Biometrics

Outline

- Biometrics
- What is a Biometric Signature?
- What is an Authentication System?
- How does a Biometric System work?
- Biometric Comparisons
- Types of Biometrics
  - Fingerprint-Scan
  - Iris-Scan

Biometrics

- Biometrics refers to the measurement of specific physical or behavioral characteristics
  - use of that data in identifying subjects
  - offer highly accurate means of comparison of measured characteristics to those in a preassembled database
- Biometric Authentication
  - technologies that measure and analyze human physical and behavioral characteristics for authentication purposes

What is a Biometric Signature?

Biometric (Digitized) Signature deals with the science of identifying or verifying a person based on physiological, behavioral, or genetic characteristics.

- Physiological Biometrics are based on measurements and data derived from direct measurements of a part of a human body:
  - Finger-scan
  - Iris-scan
  - Retina-scan
  - Hand-scan, etc.

What is a Biometric Signature?

- Behavioral Biometrics are based on measurements and data from an action taken by a person; i.e., indirect features of a body:
  - Voice-Print
  - Keystroke-scan
  - Hand-writing/Signature-scan, etc.
- DNA is a biometric as much as others but major differences:
  - Actual sample is needed instead of an impression (invasive procedure!)
  - DNA matching is not done in real-time; i.e., needs controlled lab environment.
  - It does not employ feature extraction and template matching; it represents the comparison of actual samples in the databank.

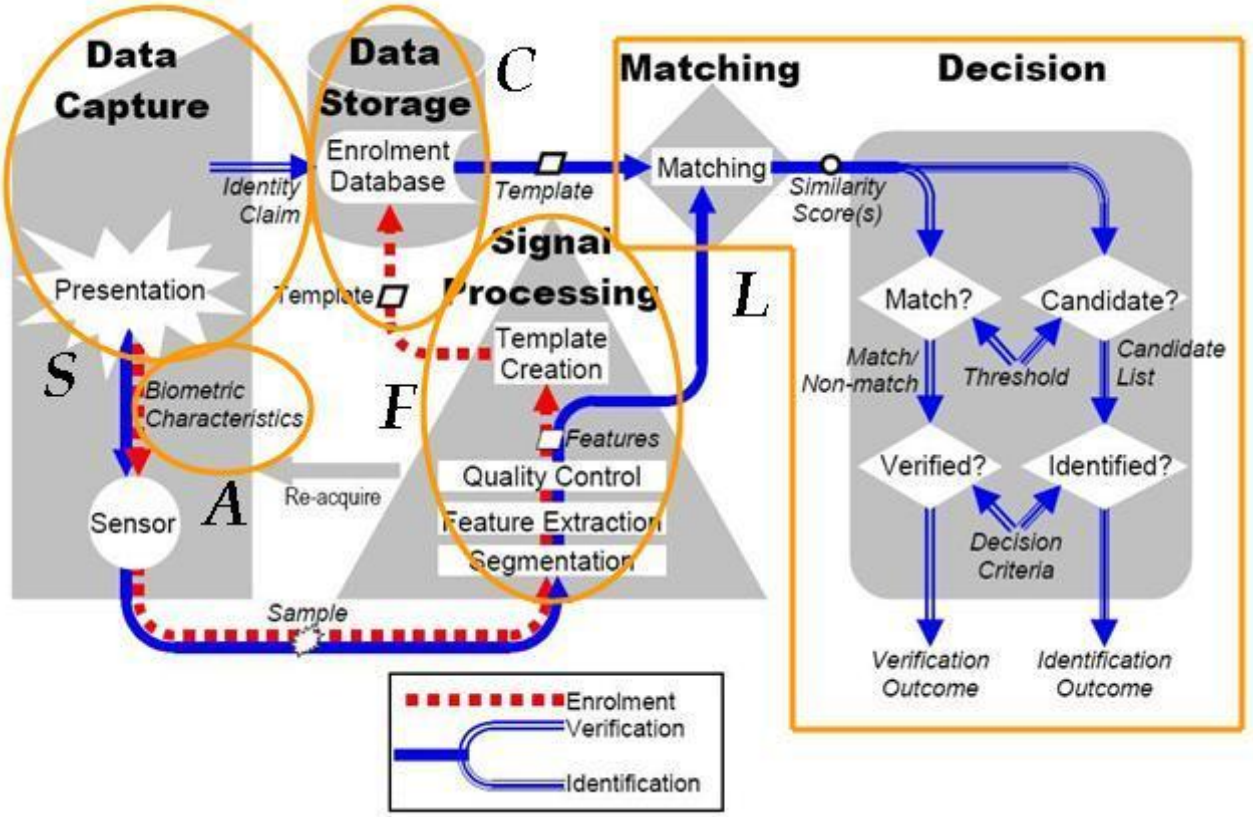
What is an Authentication System?

- *Authentication system:*
  - System that identifies the legitimate parties to a transaction, determines the actions they are allowed to perform, and limits their actions to only those that are necessary to initiate and complete the transaction

Authentication System

- Five sets of information (*A*, *C*, *F*, *L*, *S*):
  - The set ***A*** of authentication information is the set of specific information with which entities prove their identities.
  - The set ***C*** of complementary information that the system stores and uses to validate the authentication information.
  - The set ***F*** of complementation functions that generate the complementary information from the authentication information.
  - The set ***L*** of authentication functions that verify identity.
  - The set ***S*** of selection functions that enable an entity to create or alter the authentication and complementary information in *A* or *C.*

How does a Biometric System work?



- In a typical IT Biometric System
  - person registers with the system when one or more of his physical and behavioral characteristics are obtained.

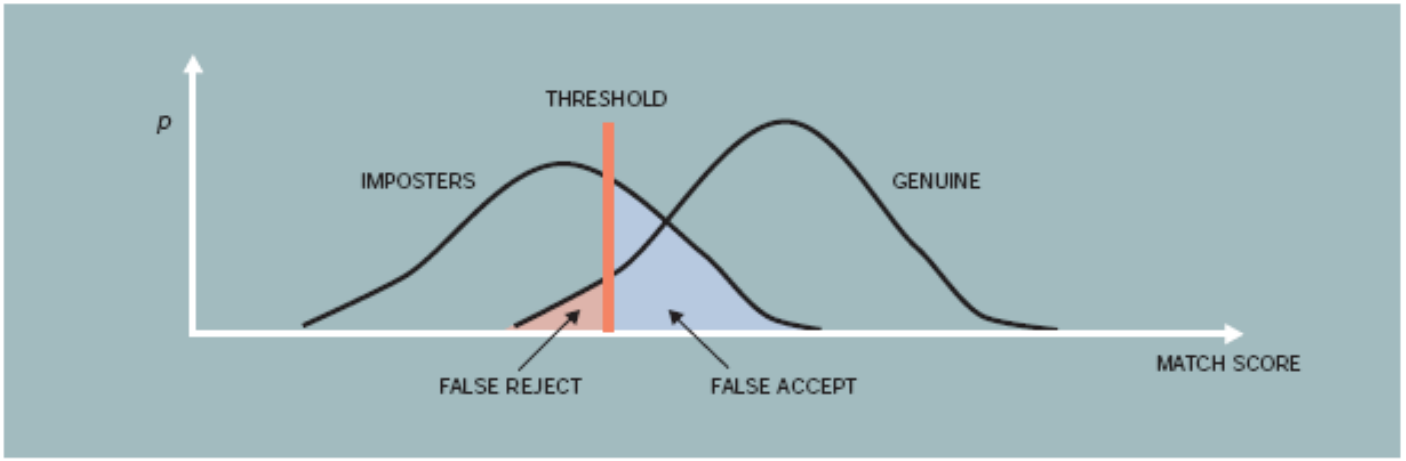
How does a Biometric System work?

- This information is then processed by a numerical algorithm, and entered into a database.
- The algorithm creates a digital representation of the obtained biometric.
- If the user is new to the system, he or she enrolls, which means that the digital template of the biometric is entered into the database.
- Each subsequent attempt to use the system, or authenticate, requires the biometric of the user to be captured again, and processed into a digital template.
- That template is then compared to those existing in the database to determine a match.

How does a Biometric System work?

- The process of converting the acquired biometric into a digital template for comparison is completed each time the user attempts to authenticate to the system.
- The comparison process involves the use of a Hamming distance.
- Ideally, when a user logs in, nearly all of his features match
- when someone else tries to log in, who does not fully match, and the system will not allow the new person to log in

Biometric System Performance



- Biometric accuracy is measured in two ways:
  - Rate of false acceptance (FAR);
    - an impostor is accepted as a match -Type 1 error.
  - Rate of false rejects (FRR)
    - a legitimate match is denied -Type 2 error.
- If the Type 1 and Type 2 error rates are plotted as a function of the threshold value, they will form curves which intersect at a given threshold value.

Biometric System Performance

- “Threshold Value" is defined which determines when a match is declared.
  - Scores above the threshold value are designated as a "Hit"
  - Scores below the threshold are designated as "No-Hit.“
- Type 2 error: If true match does not generate a score above threshold.
- Type 1 error: When impostor generates a match score above threshold.
- The point of intersection where Type 1 error equals Type 2 error is called the equal error rate (EER) or the crossover accuracy of the system.

Biometric	Crossover Accuracy
Retinal Scan	1:10,000,000+
Iris Scan	1:131,000
Fingerprints	1:500
Hand Geometry	1:500
Signature Scans	1:50
Voiceprints	1:50

Biometric System Performance

From "Biometric Product Testing: Final Report" by T. Mansfield, G. Kelly, D. Chandler and J. Kane, CESG/BWG Biometric Test Program, National Physical Laboratory, Teddington, Middlesex, TW11 0LV, U.K., March 2001.

- Very low (close to zero) error rates for both errors (FAR and FRR) at the same time are not possible.

Which Biometric is the Best?

- **Universality** (everyone should have this trait)
- **Uniqueness** (no two persons should be the same in terms of this trait)
- **Permanence** (should be invariant with time)
- **Collectability** (can be measured quantitatively)
- **Performance** (achievable identification accuracy, resource requirements, robustness)
- **Acceptability** (to what extent people are willing to accept it)
- **Circumvention** (how easy it is to fool the system)

Biometric Comparisons

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

H=High, M=Medium, L=Low

A comparison of biometrics from: Yun, Yau Wei. The '123' of Biometric Technology, 2003. Retrieved on November 21, 2005 from the World Wide Web: http://www.itsc.org.sg/synthesis/2002/biometric.pdf

Why Biometrics?

- Enhanced security and safety
- User convenience and personalization

Challenge is to design a biometric system

- with error rates as small as possible
- that will cover the entire user group for the given application
- that cannot be compromised.

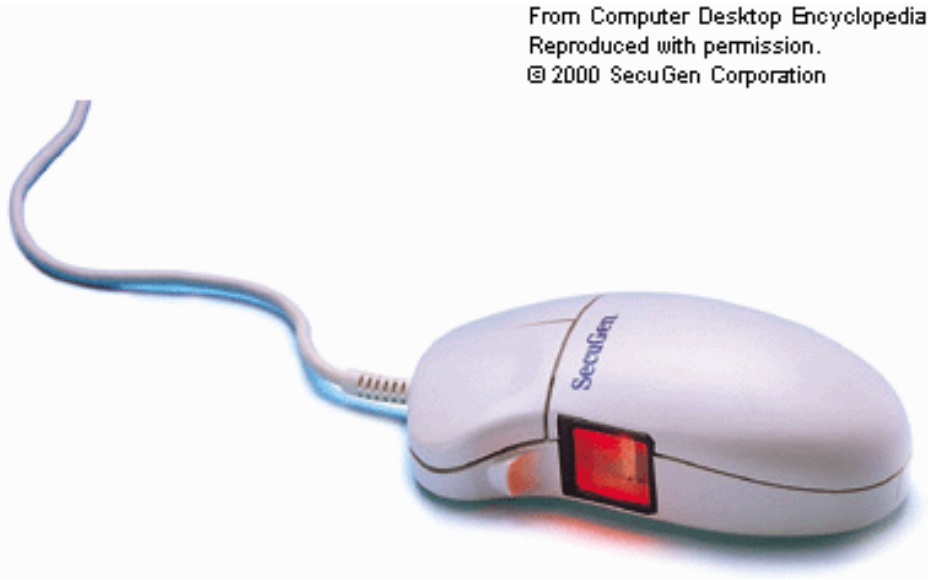
Which Biometric characteristics?

- Finger Print Scan
- Iris Scan

Fingerprint-Based Systems

- Fingerprint analysis:
  - biometric technique comparing scanned image of prints with a database of fingerprints.
- Two major methods of the identification of fingerprints:
  - comparison of lifted prints
    - Used in forensics mainly
  - live scanning
    - For authentication purposes (Security Applications)

Fingerprint-Based Systems



- Two types of fingerprint scanners are normally used:
  - capacitance scanners
  - optical scanners

Fingerprint-Based Systems

- Optical scanners
  - identify the print using light; depending on the brightness of the reflected light, optical scanners depict ridges as dark and valleys as light.
- Capacitance scanners
  - determine the print by using an electrical current. Valleys and ridges on the fingers produce different voltage output, allowing for discrimination between them.
- A typical scanner digitizes the fingerprint impression at 500 dots per inch (dpi) with 256 gray levels per pixel.

Fingerprint-Based Systems

- Figure A shows a fingerprint obtained with a scanner using an optical sensor.
  - Digital image of the fingerprint includes several unique features in terms of ridge bifurcations and ridge endings, collectively referred to as *minutiae*.

Fingerprint Analysis

- Fingerprint analysis software and scanners identify a set number of similarity points
  - 90 points are compared
- Often the score is simply a count of the number of the minutiae

Fingerprint Analysis

- Pattern-based (or Image-based) algorithms
  - Compare the basic fingerprint patterns between a previously stored template and a candidate fingerprint
    - Arch, and loops
    - Finds a central point in the fingerprint image and centers on that
- Minutia-based algorithms
  - Compare several minutia points
    - Ridge ending, bifurcation, and short ridge

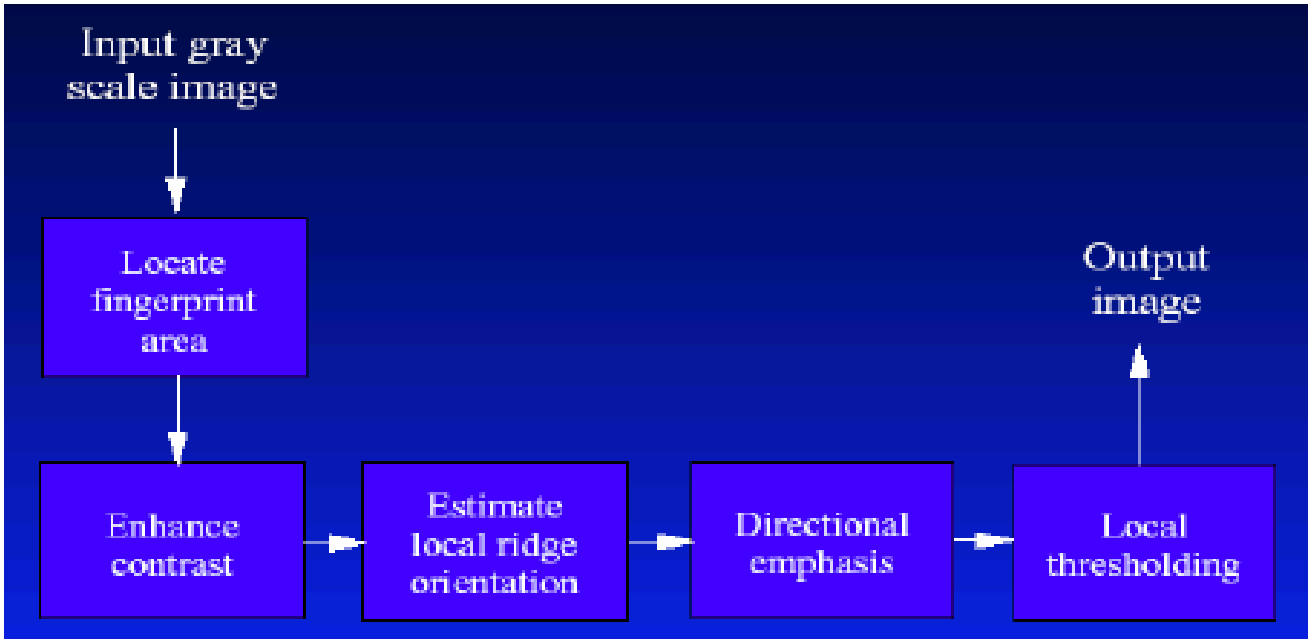
Fingerprint Advantage

- Uniqueness
  - Identical twins undistinguishable by DNA analysis can be differentiated with fingerprint analysis

Fingerprint-Scan Reliable?

- Fingerprint Images are not so well behaved in real-life.
  - Poor quality images
  - scars
  - cracks
  - dirt

Possible Improvement



- Technique:
  - A Weak Model Based Approach
    - Works with many different scanners
    - Fast to compute
    - “Hallucinates” to fill cuts
    - Improves overall system performance

Fingerprint-Scan Reliable?

Fake fingerprint

- The existing scanners are not totally immune to fraud
  - Optical scanners can be fooled by a picture
  - Capacitance scanners can be fooled by a mold of a finger
- Fingerprint scans although great for authentication is not infallible.

Iris Recognition

- Iris is the colored ring of tissue that surrounds the pupil of the eye.
- Accepted as the most personally distinct feature in the human body that is stable and unchanging throughout life.

Iris Recognition

- A method of biometric authentication
  - Uses pattern recognition techniques based on high-resolution images of the irides of an individual's eyes.
- It uses camera technology and subtle IR illumination
  - Create images of iris
    - Created to templates
- Rarely impeded by glasses or contact lenses

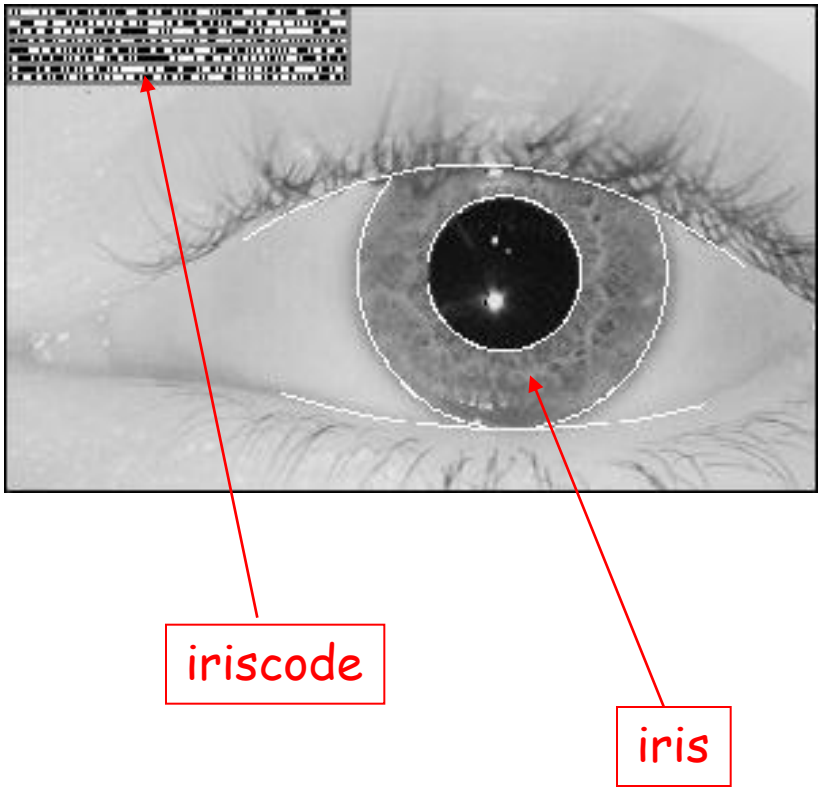
Iris Analysis

John G. Daugman, Ph.D, OBE, created the iris recognition algorithms required for image acquisition and matching.

- Identify the boundaries of the iris and the pupil in a photo of an eye
  - The set of pixels covering the iris is then transformed into a bit pattern
- A Gabor wavelet transform is used in order to extract the spatial frequency range.
- The result are a set of complex numbers that carry local amplitude and phase information for the iris image.
  - Resulting 2048 bits that represent an iris

Iris Analysis

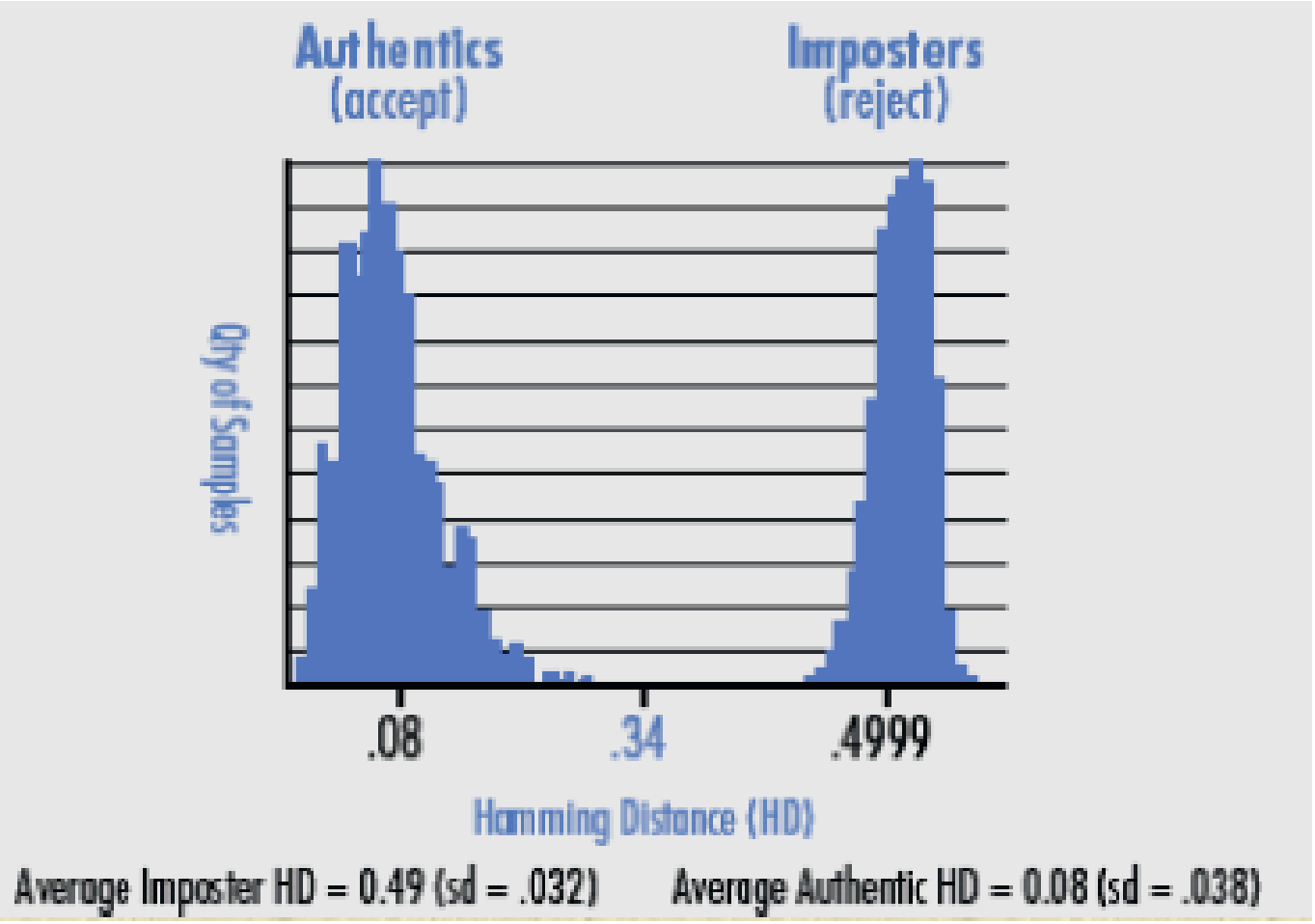
- An iriscode has an estimated 250 bits of entropy!
  - Contrast 1/10,000 false acceptance for fingerprints
- Hamming distance is the metric for iriscode similarity



Iris Analysis

- The overall Hamming Distance of paired comparisons yields a SCORE used in authentication or verification process.
- Identification Task: Candidate with the lowest SCORE is the winner.
- Verification Task: If the SCORE is lower than a set threshold the person is authenticated.

Iris Analysis



- 0.342 has been experimentally determined as the BEST Threshold and deployed.

Iris Advantages

- Advantages:
  - Its stability
  - Template longevity
  - Single enrollment can last a lifetime

Iris-Scan Reliable?

- Spoofing possibilities:
  - High-quality photograph of a face
  - Fake-iris contact lenses

Conclusion

- Biometrics not 100% reliable
- Combined Biometrics would be a better way to go.