than an area of finger (friction ridge skin)
- Ultrasound employs high frequency sound waves
- Thermal requires a swipe of a finger across a surface to measure the difference in temperature over time to create a digital image



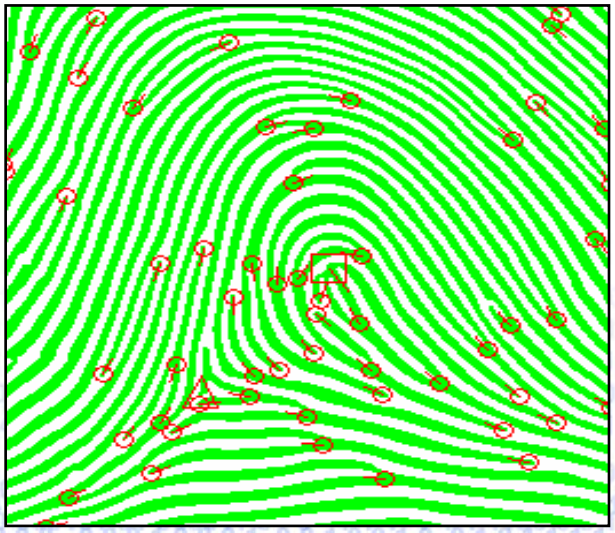
Fingerprint Software

Minutiae-based matching:

- Relies on locations and direction of minutiae points
- Most widely used matching technique

Pattern matching:

- Compares two images to judge their similarity
- Used to detect duplicates



Hand Geometry

* This graphic is for flow & doesn't represent a biometric activity

Hand Geometry History

1980s…Hand geometry introduced

1985…David Sidlauskas developed and patented the hand geometry

1986…First commercial hand geometry recognition systems

1991…Performance evaluation of biometric identification devices evaluated the relative performance of multiple biometric devices, including hand geometry

1996…Olympic Games implemented hand geometry systems to control and protect physical access to the Olympic Village

1996…Evaluation of the INSPASS Hand Geometry Data determined the effect of a threshold on system operation, established false accept and false reject rates as a function of the threshold, and presented an estimate of the Receiver Operating Characteristics (ROC) curve for the INSPASS system

1990s-present…Companies implement hand geometry systems in parallel with time clocks for time and attendance purposes.

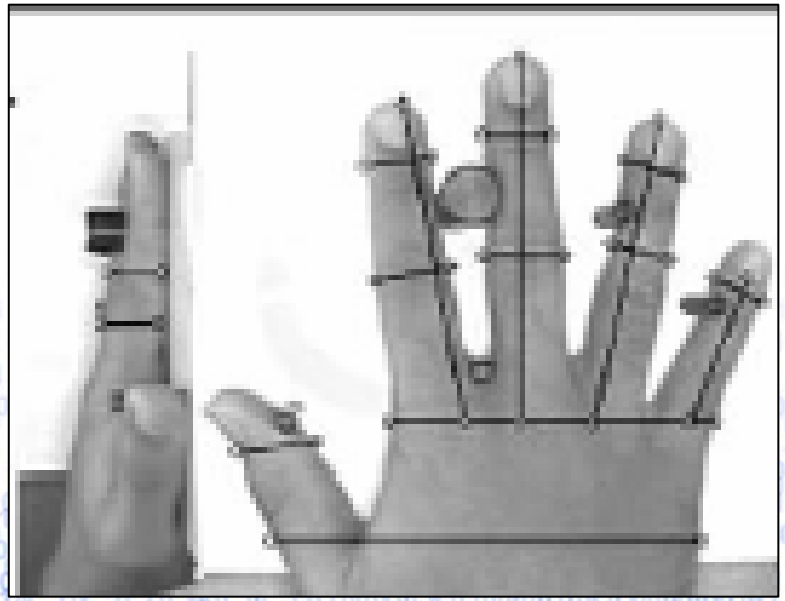
2004…Walt Disney World began using "finger" geometry to expedite and facilitate entrance to the park and to identify guests as season ticket holders to prevent ticket fraud

Hand Geometry Technology

Use measurement and recording length, width, thickness, and surface area of an individual's hand while guided on a plate

Use camera to capture hand silhouette

- Hand placed on the plate, palm down, and guided by five pegs that sense when the hand is in place
- Data capture by a Charge-Coupled Device (CCD) camera of the top view of the hand, top surface of the hand and a side image (using an angled mirror)
- 31,000 points are analyzed and 90 measurements are taken
- Information is stored in nine bytes of data



Hand Geometry Technology

Enrollment process:

- Requires the capture of three sequential images of the hand
- Creates a template of the user's characteristics

Submission process:

- System recalls the template associated with that identity
- Claimant places his/her hand on the plate
- System captures an image and creates a verification template to compare to the template developed upon enrollment
- Similarity score is produced
- Claimant accepted or rejected based on system threshold

Iris Recognition

* This graphic is for flow & doesn't represent a biometric activity

Iris Recognition History

1936…Ophthalmologist Frank Burch proposed using iris patterns as a method to recognize an individual

1985…Drs. Leonard Flom and Aran Safir, ophthalmologists, proposed the concept that no two irides are alike

1987…Drs. Leonard Flom and Aran Safir awarded a patent for the iris identification concept

1993…Defense Nuclear Agency began work to test and deliver a prototype unit

1994…Dr. Daugman awarded a patent for his automated iris recognition algorithms

1995…Prototype completed due to the combined efforts of Drs. Flom, Safir, and Daugman

1995…First commercial products

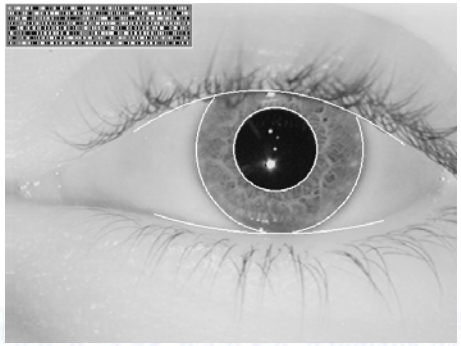
2005…Patent covering the basic concept of iris recognition expired, providing marketing opportunities for other companies that have developed their own algorithms for iris recognition

2011…Expiration of patent on the IrisCodes® implementation of iris recognition developed by Dr. Daugman

Iris Recognition Technology

Iris imaging requires use of a high-quality digital camera:

- Commercial iris cameras use infrared light to illuminate the iris without causing harm or discomfort to the subject
- 2D Gabor wavelet filters and maps the segments of the iris into phasors (vectors)
- Phasors include information on the orientation and spatial frequency (“what” of the image) and the position of these areas (“where”)
- This information is used to map the IrisCodes®



Iris is located using landmark features

Iris Recognition Technology

Phase is not affected by contrast, camera gain, or illumination levels:

- Uses 256 bytes of data using a polar coordinate system
- Control bytes exclude eyelashes, reflection(s), and other unwanted data

Recognition performed comparing two IrisCodes®

- Amount of difference between two IrisCodes® — Hamming Distance (HD) — is used as a test of statistical independence between the two IrisCodes®. If the HD indicates that less than one-third of the bytes in the IrisCodes® are different, the IrisCode® fails the test of statistical significance, indicating that the IrisCodes® are from the same iris.

Therefore, the key concept to iris recognition is failure of the test of statistical independence.

Palm Print

* This graphic is for flow & doesn't represent a biometric activity

Palm Print History

1858…Sir William Herschel, working for the Civil Service of India, recorded a handprint on the back of a contract for each worker to distinguish employees from others who might claim to be employees when payday arrived

1994…First known AFIS system to support palm prints is believed to have been built by a Hungarian company.

Late 1997…US company bought Hungarian palm system

2000s…Australia houses the largest repository of palm prints in the world. The new Australian National Automated Fingerprint Identification System (NAFIS) includes 4.8 million palm prints

April 2002…a Staff Paper on palm print technology and IAFIS palm print capabilities was submitted to the Identification Services (IS) Subcommittee, CJIS Advisory Policy Board (APB)

2004…Connecticut, Rhode Island and California established statewide palm print databases that allowed law enforcement agencies in each state to submit unidentified latent palm prints to be searched against each other's database of known offenders

Palm Print Technology

Palm print:

- Series of dark lines represents the high, peaking portion of the friction ridged skin
- White space represents the valley between these ridges
- Interprets the flow of the overall ridges to assign a classification and then extract the minutiae detail — a subset of the total amount of information available, yet enough information to effectively search a large repository of palm prints

Sensor types:

- Capacitive determines each pixel value based on the capacitance measured
- Optical uses prisms to detect the change in light reflectance related to the palm
- Ultrasound employs high frequency sound
- Thermal requires a swipe of a palm across a surface to measure the difference in temperature

Palm Print Technology

Software: scan the entire palm or segment it into smaller areas

- Palm systems partition their repositories based upon the location of a friction ridge area
- Searching only this region of a palm repository rather than the entire database maximizes the reliability of a latent palm search

Palm matching techniques

- Minutiae-based matching relies on the minutiae points described above, specifically the location, direction, and orientation of each point
- Correlation-based matching involves simply lining up the palm images and subtracting them to determine if the ridges in the two palm images correspond
- Ridge-based matching uses ridge pattern landmark features such as sweat pores, spatial attributes, and geometric characteristics of the ridges, and/or local texture analysis, all of which are alternates to minutiae characteristic extraction matching

Speaker Verification

* This graphic is for flow & doesn't represent a biometric activity

Speaker Verification History

1960…Gunnar Fant, a Swedish professor, published a model describing the physiological components of acoustic speech production, based on the analysis of x-rays of individuals making specified phonic sounds

1970…Dr. Joseph Perkell used motion x-rays and included the tongue and jaw to expand upon the Fant model

1976…Texas Instruments built a prototype system that was tested by the U.S. Air Force and The MITRE Corporation

Mid-1980s…the National Institute of Standards and Technology (NIST) developed the NIST Speech Group to study and promote the use of speech processing techniques

1996...National Security Agency funded and the NIST Speech Group has hosted yearly evaluations, the NIST Speaker Recognition Evaluation Workshop, to foster the continued advancement of the speaker recognition community

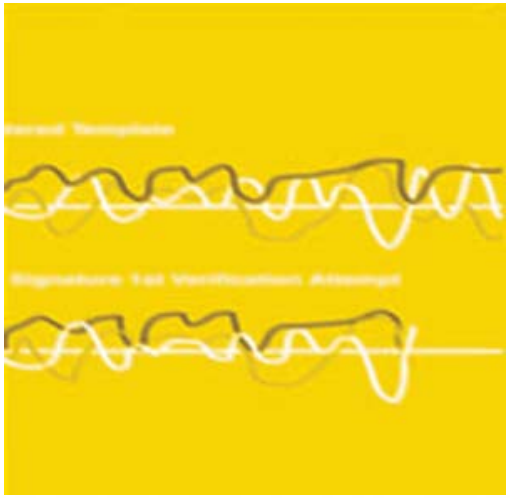
Speaker Verification Technology

Physiological component of voice recognition related to physical shape of an individual's vocal tract

Motion of the mouth and pronunciations are the behavioral components of this biometric

There are two forms of speaker recognition:

- **Text dependent** *(constrained mode):*
  - Individual presents either a fixed (password) or is prompted for a phrase *("Please say the numbers '33-54-63'")* that is programmed into the system and can improve performance especially with cooperative users
- **Text independent** *(unconstrained mode):*
  - No advance knowledge of the presenter's phrasing and is much more flexible in situations where the individual submitting the sample may be unaware of the collection or unwilling to cooperate, which presents a more difficult challenge



Speaker Verification Technology

Text dependent:

- Capture word or phrase by microphone
- Convert voice sample from analog to digital to extract voice features, and create a model
- Use Hidden Markov Models (HMMs), random based models that provide a statistical representation of the sounds produced by the individual

Text independent:

- Uses Gaussian Mixture Model, a state-mapping model closely related to HMM
- Uses the voice to create vector “states” representing sound forms characteristic of the person’s physiology and behavior

Enrollment

Speaker Verification Technology

- Same quality/duration/loudness/pitch features are extracted from the submitted sample and compared to the model of the claimed or hypothesized identity and to models from other speakers
- Other-speaker models contain the “states” of a variety of individuals, not including that of the claimed or hypothesized identity
- Input voice sample and enrolled models are compared to produce a likelihood ratio
- If the voice input belongs to the identity claimed or hypothesized, the score will reflect the sample to be more similar to the claimed identity’s model than to the “anti-speaker” model

Recognition

Vascular Pattern

* This graphic is for flow & doesn't represent a biometric activity

Vascular Pattern History

1992…Dr. K. Shimizu published paper on optical trans-body imaging and potential optical CT scanning applications

1996…K. Yamamoto, in conjunction with K. Shimizu, presented another paper in which the two discussed research they had undertaken since the earlier paper

2000…First research paper about the use of vascular patterns for biometric recognition published

2000…First commercially available device using subcutaneous blood vessel pattern in the back of the hands

Vascular Pattern Technology

Vascular hand pattern collection:

- Near-infrared rays from a bank of light emitting diodes (LEDs) penetrate the skin of the back or palm of the hand
- Reflected near-infrared rays produce an image on the sensor caused by absorbance of blood vessels and other tissues
- Image is digitized and image processing techniques produce extracted vascular pattern
- Various feature make up template:
  - Vessel branching points
  - Thickness
  - Branching angles

Vascular Pattern Technology

Vascular finger pattern collection:

- Near-infrared rays generated from a bank of LEDs penetrate the finger or hand and are absorbed by the hemoglobin in the blood
- Areas in which the rays are absorbed (i.e., veins) appear as dark areas similar to a shadow in an image taken by a charge-coupled device (CCD) camera
- Image processing can then construct a vein pattern from the captured image
- Pattern is digitized and compressed so that it can be registered as a template

Biometric Standards

- What are biometric standards?
- Why are biometric standards important?
- What types of biometric standards are there?
- Who develops standards?
- How are standards developed?
- What is conformity assessment?
- Is the use of biometric standards mandatory or optional?
- Where do I find more information about a specific standard?

Biometric Standards

- Enable development of integrated, scalable, and robust solutions
- Reduce the cost of development and maintenance of system solutions
- National and International efforts:
  - Creating a standard set of biometric data interchange definitions
  - Developing standards to promote interoperability between various systems
  - Testing biometrics and for testing conformance to biometric standards

Standards should be technology neutral and not favor any particular vendor or modality

Biometric Standards

- Formats for the interchange of biometric data
- Common file formats that provide platform independence and separation of transfer syntax content definition
- Application program interfaces and application profiles
- Performance metric definitions and calculations
- Approaches to test performance
- Requirements for reporting the results of performance tests

Specifications

Standards' Importance

- Enable development of integrated, scalable, and robust solutions
- Reduce the cost of development and maintenance of system solutions
- Guide national and international efforts to:
  - Create a standard set of biometric data interchange definitions
  - Promote interoperability between various systems
  - Create standards for testing biometrics and for testing conformance to biometric standards
- Standards should be technology neutral and not favor any particular vendor or modality

Technical Interfaces

Specify interfaces and interactions between biometric components and subsystems:

- Security mechanisms to protect stored data and data transferred between systems
- Architecture and operation of biometric systems in order to identify the standards that are needed to support multi-vendor systems and their applications

Examples include:

- ANSI INCITS 358-2002 BioAPI Specification v1.1
- ANSI INCITS 398-2005 [NISTIR 6529-A] Common Biometric Exchange File Format (CBEFF)

Data Interchange Formats

Specify Content …

Meaning …

Representation of formats for the interchange of biometric data:

- Finger Pattern Based Interchange Format
- Finger Minutiae Format for Data Interchange
- Face Recognition Format for Data Interchange
- Iris Interchange Format
- Finger Image Based Interchange Format
- Signature/Sign Image Based Interchange Format
- Hand Geometry Interchange Format

Examples:

- ANSI INCITS 377-2004 Finger Pattern Based Interchange Format
- ANSI INCITS 378-2004 Finger Minutiae Format for Data Interchange
- ANSI INCITS 379-2004 Iris Image Interchange Format

Application Profile Standards

Specify one or more base standards and standardized profiles

Identifies chosen classes, conforming subsets, options, and parameters of those base standards or standardized profiles necessary to accomplish a particular function

Examples:

- ANSI INCITS 383-2003 Biometrics-Based Verification
- Identification of Transportation Workers
- ANSI INCITS 394-2004 Data Interchange
- Data Integrity of Biometric-Based Personal Identification for Border Management

Performance Testing and Reporting

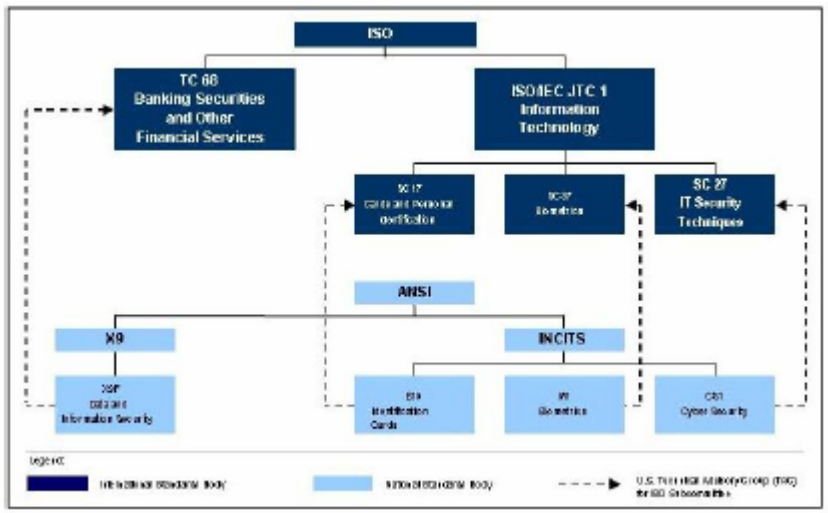
Approaches and requirements for Performance Testing and Reporting specify biometric performance metric definitions and calculations

Examples:

- ANSI INCITS 409.1-2005 Biometric Performance Testing and Reporting Part 1 - Principles Framework
- ANSI INCITS 409.2-2005 Biometric Performance Testing and Reporting Part 2 - Technology Testing Methodology
- ANSI INCITS 409.3-2005 Biometric Performance Testing and Reporting Part 3 - Scenario Testing Methodologies

Agencies & Standard Development Organizations

- InterNational Committee for Information Technology Standards (INCITS) M1
- National Institute of Standards
- Technology Joint Technical Committee 1 (JTC 1)/ Subcommittee 37 (SC 37)
- Organization for the Advancement of Structured Information Standards (OASIS)



M1 Standing Task Groups

M1.2 Biometric Technical Interfaces — develops standards for interfaces and interactions between biometric system components and subsystems, including the possible use of security mechanisms to protect stored data and data transferred between systems

M1.3 Biometric Data Interchange Formats — develops standards for content, meaning, and representation of biometric data interchange formats

M1.4 Biometric Profiles — develops profile standards to ensure the interoperability of biometric information in specific applications (e.g., Biometric Based Verification and Identification of Transportation Workers, Border Management, Point of Sale)

M1.5 Biometric Performance Testing and Reporting — develops standards for biometric performance metric definitions and calculations, and approaches to test performance and requirements for reporting the results of these tests

M1.6 Societal Aspects of Biometric Implementations — develops technical reports that address the study and standardization of technical solutions to cross-jurisdictional and societal aspects of biometric implementations

Other Standard Supporting Organizations

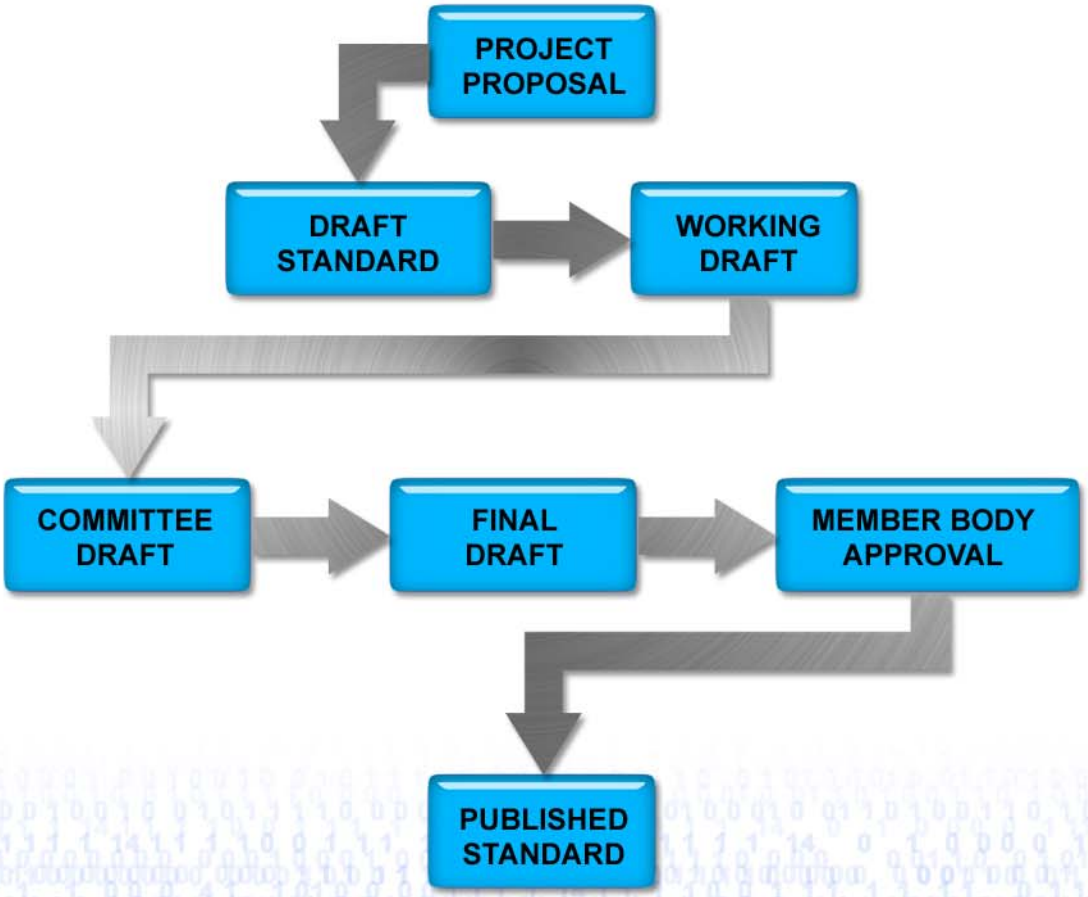
National Institute of Standards and Technology (NIST):

- Under the Information Technology Management Reform A (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by NIST for federal computer systems
- Standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide

JTC 1/SC 37 is responsible for the international projects for generic interchange, interoperability, and testing

OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards

Standards Development Process



Ideal progression depicted. Many times, drafts go forward and backward multiple times through this progression. Successive drafts may be considered until consensus.

Conformity Assessment

- Any activity concerned with determining directly or indirectly that relevant requirements are fulfilled
- Conformity assessment raises the user's assurance that the product will perform in the manner expected with regard to the intent of the written specification
- Conformity assessment provides assurance to users by increasing consumer confidence when personnel, products, systems, processes, or services are evaluated against the requirements of a standard
- Conformance tools makes possible:
  - Establishment of conformity assessment programs to validate conformance, e.g., to ANSI INCITS 358-2002 BioAPI Specification v1.1
  - Support development of products conforming to voluntary consensus biometric standards
- Developers may use these same test tools to ensure standards conformance before products are released

Performance Evaluations

- **Technology**
- **Scenario**
- **Operational**

Technology Evaluations measure biometric system performance, and typically only the recognition algorithm component

Evaluation Types

- Highlights specific areas that require future research and development
- Provides performance data
- Uses results to plan future R&D activities
- Employs results to select systems

FACE RECOGNITION VENDOR TEST 2006

Technology Evaluation

Evaluation Types

- Measures biometric system performance operating in a particular application
- Enables users to determine the best system for their specific application
- Develops good understanding of how it will operate at the proposed location

Scenario Evaluation

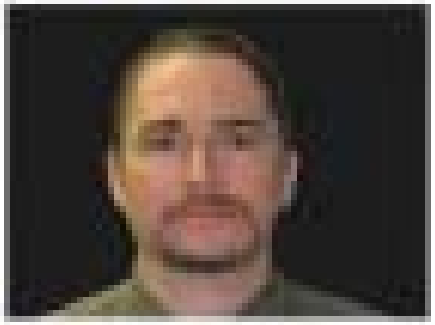
Evaluation Types

- Conducts test at the actual site using actual end users, a subset of the end users, or a representative set of subjects
- Aims to determine the workflow impact caused by the addition of a biometric system
- Enables decision makers to develop a solid business case for potential installations

Operational Evaluation

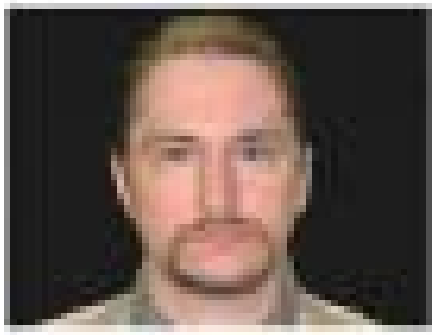
True Accept Rate

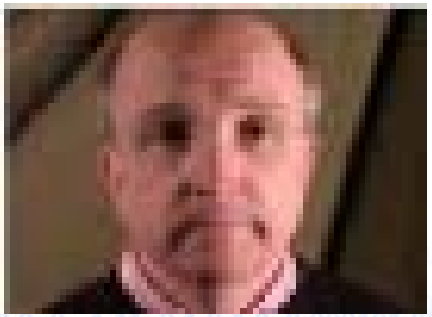
- End user must first make a claim as to his/her identity (e.g., I am John Q. Public)
- Biometric system then determines if the end-user's identity claim is true or false
- The gentleman at bottom makes a claim that he is the gentleman at top. Assume that the system's verification threshold was set at 0.90
  - Since 0.93 is higher than 0.90, the system in this example has correctly determined that the gentleman in the top picture is the same as the gentleman in the bottom picture
  - This is called a true accept or correct verification
- Now assume that the same individual makes the same claim, except the system's verification threshold is 0.95. The demonstration face recognition system will not make a correct decision
- After many trials with this gentleman, as well as other correct matches, we will know the rate legitimate end users are correctly verified by the system. This is called the true accept or correct verification rate



False Accept Rate

- The gentleman on the bottom claims to be the gentleman at top
  - Assume that the system returns a similarity score of 0.86 and verification threshold was set at 0.9
  - Face recognition system determines the gentleman on the bottom is not the gentleman on the top
- Look at the case where the same individual makes the same claim, but the system's verification threshold is set at 0.85
  - The system incorrectly verifies that the gentleman is the gentleman in the system
  - This error is called a false accept
  - Trials run with incorrect claims will determine the rate at which the system incorrectly matches an imposter individual to another individual's existing biometric

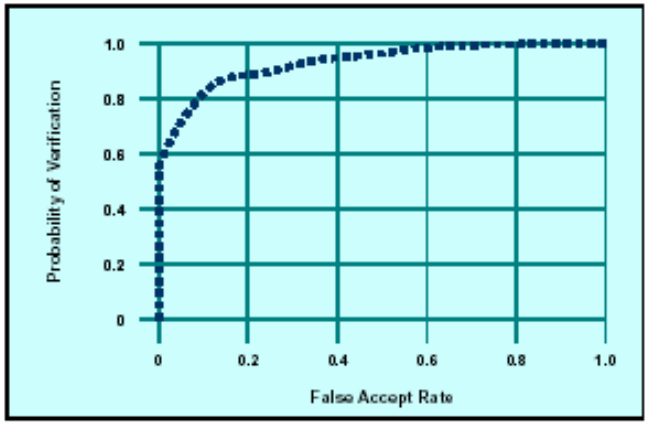




Ideally, biometric systems would always provide a probability of verification of 100% with a false accept rate of 0%

Accept Rate Threshold

- Optimal system threshold for a given application
- Determining threshold can be difficult because the verification rate and false accept rate are not independent variables
- If the threshold in the example face recognition system is raised, the verification rate decreases, but the false accept rate also decreases
- If the threshold in the example system is lowered, the verification rate increases, but the false accept rate also increases
- Plotting verification accept rates against the associated false accept rates, called a Receiver Operating Characteristic (ROC) curve, allows for a visualization of this trade-off relationship
- Varying the system's threshold moves the operating point along its ROC curve



Identification

Open-set identification, the biometric system determines if the individual's biometric template matches a biometric template of someone in the database

Task examples:

- Comparing biometrics of visitors against a terrorist database
- Comparing a biometric of a "John Doe" to a missing person's database

Face recognition system:

- The system first compares the submitted image to each image in the database. Assume that the similarity score for each comparison is 0.6, 0.86, 0.9, and 0.4, respectively. Also assume that the system's watchlist threshold is set at 0.85
- Face recognition system sounds an alarm each time one or more of the similarity scores is higher than the threshold
- Since an alarm sounded, the system user would look more closely at the similarity scores to see which image attained the highest score, which is the system's best guess at the identity of the individual

Open-Set Identification

Identification

Every input image has a corresponding match in the database

Biometric template of an individual is presented to the biometric system

Face recognition system:

- Compares the input image to each image in the database
- Let us assume that the similarity score for each comparison is 0.6, 0.86, 0.9, and 0.4, respectively. In this example, the correct match has the top similarity score.
- If we run the same trial for all subjects in the database, we will know how often the system will return a correct result with the top match, which is termed the identification rate at rank 1

Closed-Set Identification

Failure to Acquire

Rate at which a biometric system fails to capture and/or extract information from an observation

Numerous issues can cause a Failure to Acquire:

- Device/software malfunction
- Environmental concerns
- Human anomalies (e.g., amputees not able to use hand geometry system, bricklayers with worn fingerprints, etc.)

Biometric challenging issues will produce lower performance measures

Others only show performance (usually referred to as False Match Rates and False Non-Match Rates) on properly acquired signatures and show the Failure to Acquire rate separately

Other Performance Statistics

- Crossover Error Rate (CER)
- Detection Error Trade-off (DET)
- Difference Score
- Equal Error Rate (EER)
- Failure to Enroll (FTE)
- False Match Rate
- False Non-Match Rate
- Hamming Distance
- Throughput Rate
- True Accept Rate
- True Reject Rate
- Type I Error
- Type II Error

Other Test Methods

Acceptance Testing: The process of determining whether an implementation satisfies acceptance criteria and enables the user to determine whether or not to accept the implementation

Conformity: Fulfillment by a product, process or service of specified requirements

Conformity Evaluation: Systematic examination of the extent to which a product, process or service fulfills specified requirements

Conformance Testing: (or Conformity Testing): Conformity evaluation by means of testing

Interoperability Testing: The testing of one implementation (product, system) with another to establish that they can work together properly

Performance Testing: Measures the performance characteristics of an Implementation Under Test (IUT) such as its throughput, responsiveness, etc., under various conditions

Robustness Testing: The process of determining how well an implementation processes data which contains errors

Performance Evaluation Report

Not all evaluation results are relevant

- If an evaluation report, particularly for a Scenario or Operational Evaluation, does not match the user's intended application, the usefulness of the results will be significantly diminished

Biometric evaluation results have a very limited shelf life

- if the report is more than 9-18 months old, the results should not be considered conclusive, but merely used as a general guide and reference

Key Factors

Biometric Standards: Yes/No

Standards usage is optional, however…

- Real benefits of standards are realized by organizations that require the application and use of standards
- Some organizations maintain a registry or database of standards that must be applied in acquiring, developing, and maintaining systems
- These organizations will not purchase products or services that do not conform to such required standards

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