

Cristina Nita-Rotaru



CS355: Cryptography

Lecture 21: Biometrics.

Authentication

- ▶ Something that you know
- ▶ Something that you have
- ▶ Something that you are

What Are Biometrics ?

(ancient Greek: *bios* = "life", *metron* = "measure")

- ▶ **Biometrics are automated methods of recognizing a person based on a physical or behavioral characteristic.**
- ▶ Physical Features
 - ▶ Fingerprint or fingerscan
 - ▶ Hand geometry
 - ▶ Face recognition
 - ▶ Retinal scans
 - ▶ Iris scans
- ▶ Behavioral Characteristics
 - ▶ Handwritten signature
 - ▶ Voice recognition
 - ▶ Typing
 - ▶ Gait



Biometric System

▶ Registration:

- ▶ A person registers with the system when one or more of his physical and behavioral characteristics are obtained.
- ▶ Information registered in a database (digital template), based on some algorithm.

▶ Use of biometrics:

- ▶ Biometric of the user is captured and processed into a digital template
- ▶ **Verification:** Compare a sample against a single stored template
- ▶ **Identification:** Search a sample against a database of templates.

Performance of Biometric Systems

- ▶ **False accept rate (FAR):** percent of invalid users who are incorrectly accepted as genuine users.
- ▶ **False non match or reject rate (FRR):** percent of valid users who are rejected as impostors.
- ▶ FAR and FRR can typically be traded off against each other by changing some parameter.
- ▶ High degree of confidence, forensic DNA evidence and iris recognition technology (can discriminate between individuals with identical DNA, such as monozygotic twins)

Applications of Biometric Technologies

- ▶ **Secure identification and personal verification**
- ▶ WHERE: Federal, state and local governments, in the military, travel and transportation, financial, law enforcement, health and social services.
- ▶ Specific applications:
 - ▶ Civil and government ID
 - ▶ Network security infrastructures
 - ▶ Surveillance and screening
 - ▶ Retail/ATM/point of sale
 - ▶ Secure electronic banking
 - ▶ Telephony
 - ▶ Criminal ID

More about Applications...

- ▶ Biometrics can be used alone or integrated with other technologies such as smart cards, encryption keys and digital signatures
- ▶ Think about the number of passwords you must remember...Use of biometrics personal authentication: convenience, accuracy (?), provide audit trail
- ▶ Many countries started using biometrics

Use of Biometrics...

- ▶ Japan has been using retinal and/or iris scans for bank ID since 1997
- ▶ Malaysian airport uses face recognition for baggage claim
- ▶ USA started using it for airport security Dec. 2004
- ▶ UK airports
- ▶ European standard for biometric passports, US
- ▶ Identity cards including biometrics: UK, Oman, United Arab Emirates, Brazil

Biometrics: the DARK SIDE ...

- ▶ **Social acceptance:** Perceived as invasive; people liked facial scans less than fingerprints as a substitute for a PIN in ATM.
- ▶ **Easy to forge:** Biometric measurements are easy to forge. It is easy to steal a biometric after the measurement is taken.
- ▶ **Impossible to revoke:** What happens if a biometric is stolen? It can not be revoked... Once someone steals your biometric, it remains stolen for life.
- ▶ **Privacy:** issues...Biometrics are personal.



Handwritten Signature

- ▶ Handwritten signatures used a lot in the past to validate deals or identification
- ▶ Seals were mostly used in Europe
- ▶ How easy is to forge handwritten signatures? Depends who verifies, how trained the verifiers are
- ▶ **Experiment:** 105 professional document examiners, 144 pairwise comparisons, **mistake rate** was **6.5%**
- ▶ Rules and conventions of accepting handwritten signatures differ from country to country



...-Rotaru

Handwritten Signature

- ▶ Automated signature recognition/storage: signature tablet
 - ▶ Signature tablet: sensor surface on which the client signs
 - ▶ Uses shape, speed, stroke order, off-tablet motion, pen pressure and timing information captured during the act of signing.
- ▶ **Equal error rate (false accept = false reject)** is about **0.01** for current commercial products, not acceptable for retail stores
- ▶ Used for financial document to prevent identity fraud



Handwritten Signature

- ▶ SMARTpen Biometric Authentication System (BiAS):
 - ▶ pen that uses sensors to authenticate individuals by the biometric characteristics of their signatures.
 - ▶ writes on regular paper
 - ▶ built-in sensors register the dynamics of writing, including the forces that are applied in 3D on paper, such as the speed, acceleration and angles of writing.
- ▶ **Equal error rate (false accept = false reject)** is about **0.01** for current commercial products, not acceptable for retail stores



Face Recognition

- ▶ Human ability to recognize other people's facial features and expression is much better than any automatic system to date.
- ▶ Photo identification widely used.
- ▶ **Experiment:** Psychologists at University of Westminster, supermarket chain and bank
 - ▶ Recruited 44 students and issued them 4 credit cards with 4 different pictures with varied quality of the photos
 - ▶ **Optimal conditions:** experienced cashiers, enough time, students used any of the cards, several times'
 - ▶ Result: **cashiers could not tell the difference**



Face Recognition

- ▶ How well does the technology works?
- ▶ Methods not very robust, depends on lighting, viewpoint and expression. **Error rates were up to 20%.**
- ▶ Error rate very high when compared with other biometrics recognition (**less than 1%**)
- ▶ Many companies are providing face recognition products
- ▶ Several countries use face recognition for identification in airports



Face Recognition



- ▶ Interesting psychological aspect: technology has problems, but system seems to work
- ▶ Studies done by banks showed that fraud dropped substantially when credit cards with photo IDs were issued/used
- ▶ In a borough in London a computer system that was said to **scan faces in the crown for local criminals** got a significant decrease in burglary, shoplifting and street crime

Fingerprint: Some History ...

- ▶ First modern systematic use of fingerprints seems to be in India in mid 19th century: use of fingerprints to prevent rich people to pay poor people to serve in prison in their place
- ▶ Discovered independently by a medical missionary in Japan
- ▶ Mainstream use in 1900 when a former chief officer from Bengal becomes Commissioner of the Metropolitan Police in London



Fingerprint: Applications

- ▶ Finger print technology captures a representation of the finger; it involves storing the image of the finger and comparing
- ▶ Two main applications:
 - ▶ Government identification
 - ▶ Criminal identification: IAFIS “Integrated Automated Fingerprint Identification System” is the law enforcement tool used either to identify a fingerprint’s maker or to confirm prints



IAFIS

- ▶ Became operational in July 1999
- ▶ It is the national fingerprint and criminal history system maintained by the FBI
- ▶ It provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.
- ▶ Answer received between 2 hours to 24 hours (before the integration/digital it took days sometime months)
- ▶ Largest biometric database in the world, containing the fingerprints and corresponding criminal history information for more than 66 million subjects.

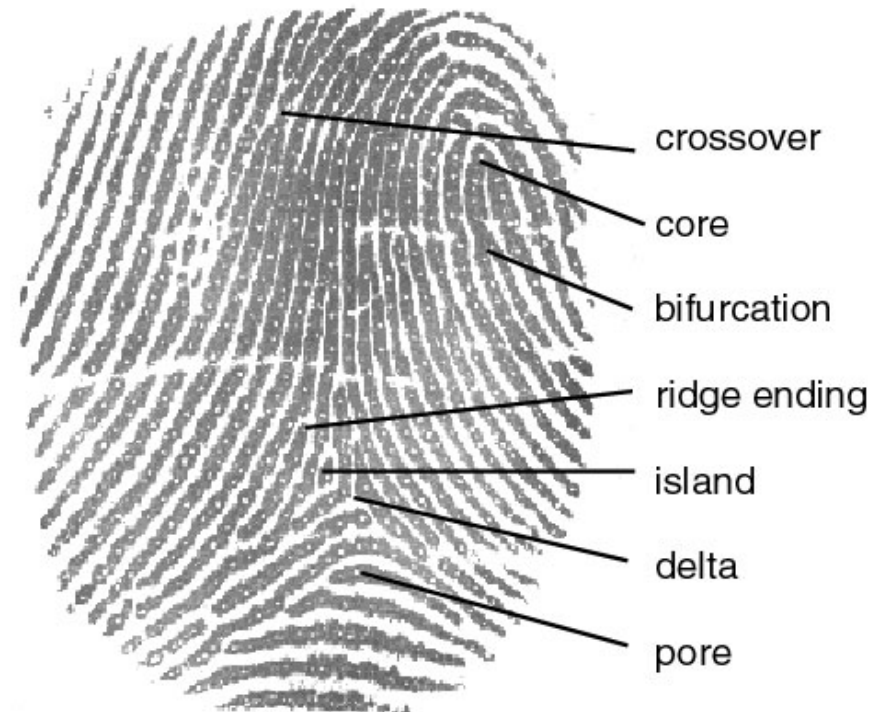
Fingerprint: Storage



- ▶ Storage is an issue
- ▶ FBI and NIST developed an image coding standard for digitized fingerprints
- ▶ The standard is a discrete wavelet transform-based algorithm referred to as Wavelet/Scalar Quantization (WSQ).
- ▶ Storage requirements...500 dots per inch with 8 bits of grayscale resolution. Do the math ...

Fingerprint Identification

- ▶ Fingerprint is made of a series of ridges and furrows
- ▶ Fingerprint uniqueness: determined by the pattern of ridges and furrows as well as the minutiae points
- ▶ **Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending**



Fingerprint Identification Accuracy

- ▶ Error rate in forensic applications is very low, it depends on the quality and size of the image taken at the crime
- ▶ Fingerprints require a number of match points, different from country to country. UK requires 16 points

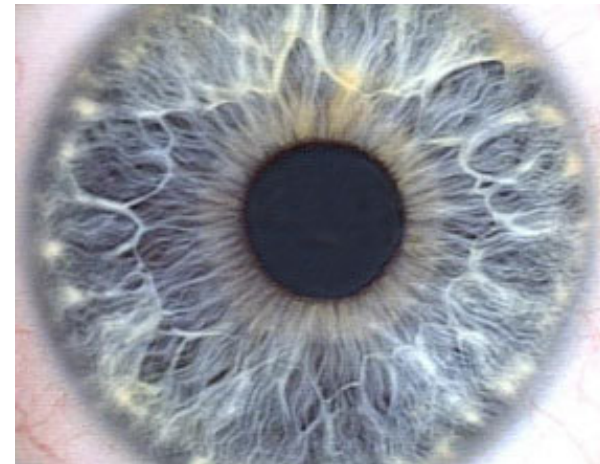
Finger-scan

- ▶ A live acquisition of a person's fingerprint.
- ▶ Different type of devices:
 - ▶ Glass plate
 - ▶ Electronic
 - ▶ Ultrasound



Iris Scan

- ▶ Probability that two people have the same Iris Code is less than $1/10^{52}$
- ▶ 512 byte Iris Code represents the visible characteristics of the eye
- ▶ Iris Code includes “266 spots” to distinguish between irises (claim is most other biometrics have between 10-60 distinguishing spots)
- ▶ Issues: obtain the information without being intrusive
- ▶ Other issues: blinking, eyelashes, sunglasses



Retinal Scan

- ▶ Analyses the layer of blood vessels at the back of the eye.
- ▶ Scanning involves using a low-intensity light source and an optical coupler
- ▶ Retina scan devices are probably the most accurate biometric available today.
- ▶ Retinal pattern changes very rarely, only from degenerative diseases, in case the person dies it deteriorates very quickly

Retinal Scan: Disadvantages

- ▶ Expensive
- ▶ Difficult to use
- ▶ Requires participant cooperation
- ▶ Psychological factor: consumer's thinking it is potentially harmful to the eye

Attacks on Biometrics-Based Systems

- ▶ Villain gives policeman fingerprinted fingers in the wrong order...
- ▶ Forensic biometrics: information can be planted, or not fresh; freshness is a critical aspect.
- ▶ Recordings attacks: on voice recognition systems, imprinted lens to fool iris scanners
- ▶ Collusions: handwriting systems, by giving childish samples, they can force the machine to accept a lower threshold than usual.
- ▶ Biometrics are not as accurate for all people. Biometrics referred to these people as goats.
- ▶ Political and religious issues