Biometric System Security
and
Policy Implications

Biometrics
CSE 190-a
Lecture 19

Outline

1. Serge's Video
2. Biometrics System Security
3. Policy

Computer Vision: Fact and Fiction
Biometrics

Video by
Serge Belongie et al

Biometrics System Security Outline

- **Attacks against Biometric Systems**
  - Taxonomy of Attacks
  - Attack Examples
- **Solutions to Attacks**
  - Liveness Detection
  - Challenge/Response
  - Watermarking

Types of Threats

Six major types of threats

- Circumvention: An attacker gains access to the system protected by biometric authentication
  - Privacy attack: Attacker accesses the data that she was not authorized (e.g., accessing the medical records of another user)
  - Subversive attack: Attacker manipulates the system (e.g., submitting bogus insurance claims)
- Repudiation: An attacker denies accessing the system
  - A bank clerk modifies the financial records and later claims that her biometric data was stolen and denies that she is responsible
- Contamination (covert acquisition): An attacker illegally obtains biometric data of genuine users and uses it to access the system
  - Lifting a latent fingerprint and constructing a synthetic finger

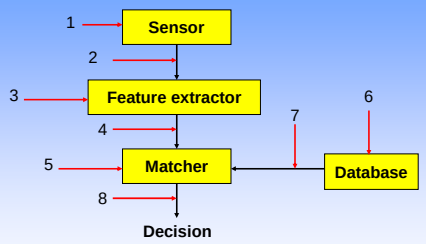
Maltoni et al. 2003 & Uludag, Jain 2004 (1)

Types of Threats

- Collusion: A user with wide super user privileges (e.g., system administrator) illegally modifies the system
- Coercion: An attacker forces a legitimate user to access the system (e.g., using a fingerprint to access ATM at a gunpoint)
- Denial of Service (DoS): An attacker corrupts the biometric system so that legitimate users cannot use it
  - A server that processes access requests can be bombarded with many bogus access requests, to the point where the server's computational resources can not handle valid requests any more.

Maltoni et al. 2003 & Uludag, Jain 2004 (1)

Attacks Against Biometric Systems



Points of attack for a generic biometric system

Adapted from *Ratha et al. 2001 (1)*

Attacks Against Biometric Systems

- Attack 1: A fake biometric (e.g., an artificial finger) is presented at the sensor
- Attack 2: Illegally intercepted data is resubmitted (replay)
- Attack 3: Feature detector is replaced by a Trojan horse program
  - It produces feature sets chosen by the attacker
- Attack 4: Legitimate features are replaced with a synthetic feature set
- Attack 5: Matcher is replaced by a Trojan horse program
  - It produces scores chosen by the attacker
- Attack 6: Templates in the database are modified, removed, or new templates are added
- Attack 7: The transferred template information is altered in the communication channel
- Attack 8: The matching result (e.g., accept/reject) is overridden

Attack Examples

Attack 1: Synthetic Biometric Submission

- No detailed system knowledge or access privileges is necessary
- Digital protection mechanisms (e.g., encryption) are not applicable

Putte, Keuning 2000:

- 6 fingerprint verification systems attacked
- 5 out of 6 accepted the dummy finger in the first attempt

Dummy finger created with cooperation of the user in a few hours with liquid silicon rubber

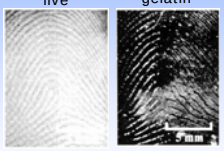
Dummy finger created from a lifted impression of the finger without cooperation of the user in eight hours with silicon cement

Attack 1: Synthetic Biometric Submission

Matsumoto et al. 2002:

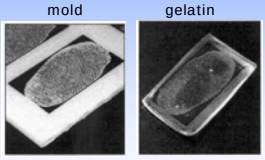
- 11 fingerprint verification systems attacked with artificial gelatin fingerprints
- Gelatin fingers accepted with a probability of 67-100%

live gelatin



With cooperation (finger pressed to plastic mold)

mold gelatin



Without cooperation (residual fingerprint lifted from a glass)

Attack 1: Dislocated Biometric Submission

Malaysia car thieves steal finger, by Jonathan Kent, BBC News

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system. Accountant K. Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb. The gang, armed with long machetes, demanded the keys to his car. It is worth around $75,000 second-hand on the local market, where prices are high because of import duties.

The attackers forced Mr. Kumaran to put his finger on the security panel to start the vehicle, bundled him into the back seat and drove off. But having stripped the car, the thieves became frustrated when they wanted to restart it. They found they again could not bypass the immobiliser, which needs the owner's fingerprint to disarm it. They stripped Mr. Kumaran naked and left him by the side of the road - but not before cutting off the end of his index finger with a machete.

Police believe the gang is responsible for a series of thefts in the area.

http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

Attack 2: Bypass Sensor

Soutar 2002:

- Hill-climbing attack for a simple image recognition system
  - Matching: Template images create correlation filters, these filters are then used with input images.
  - Attack: Synthetic images are input to the system:
    - At each iteration, randomly alter the gray level (8 bits) of 64 pixels: if matching score improves, keep the new image
    - Continue till the system is compromised

Unknown template image

Initial input image

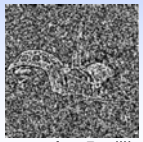
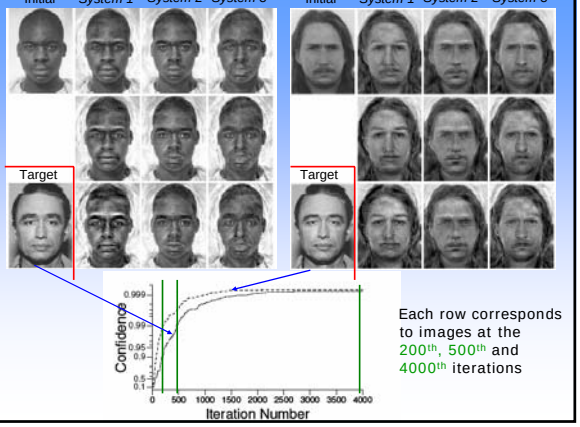


Image after 7 million iterations

Attack 2: Bypass Sensor

Adler 2003:

- Hill-climbing attack for three well known commercial face recognition systems
  - Attack:
    - Select an initial image from a local database, based on the highest matching score
    - At each iteration, successively add an eigenface multiplied with 6 constants (-3c, -2c, -c, c, 2c, 3c) to the current synthetic image: keep the change that results in the best matching score improvement
    - Crop the gray scale values if they are outside the image capacity (8 bit → 0-255 values are allowed)
    - Continue till the system is compromised



Each row corresponds to images at the 200th, 500th and 4000th iterations

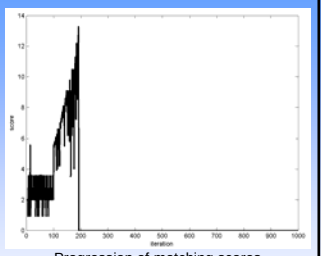
Hill climbing for Fingerprints

Experimental Results

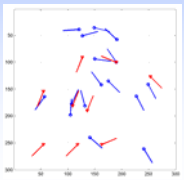
- FAR=0.1% implies that, on the average, 1 in 1,000 imposter attempts will be accepted as a genuine match
- Attacker broke all the 160 user accounts with much fewer than 1,000 attempts/account
- The minimum, mean, and the maximum number of required attempts are: 128, 195, and 488, respectively
- The minimum, mean, and the maximum number of minutiae in the templates that broke the accounts are: 10, 14.2, and 21
- The minimum, mean and the maximum number of matching minutiae between the original template and the templates that broke the accounts are: 5, 6.8, and 10

Sample Account: account# 11

Original image with minutiae



Progression of matching scores



Synthetic (∀) and original (o) minutiae

Account broken at iteration# 192: original template has 16 minutia; synthetic template has 10 minutia; 5 minutiae match; final matching score: 13.3.

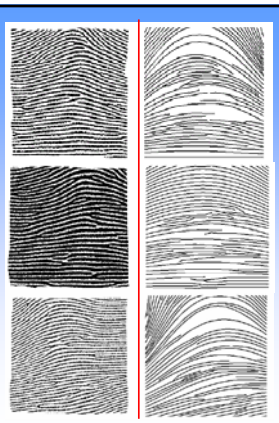
Attacks 6 & 7: Generate Biometric from Template Data

Hill 2001:

- Synthetic images generated from reverse engineered minutiae template data from a commercial (undisclosed) fingerprint authentication system:
  - Author accessed unencrypted template data from a computer hard drive
  - The format of the accessed template discovered by trial/error and by introducing controlled changes in input images. For each minutiae, its 2D location, angle and ridge curvature was found
  - Orientation field of the target image estimated based on core and delta point locations.
  - Lines starting at minutiae points are drawn, by taking into account the orientation field
  - Synthetic images are not very realistic, but still they were accepted as genuine template images

Hill 2001:

Target images



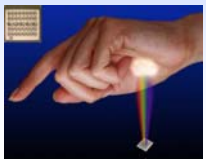
Synthetic images

Solutions to Attacks

Solution to Attack 1: Fingerprint Liveness Detection

- Hardware-based systems:
  - Temperature: The temperature of the epidermis is about 8-10 ^{0}C above the room temperature
  - Conductivity: Typical skin conductivity is nearly 200 kOhm.
  - Dielectric constant: Relative Dielectric Constant of human skin (in the range 20-50) is different from that of silicon
  - Heart Beat: Can be used against fingers from cadavers

Lumidigm: Analyzes signals that are backscattered from skin layers when illuminated with multiple wavelengths of visible and near-infrared light



Solution to Attack 1: Fingerprint Liveness Detection

Derakhshani et al. 2003:

- Software-based system
- Static (periodicity of sweat pores along the ridges) and dynamic (sweat diffusion pattern along the ridges over time) features are used for liveness detection
- Input to liveness detection module is 5 sec. video of the finger
- Live fingers, fingers from cadavers, and dummy fingers made up of play dough are used in the experiments
- Neural network is trained for classification:
  - Static method leads to an Equal Error Rate (EER) of nearly 10%; dynamic methods lead to EER of 11-39%
    - False accept: cadaver/dummy finger classified as live
    - False reject: live finger classified as cadaver/dummy

Solution to Attack 2: Eliminate Replay

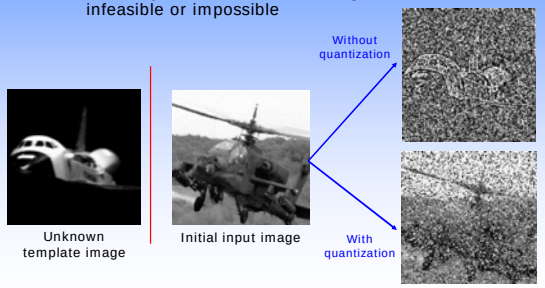
Ratha et al. 2001 (1):

- A challenge-response based system guarantees that image is really coming from the fingerprint sensor (i.e., the attacker has not bypassed the sensor):
  - Server generates a pseudo-random challenge after transaction gets initiated by the client
  - Secure server sends the challenge to intelligent sensor
  - The sensor acquires the fingerprint image and computes the response to the challenge
  - The challenge can be the checksum of a segment of the image, a set of samples from the image, etc.
  - The response and the sensed image are sent to the server
- The validity of response/image pair is checked

Solution to Attacks 2 & 4: Eliminate Hill-Climbing

Soutar 2002:

- Do not reveal the actual matching scores; only reveal a coarsely quantized version:
  - This may render the hill-climbing based attack infeasible or impossible



Soln. to Attacks 6 & 7: Protect Templates via Cancelable Biometrics

Ratha et al. 2001 (2):

- Apply repeatable (but noninvertible) distortions to the biometric signal or the feature vector:
  - If a specific representation of biometric template is compromised, replace that distortion with another one from a distortion database.
  - Every application can use different distortions (e.g., health care, visa) so the privacy concerns related to database sharing between institutions can be addressed

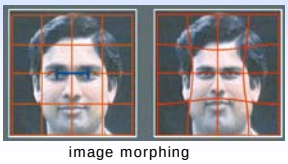


image morphing

block scrambling

Solutions to Attacks 6 & 7: Watermarking Templates

Digital Watermarking:

- Embed extra information (e.g., origin, access level, destination) into the host data itself.
- Applications: Copyright protection, authentication, data monitoring, transmission of value-added services …

Traditional Watermarking:

Paper watermark and mold used to generate the watermark

Digital Watermarking in Biometrics

Yeung, Pankanti 1999:

- Use fragile watermarking (if the image is altered, watermark is changed) of fingerprint images to verify integrity:
  - The decoded mark can indicate image alteration after it has been marked by an authorized agent (i.e., a secure sensor)
- Watermark insertion: Merge input image I(i,j) with a watermark image W(i,j) to produce the watermarked image I'(i,j):
  - Each pixel is input to a watermark extraction WX() function to yield extracted watermark value b(i,j). If b(i,j) is equal to W(i,j), the processing moves to the next source pixel. If not, the value of pixel at (i,j) is modified until they are equal.
- Watermark extraction: Apply WX() to the watermarked image I'(i,j) to produce output watermark image b'(i,j).
  - The tampering of the watermarked image leads to distortions in the decoded watermark image.

Soln. to Attacks 6 & 7: Protect Templates via Watermarking

Jain, Uludag 2003:

- Embed eigen-face coefficients into the fingerprint images:
  - Depicted face is associated with the host fingerprint image
  - Based on amplitude modulation in spatial domain:
    - Modify the host pixels by also considering watermark visibility and fingerprint matching performance
  - If the watermarked fingerprint image is stolen, it is useless since face matching with the extracted face watermark is needed

References

- *Ratha et al. 2001 (1)*: N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", *Proc. AVBPA 2001*, pp. 223-228.
- *Maltoni et al. 2003*: D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.
- *Uludag, Jain 2004 (1)*: U. Uludag and A.K. Jain, "Attacks on biometric systems: a case study in fingerprints", *Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI*, vol. 5306, pp. 622-633.
- *Putte, Keuning 2000*: T. Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned", *Proc. IFIP TC8/WG8.8, Fourth Working Conf. Smart Card Research and Adv. App.*, pp. 289-303, 2000.
- *Matsumoto et al. 2002*: T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems", *Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, pp. 275-289, 2002.
- *Soutar 2002:* C. Soutar, "Biometric system security", http://www.bioscrypt.com/assets/security_soutar.pdf
- *Adler 2003*: A. Adler, "Sample images can be independently restored from face recognition templates", http://www.site.uottawa.ca/~adler/publications/2003/adler-2003-fr-templates.pdf

References

- *Uludag, Jain 2004 (2)*: U. Uludag and A.K. Jain, "Fingerprint Minutiae Attack System", *The Biometric Consortium Conference*, Virginia, September 2004.
- *Hill 2001:* C.J. Hill, "Risk of masquerade arising from the storage of biometrics", B.S. Thesis, http://chris.fornax.net/biometrics.html
- *Ross et al. 2005*: A. Ross, J. Shah, A. Jain, "Towards Reconstructing Fingerprints From Minutiae Points", *Submitted to SPIE Biometrics Conference*, 2005.
- *Derakhshani et al. 2003*: R. Derakhshani, S.A.C. Schuckers, L.A. Hornak, and L.O. Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners", *Pattern Recognition*, vol. 36, pp. 383-396, 2003.
- *Ratha et al. 2001 (2):* N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, 2001.
- *Yeung, Pankanti 1999*: M.M. Yeung and S. Pankanti, "Verification watermarks on fingerprint recognition and retrieval," *Proc. SPIE EI 1999*, vol. 3657, pp. 66-78.
- *Jain, Uludag 2003*: A. K. Jain and U. Uludag, "Hiding biometric data", *IEEE Trans. PAMI*, vol. 25, no. 11, pp. 1494-1498, November 2003.

Policy References

- "Biometrics at the Frontiers: Assessing the Impact on Society", Report for the European Parliament
  Committee on Citizens' Freedoms and Rights,
  Justice and Home Affairs (LIBE)
  http://www.europeanbiometrics.info/images/resources/21_936_file.pdf
- A. Alterman``A piece of yourself": Ethical issues in biometric identification,"Ethics and Information Technology, 5(3) 2003, 139-150
  http://www.springerlink.com/content/1572-8439/
- K. Bowyer, "Face Recognition Technology: Secruity vs. Privacy," IEEE Technology and Society Magazine, Spring 2004, pp. 9-20.
- R. Rosenzweig, A. Kochems, A. Schwartz, "Biometric Technologies, Secruity, Legal, and Policy Implications. Heritage Foundation Legal Memorandum
- ACLU Opposes Use of Face Recognition Software in Airports Due to Ineffectiveness and Privacy Concerns
  http://www.aclu.org/privacy/spying/14875res20030902.html
  http://www.aclu.org/privacy/gen/15100res20020221.html

Some issues (1)

To make rational policy decisions, one must really understanding the technology, limitations, benefits, tradeoffs.

- Biometric X is the "best" for all applications
- Biometric X is unique for each individual
- A single number quantifies system accuracy
- Our system is "plug and play"
- Real accuracy performance can be predicted.
- The vendor reporting best FAR and FRR has the most "accurate system"
- Our biometric system does not use a decision threshold.
- Our feature extractor can be used with any match engine

Some issues (2)

- Large templates mean better accuracy
- Biometric sensors are unhygienic or otherwise harmful
- Face recognition prevents terrorism
- Biometrics means 100% security
- Biometrics systems are no threat to our privacy
- Biometric systems invade our privacy

Security versus Privacy

"They that can give up essential liberty to obtain a little temporary safety deserve neither liberty or safety."

- Benjamin Franklin

Fourth Amendment

- *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

John Woodward's analysis

- "Under current law, however, the type of facial recognition used at the Super Bowl would almost certainly be constitutional. The Supreme Court has explained that government action constitutes a search when it invades person's reasonable expectation or privacy. But the court has also found that a person does not have a rasonable expectation of privacy with regard to physical characteristics that are constantly exposed to the public, such as one's facial features, voice, and handwriting."

Palm Beach Airport

- A face recognition system installed in Palm Beach Airport in 2002
- 10,000 Face images per day of about 5,000 people
- 250 people in database, 15 were airport employees
- 958 images contained people in database
- 455 successful matches
  - False alarm rate: 0.4%, or 2-3 per hour
  - 47% Succes rate

Was face rec useful?

Some Pros

- 50% detection rate can be a significant deterrent
- Crime rate in London dropped 20-40% in places where it was announced that surveillance cameras with face were installed.
- 2-3 False alarms are managable

Cons

- 0.4% false alarm vs. news arrticle reporting 1,000 false alarms over four weeks of testing.
- "Face recognition is a disaster" ACLU Rep

Super Bowl XXXV

- A face recognition system was deployed at the Superbowl and scanned all 100,000 attendees.
- About 20 people were identified as being on a "watch list."

Media Reports / Opinions

"A computer glitch could match the face of an innocent person with the digital image of a criminal."

"Super bowl snooping," *NY Times*, Feb 4, 2001.

Is it really a "glitch?"
Or an unavoidable "feature?"

Media Reports / Opinions

On the system used at Super Bowl – "The beauty of the system is that it is disguise-proof. You can grow a beard and put on sunglasses, and FaceTrac will still pick you out of a crowd."

Lev Grossman, "Welcome to the snooper bowl," *Time*, Feb 12, 2001.

Media Reports / Opinions

"A woman in Texas who saw the image claimed the man in the picture was wanted for crimes. She called the Tampa police, who questioned the man, a construction worker. It was the wrong person ...
The system … is not 100 percent accurate."

"Electronic surveillance: From `Big Brother' Fears to Safety Tool," *NY Times*, Dec 6, 2001.

Media Reports / Opinions

Congressman Ed Markey (D., Mass.) –
"It's chilling, the notion that 100,000 people were subject to video surveillance and had their identities checked by the government."

Lev Grossman, "Welcome to the snooper bowl," *Time*, Feb 12, 2001.

Media Reports / Opinions

An ACLU representative –
"We do not believe that the public understands or accepts that they will be subjected to a computerized police lineup as a condition of admission."

D. McCullagh, "Call It Super Bowl Face Scan I," www.wired.com, Feb 2, 2001.

Media Reports / Opinions

A news report –
"Police are enthusiastic about the system, saying it is no different from an officer standing on a street corner with a criminal's photograph in hand and checking out a passing crowd."

J. Cienski, "Police cameras denounced as threat to privacy," www.nationalpost.com, July 12, 2001.

Ethical Issues

Ethical issues arise in (at least)

- **Protection of privacy.**
- **Performance claims.**
- **Public understanding.**

Code of Principles
"Heritage Foundation Report"

- Enrollment in biometric systems should be overt instead of covert
- Biometric systems are better used for verification than identification
- Biometric systems should be designed to operate with local storage of data
- Prefer biometric systems that are "opt in" and require consent.
- Prefer biometric systems that reduce the biometric to a template, rather than maintaining a stored image
- Any biometric system should have strong audit oversight programs to prevent misuse
- Any biometric system is only as strong as the initial enrollment system
- A biometric system is only as strong as its back-up alternative