Biometrics

CSH6 Chapter 29

"Biometric Authentication"

Eric Salveggio, Steven Lovaas,
David R. Lease, & Robert Guess

Topics

- Introduction
- Importance of I&A
- Fundamentals & Applications
- Types of Biometric Technologies
- Types of Errors & System Metrics
- Disadvantages & Problems
- Recent Trends in Biometric Authentication

Introduction

- Biometrics = automated recognition of people
  - Static or physical (fingerprint, face, iris,…)
  - Dynamic (physiological or behavioral) (voice, speech, typing patterns, gait, brain waves …)
- Growing acceptance
- Improvements
  - Security
  - Convenience
  - Portability
  - Costs

Authentication is based On something you

- ***Know***
- ***Have***
- ***Are (static biometrics)***
- ***Do (dynamic biometrics)***

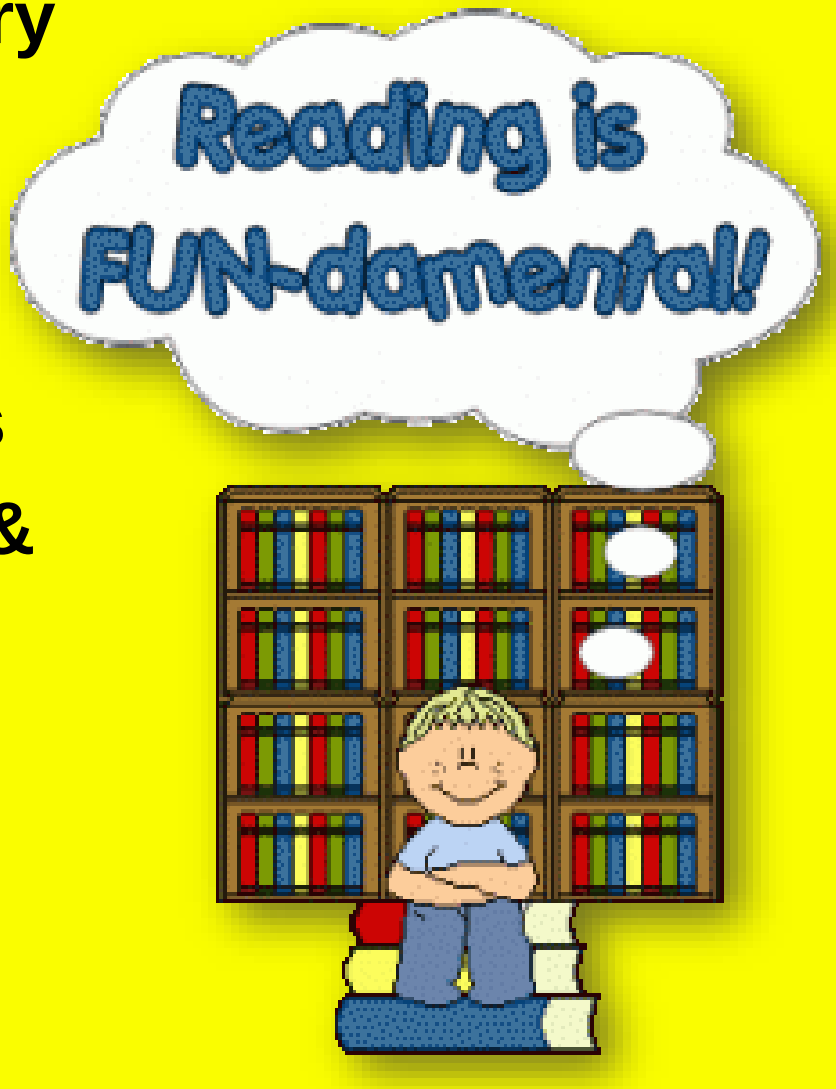
that others don't / aren't / cannot.

Importance of I&A

- Prerequisite to security & efficiency
  - Exclude intruders
  - Allocate resources
  - Authorize access modes
- Identification by person not scalable for computing systems
  - Voice, appearance, gait…
  - Inefficient & inaccurate
  - Foolable using social engineering
  - Impossible to manage remote access

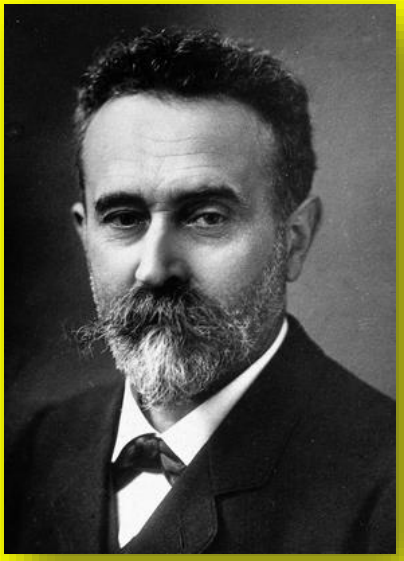
Fundamentals & Applications

- Overview & History
- Properties of Biometrics
- IA&A
- Application Areas
- Data Acquisition & Presentation



Overview & History

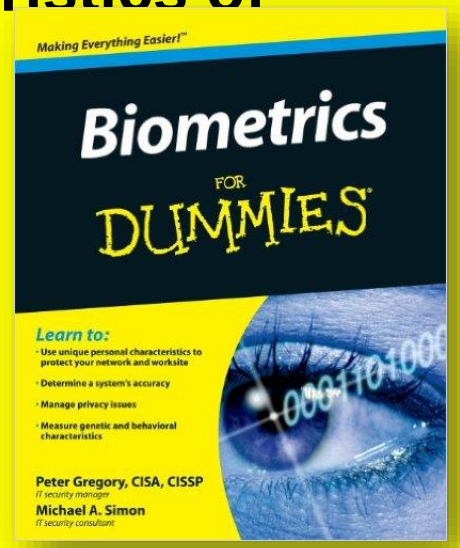
- Non-automated biometrics
  - Biological systems recognize others as individuals or as members of species/group
  - Human beings routinely recognize each other using face, voice, body appearance…
- Potters in Assyria used thumbprints (300 BCE)
- Handwritten *chops* (signatures) in China
- Fingerprints used in Tang Dynasty (618-906 CE)
- Alphonse Bertillon introduced anthropometry (1882)
- Edmond Locard proposed fingerprint analysis (1918) using 12 specific points –
- still used today



Alphonse Bertillon

Properties of Biometrics (1)

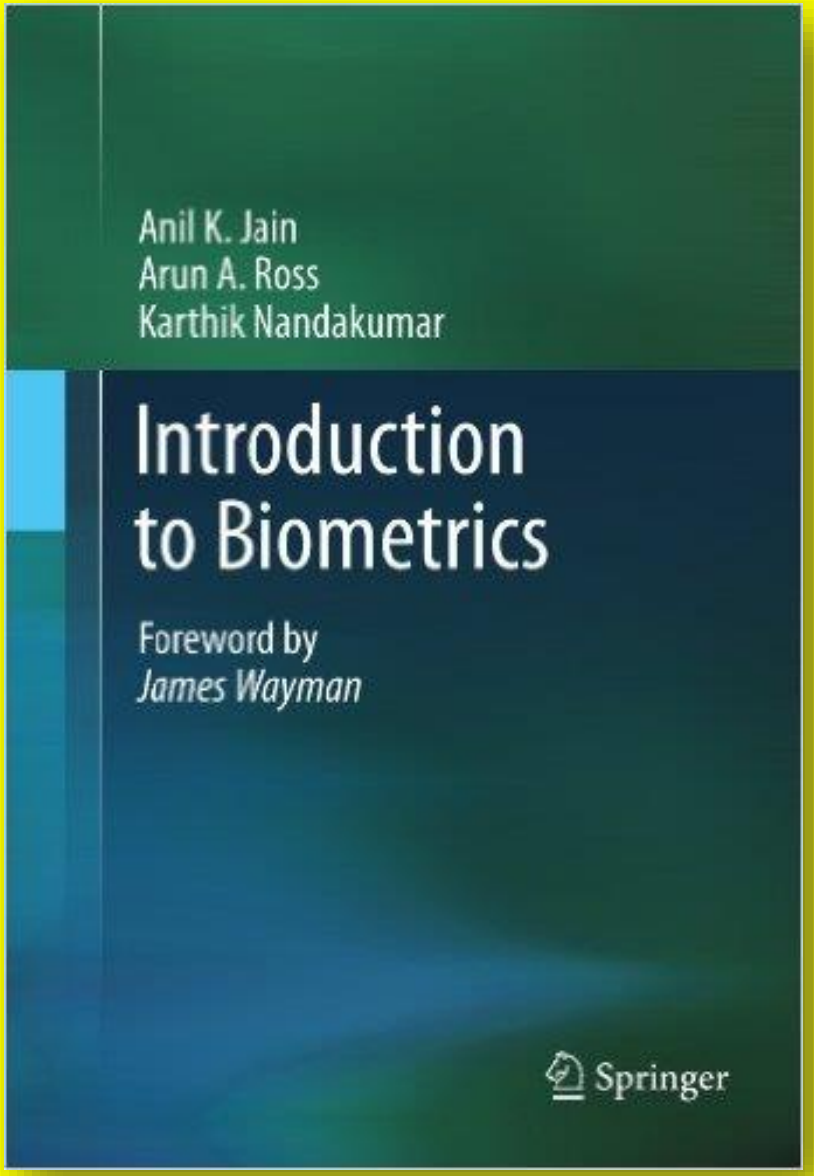
- Focus on "automatic identification of a person based on his or her physiological or behavioral characteristics."
- *Biometric* can be noun or adjective
- Currently using unique characteristics of
  - Fingerprints
  - Hand geometry
  - Face
  - Iris
  - Voice
  - Signature



- Biometrics difficult to circumvent through deceit
  - But gummy bears are a problem!

Properties of Biometrics (2)

- Requirements:
  - Universality
  - Uniqueness
  - Permanence
  - Collectability
  - Acceptability
- Additional factors in evaluation of biometrics
  - Performance
  - Circumvention



IA&A

- Identification is allocation of a unique *identifier* to a person or a system
- Authentication is the binding of identifier to user of that ID
- Verification is process of establishing whether authentication offered is correct
- Biometrics can serve for identification & authentication in one process
  - Identification through a biometric automatically leads to authentication
  - Except in case of identical twins or other identical ‘tuplets (effectively genetic clones)

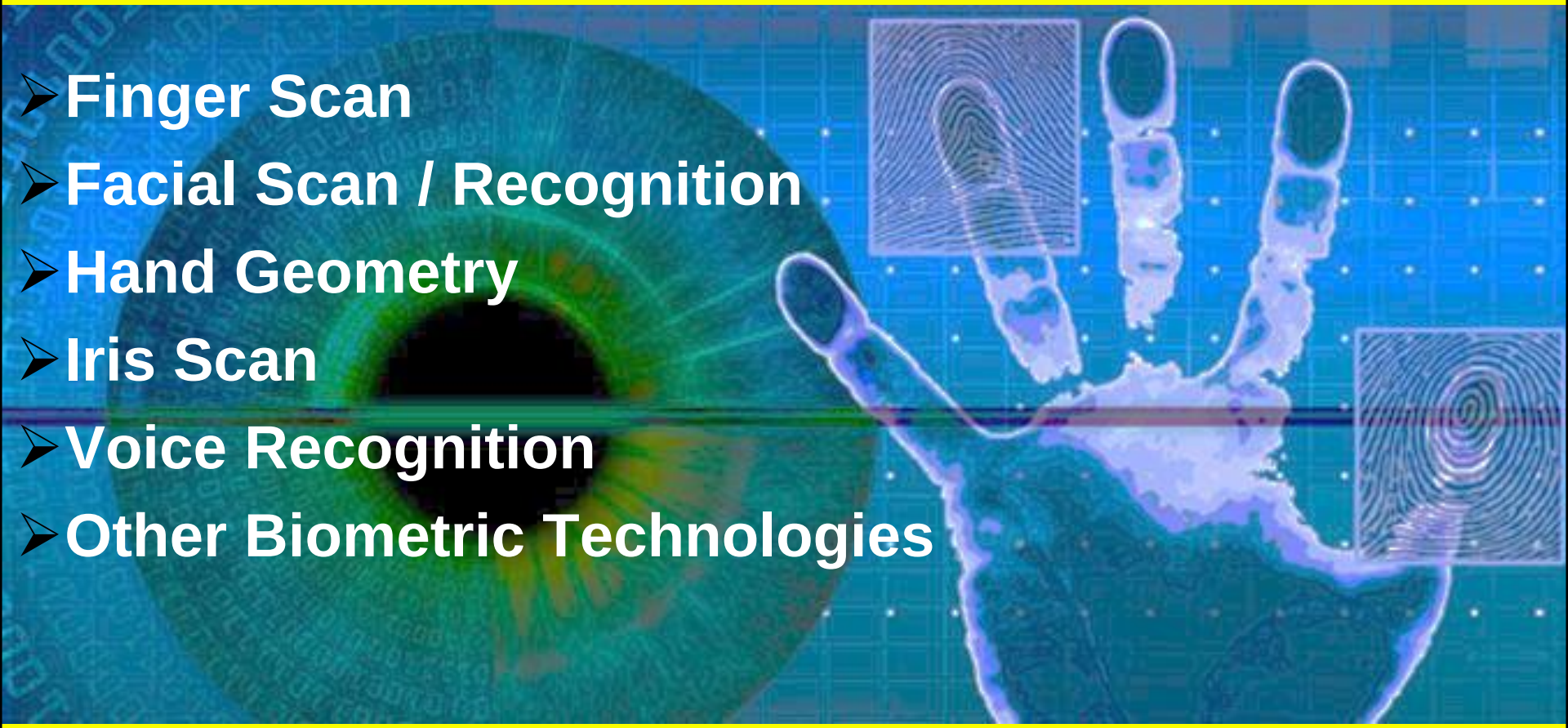
Application Areas

- Security (logical access systems)
  - Access to computer systems, networks, data storage…
- Facilities access (physical access systems)
  - Access to buildings, rooms, cabinets, safes…
- Ensuring uniqueness of individuals
  - Prevent double-dipping in public sector
- Public identification systems
  - Identifying terrorists, criminals
  - Or forensic applications such as dental records
- Data acquisition and presentation (see next slide)

Data Acquisition & Presentation

- **Enrollment**
  - **Initial data collection and processing**
  - **Templates are mathematical representation of biometric information**
    - ✓**Think of it as a kind of hash function**
    - ✓**Little interoperability among systems**
- **Presentation**
  - **How user provides system with new data for comparison with template**
  - **E.g., scanners, cameras, microphones**
  - **Typically do not store original data (e.g., face images) but only template**

Types of Biometric Technologies



- Finger Scan
- Facial Scan / Recognition
- Hand Geometry
- Iris Scan
- Voice Recognition
- Other Biometric Technologies

Finger Scan (1)

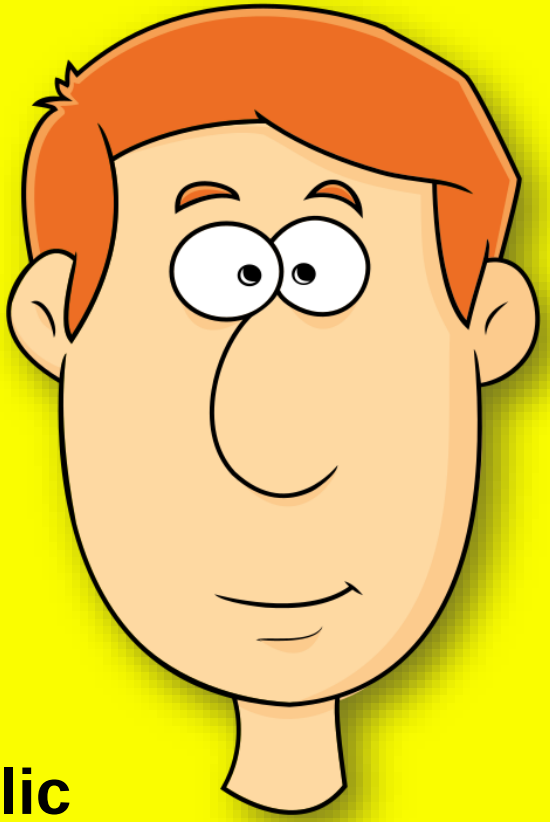
- Most widely deployed technology
  - Even excluding police fingerprinting
- Typically scan a single finger on one hand
  - But can enroll more than one finger in case there's a Band-Aid™ in the way – or no finger after an amputation(!)
- Advantages
  - Costs low
  - Easy to use
  - Low error rates
  - Quick to process
  - Easy to deploy (but some resistance due to association with law enforcement)

Finger Scan (2)

- Wide access to methods for defeating biometric finger scanning technology
  - Dummy latex finger
  - Gummy Bears™ with fingerprints etched on surface
  - Manipulation of scanner to raise latent print of previous user
  - Use of detached real amputated finger *(eeeeuuuuwww)*
- Countermeasures
  - Force use of more than one finger
  - Use thermal and moisture sensors to discount fake or dead fingers
- Problems with dry/wet fingers

Facial Scan / Recognition (1)

- Used by most people every day – naturally
  - May be more acceptable than other biometrics to some non-technical subjects
  - Acceptance of individual, open recognition & authentication
  - Well-established database + controllable input conditions = low error rates
- Covert use for *recognition*
  - Airport scanners
  - Crowd scanners
  - Strongly opposed by much of public
- Accuracy can be terribly low; e.g., >50% error rate in trials at Palm Beach FL Intl Airport



Facial Scan / Recognition (2)

Weaknesses

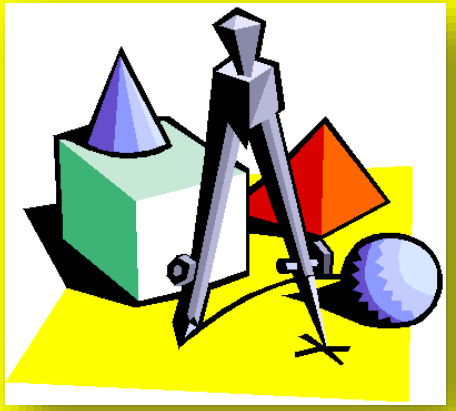
- False matches (acceptances)
  - Common for identical twins
  - May be exploited by impersonators
- False non-matches (rejections)
  - Facial expressions
  - Hairstyle, makeup, facial hair, eyeglasses
  - Changes in body weight
  - Age-related face changes
- Perceived threat to privacy
  - Public dislike concept of covert facial recognition
  - Most people do not know that pictures are not stored – only templates

Hand Geometry (1)

- Distinctive aspects of hand
  - ❑Height & width of hand & fingers
  - ❑Recognition Systems Inc (RSI) scanner
    - ✓90 different measurements
    - ✓3-4 enrollments
    - ✓Length, width, thickness, surface area
- Anti-exploit methods against fakes and amputations
  - ❑Temperature sensors
- Used exclusively for verification, not identification
- Mostly for physical access & time/attendance

Hand Geometry (2)

- **Strengths**
  - Resistant to environmental stresses
  - Established & reliable
  - Easy to use
  - Difficult to defeat
  - Small template size (store lots of them)
  - Stable characteristics
  - High user acceptance / low stigma
- **Weaknesses**
  - Limited accuracy
  - Relatively large scanner
  - Resistance to touching surfaces (clean freaks)
  - Difficulties for disabled people
  - Relatively expensive



Iris Scan

- Unique patterns of color in iris
  - Even left/right irises of same person differ
  - Ideal to enroll both eyes – more difficult to spoof
  - Both I & A
  - Stable over time – but affected by age & disease
- Highly accurate
  - Lowest error rate
  - Highest accuracy

- Weaknesses
  - Moderately demanding enrollment & acquisition
  - Some resistance to have eyes scanned
    - ✓Physical & psychological
  - Affected by lighting conditions
  - Problems with eyewear
  - Expensive

Voice Recognition

- Distinctive aspects of voice
  - Pitch
  - Waveform
  - Dynamics (amplitude, inflection)
  - Phonetics (accent)
- Advantages
  - Can use telephone equipment
  - Inexpensive & easy to use
  - Can speak passwords
  - No stigma – generally accepted
- Disadvantages
  - Replay attacks
  - Low accuracy
  - Ambient noise
  - Low-quality capture
- Accuracy variable
  - Soft/loud speech
  - Hoarseness, stuffed nose
  - Illness, aging, smoking…

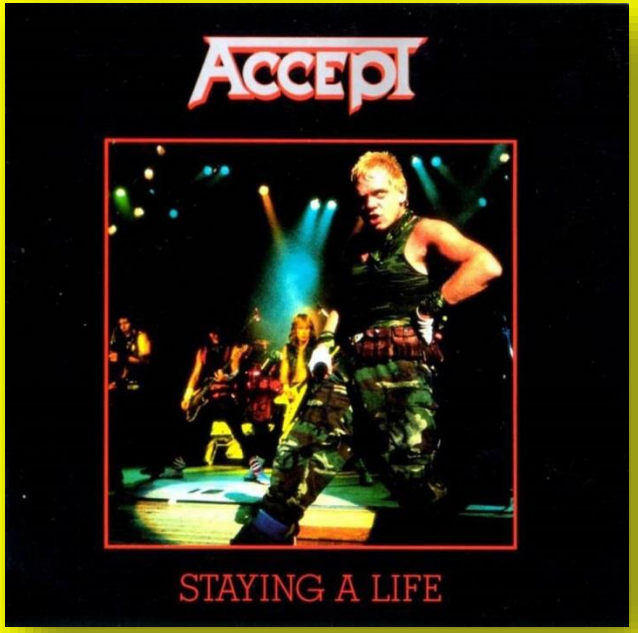
Other Biometric Technologies

- Signature scanning
- Typing (keystroke) dynamics
  - Interval between keystrokes on passphrase
- Gait patterns
- Lip movements
- Retinal scanning
  - Lack of user acceptance
  - High cost
  - Difficult / painful acquisition
  - Expense
- Future possibilities
  - Body odor (☹)
  - Skin reflectance
  - Ear shape
  - Brain waves

Types of Errors & System Metrics

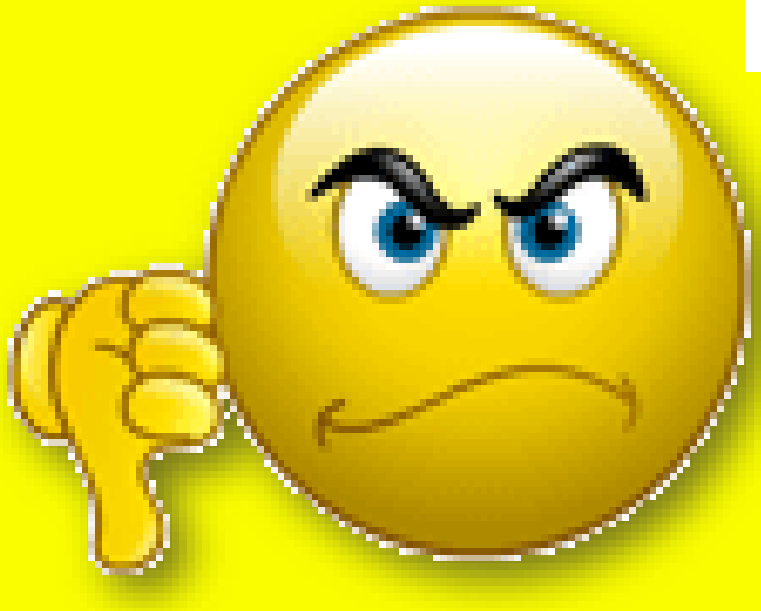
- False Accept
- False Reject
- Crossover Error Rate
- Failure to Enroll
- Transaction Time

False Accept



- Imposter will be accepted
- AKA
  - False match
  - False positive
  - Type 1 error
- Importance depends on context
  - Bank / root access – high concern
  - Facial recognition in casinos vs card-counters – low concern

False Reject



- Legitimately enrolled user NOT accepted
- AKA
  - False nonmatch
  - False negative
  - Type 2 error
- Typically lock user / employee out of system / facility
- Can occur because of
  - Changes in user's biometric data
  - Environmental changes
  - Problems with sensors
- Biometric systems typically more susceptible to false rejects than to false accepts

Crossover Error Rate (CER / EER)

- The rate at which Type 1 and Type 2 errors become equal is called the CER or EER
- Power of the test: Rates of Type 1 & Type 2 errors are inversely affected by change
  - As we reduce the probability of false accept (Type 1 error), we tend to increase the probability of false reject (Type 2 error)
  - As we reduce the probability of false reject (Type 2 error), we tend to increase the probability of false accept (Type 1 error)
- Used as a measure of strength: the lower the rate, the stronger the authentication
- Generally used to compare biometric systems

Failure to Enroll (FTE)

- User cannot complete enrolment into biometric authentication system
  - Physical disability
  - Static or dynamic biometric profile less distinctive than required by system
- Can be significant problem
  - "Internal, employee-facing deployments"
  - Increased security risks
  - Increased system costs

Transaction Time

- How long it takes to match data input to reference sample
- Long delays problematic
  - Processing queues of employees through chokepoint
  - Small delays can add up to significant pile-ups & delays for entire queue
  - Leads to employee resistance
  - Security guards can waive identification & authentication if lines become intolerable

Disadvantages & Problems

- General Considerations
- Health & Disability
- Environmental & Cultural
- Cost
- Attacks on Biometric Systems
- Privacy Concerns
- Legal Issues

General Considerations (1)

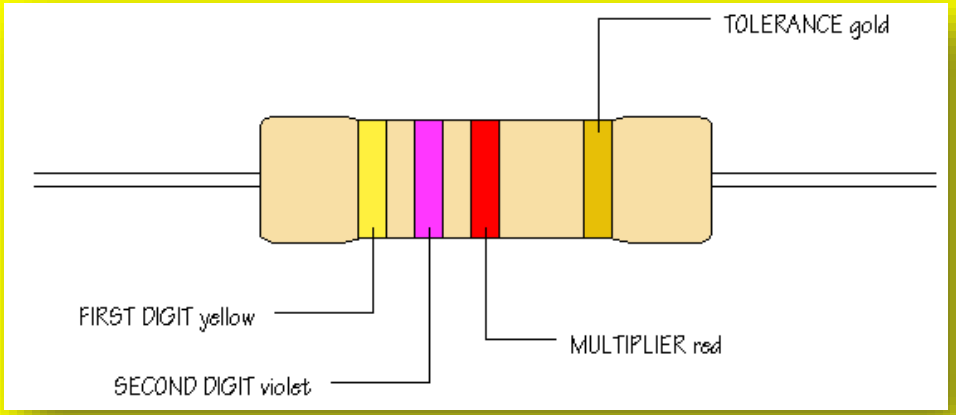
- Errors inevitable
- False accept / match / positive (Type 1 error)
  - Particularly serious
  - Threatens security by admitting unauthorized personnel
- False reject / nonmatch / negative (Type 2 error)
  - Reduce productivity & efficiency
  - Increase costs

General Considerations (2)

- Define acceptable (reasonable) error thresholds
- Some systems almost impervious to fraud
  - Iris scans
- Others easy to defeat
  - Face: makeup, glasses, hairstyle
  - Fingerpints: gelatin/rubber fake fingers
- Increased training required cf badges/passwords
- Hypersensitivity to nonstandard data capture

General Considerations (3)

- Resistance to biometric I&A
  - Privacy
  - Intrusiveness
  - Safety/cleanliness
  - Fear of eye scans
- Religious objections
  - Some cultures do not permit photographs
  - Some see eye as special soul-related organs
- Have backup methods available to avoid serious personnel problems

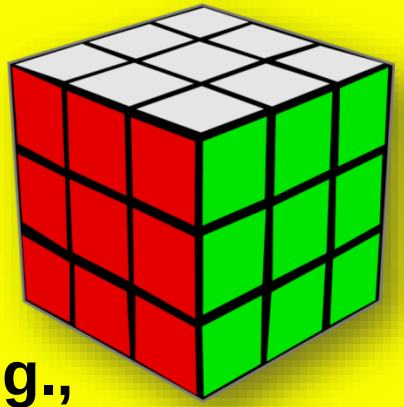


Health & Disability

- Arthritis, other deforming disease
  - Interfere with data capture in enrolment
    - ✓E.g., hand geometry
  - May prevent effective physical positioning for data entry during I&A
    - ✓Neck injuries, back problems, broken limbs/hands
- Sensitivity to environmental stress
  - Bright light of iris/retinal scans may be intolerable for photophobic people
- Tremor can interfere with many biometrics (both enrolment and data entry)
- Variations in physical size can interfere
  - Too big, too small, too tall, too short….
- Speech: too slow/fast, loud/soft, laryngitis,…
- Excessive skin moisture/dryness,…

Biological Variations

- Fingerprints
  - Missing
  - Damaged (calluses)
  - Chemicals
  - Scarring
- Iris scans
  - Dark irises
  - Retracted pupils (e.g., drug use)
- Aging effects
  - Skin
  - Face shape
  - Voice



- Preventing discrimination
  - American with Disabilities Act precludes adverse effects on
    - ✓Disabled
    - ✓Ill
    - ✓Ethnic minorities
    - ✓Elderly
    - ✓….
  - Resentment if
    - ✓Takes much longer
    - ✓Causes repeat scans
  - Be sure to have backup I&A methods on hand

Environmental & Cultural Factors

- Changes in appearance can influence face recognition
  - Hairstyle
  - Facial hair
  - Headwear
  - Weight gain / loss
- Voice recognition – ambient noise, sore throat
- Fingerprints: frequent hand-washing – e.g., health-care staff
- Ambient light
  - Face
  - Iris

Cost

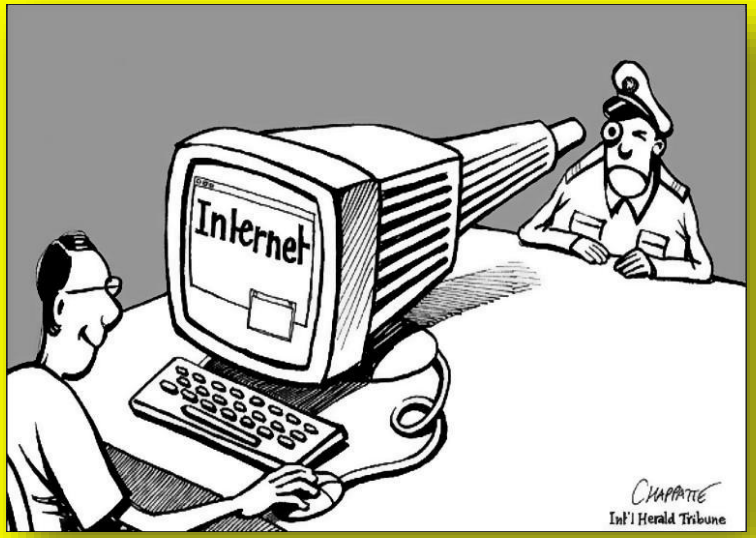
- Cost falling dramatically in recent years
  - Fingerprint scanners $50 or less
  - But voice-recognition >$50K
  - Minimum costs
    - ✓~$200/user
    - ✓$150K or more for medium-sized business
  - Still major barrier for many organizations
- Lack of widely-accepted standards
- Poor interoperability
- May cope with problems through
  - Better training
  - Combination with other I&A methods

Attacks on Biometric Systems

- Less vulnerable to attack than other I&A systems
- Stolen biometric identity serious problem
  - Cannot easily be canceled & replaced
  - Difficult to revoke
  - Long-term usability of stolen identifier
- Current work on cancelable biometrics
  - Would include a repeatable modification of the biometric data at each enrolment
  - Thus limit damage to 1 system only, not all others

Privacy Concerns

- Biometrics combine I & A
  - Facial recognition (FR), for example, can run covertly
    - ✓2001 Super Bowl – Tampa Police deployed FR
    - ✓But wider acceptance at airports after 9/11 attacks
  - Finger scanning associated with police work & criminals
  - Concern over using biometrics for nationwide identification
- Summary of concerns:
  - Loss of anonymity & privacy
  - Unauthorized use of biometric data
  - Unauthorized disclosure
  - Reduced expectation of privacy
  - Abuse by government agencies



Legal Issues

- In US, 4 categories of invasion of privacy
  1. Intrusion into private life
  2. Public disclosure of private facts
  3. Impersonation
  4. Publication putting victim in false light (defamation)
- Biometrics generally involve (1) and (2)
- Storing hashed version of recognition templates may resolve these issues
  - One-way encryption (like passwords)
  - Can recognize match with data but not store original data

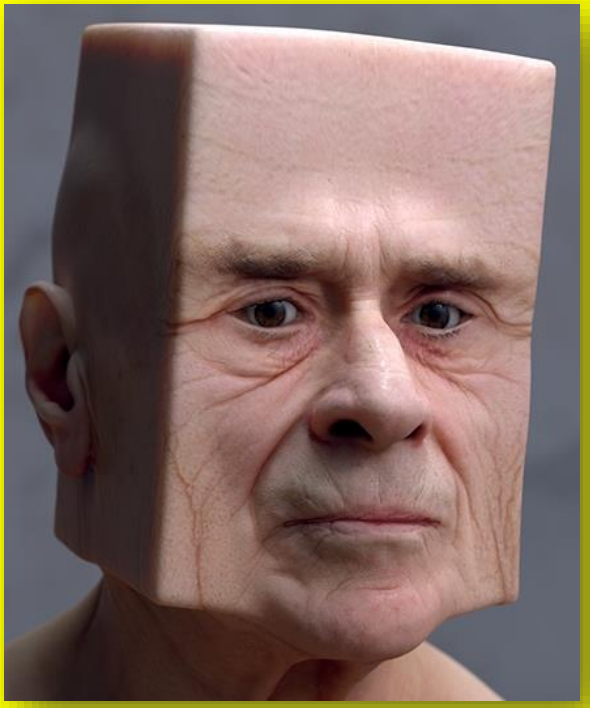
Recent Trends in Biometric Authentication

- Government Advances
- Face Scanning at Airports & Casinos
- Deployment in Financial Industry
- Healthcare Industry
- Time & Attendance Systems

Government Advances

- US government major user of biometrics
  - DoD – Common Access Card (smart card with biometric data)
  - DHS
    - ✓US-VISIT (face, fingerprint)
    - ✓TWIC (Transportation Worker Identity Credential)
  - INS
  - DoT

Face Scanning at Airports & Casinos



- Airports moving to include face-scanning
  - Studies show high error rates
  - Low accuracy rates
- Casinos
  - Identify intelligent people who win more than casinos want them to
  - Spot frauds
  - Networked 100s of casinos to share info on whom they want to exclude
- International law
  - Question of whether these systems violate UN Universal Declaration of Human Rights, Article 12

Deployment in Financial Industry

- Facial recognition at ATMs
- Fingerprint scanners for brokers
- Iris scanning for high-security points
- United Bankers' Bancorporation (UBB)
  - Fingerprint recognition
  - Employees
  - Customers
- Others:
  - Wells Fargo
  - Bloomberg Financial
  - Janus Capital Management

Healthcare Industry

- HIPAA regulations force better privacy & security for patient data
  - E.g., Mayo Clinic – fingerprint ID 2002
- Slower adoption than in financial industry
  - Physical contact with fingerprint reader
  - Error rates higher & accuracy lower than expected
  - May be affected by chronically dry hands from repeated hand-washing and repeated use of disinfectants
- High costs of implementation in hospitals

Time & Attendance Systems

- Biometric systems
- Originally implemented in factories
- Extending to white-collar workers
- Mostly using finger-scanning systems

Racial Bias in Facial Recognition

Lohr, S. (2018). "Facial Recognition is Accurate, if You're a White Guy." *New York Times* (Feb 9, 2018).
< https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html >

- **Disturbing results of study**
  - **Lighter-skinned men: 99% accuracy**
  - **Lighter-skinned women: 93% accuracy**
  - **Darker-skinned men: 88% accuracy**
  - **Darker-skinned women: 65% accuracy**
- **Possible reasons:**
  - **Data samples widely used for AI in facial recognition are as high as 75% male & >80% white**
- **Very little government regulation of this technology**

Now go and study