Biometric System Security

Anil K. Jain

Dept. of Computer Science and Engineering

Michigan State University

http://biometrics.cse.msu.edu

Identity Questions

- Should this person be granted a visa?
- Has this person already been issued a driver license?
- Is this person authorized to access the information?
- Is the person withdrawing money from the ATM machine really the account holder?

How Do I know Who You Are?

Current Methods based on credentials (passwords and ID) are not adequate

The nineteen 9/11 hijackers had a total of 63 valid driver licenses

~5 million identity thefts in U.S. in 2004

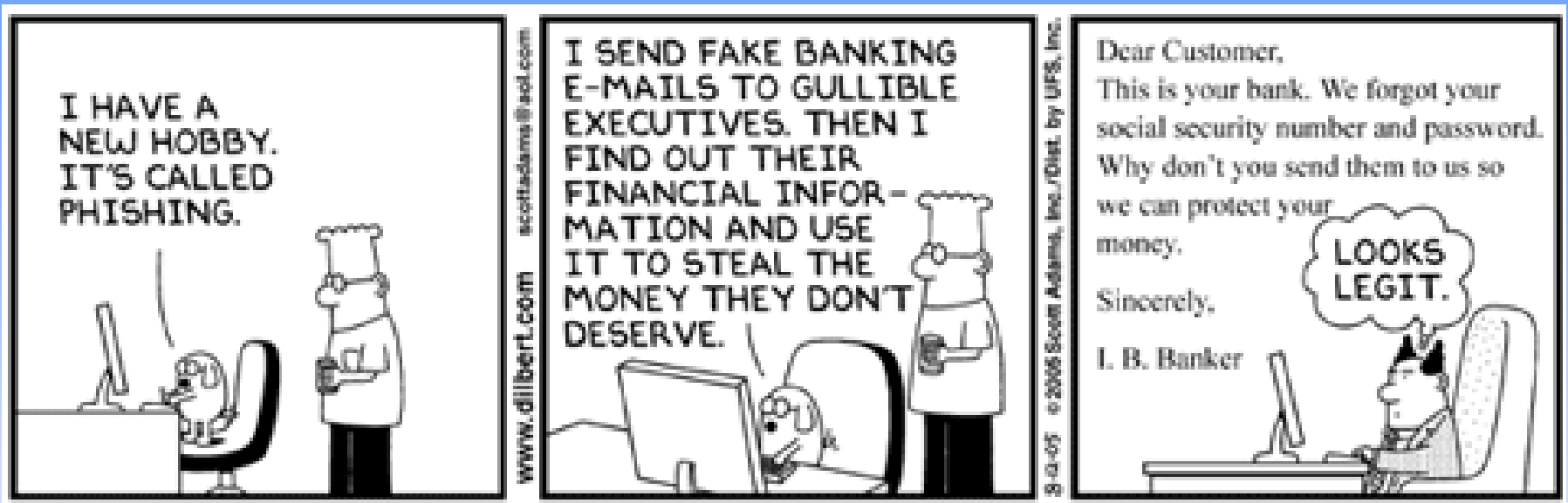
6.7 million victims of credit card fraud

People do not protect their credentials

Too Many Passwords!

• Heavy web users have an **average of 21 passwords**; 81% of users select a common password and 30% write their passwords down or store them in a file. *(2002 NTA Monitor Password Survey)*

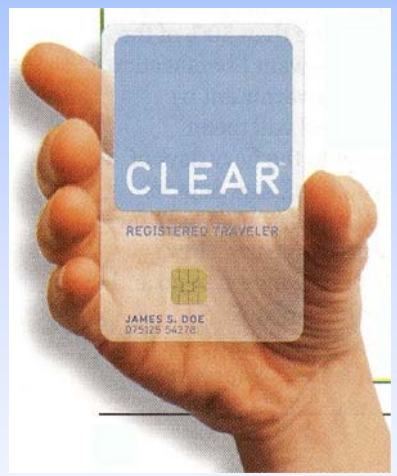
Phishing



"A recent survey found 70% of those asked said that they would reveal their computer passwords for a bar of chocolate. Sweet!" (Technology Review, March 2005, p. 78)

Biometric Recognition

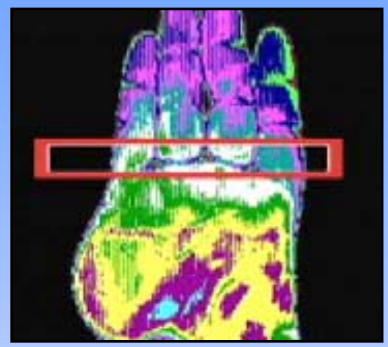
Personal recognition based on "who you are" as opposed to/in conjunction with "what you know" (PIN) or "what you have" (ID card)

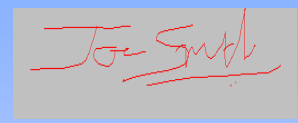


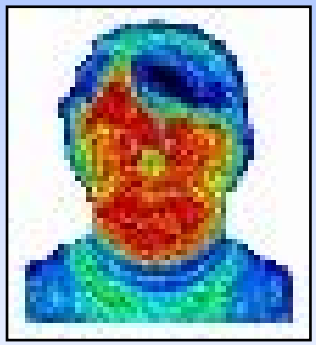
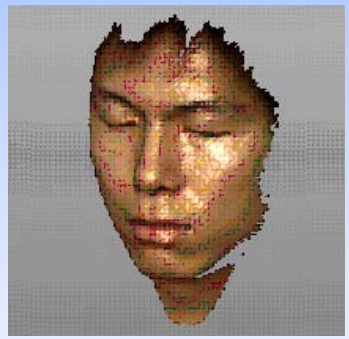
Recognition of a person by his body, then linking that body to an externally established "identity", forms a very powerful tool for identity management

Biometric Traits

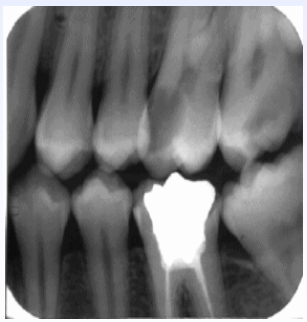


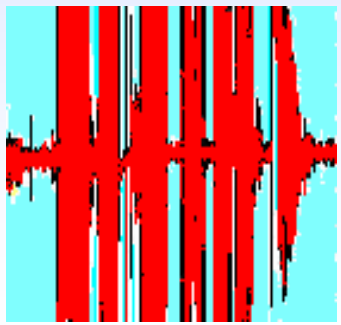
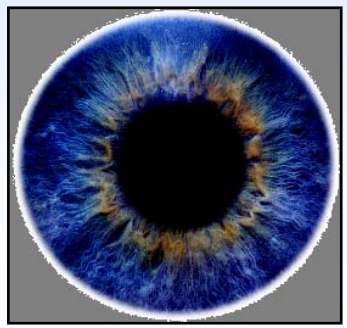
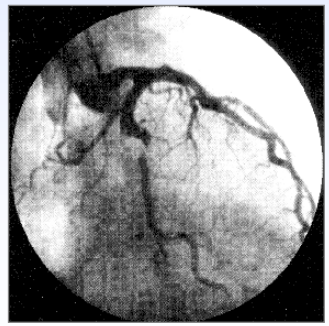








Applications

Goal: Automatic & reliable person identification in unattended mode, often remotely

Iris matching: Heathrow Airport

US-VISIT Program

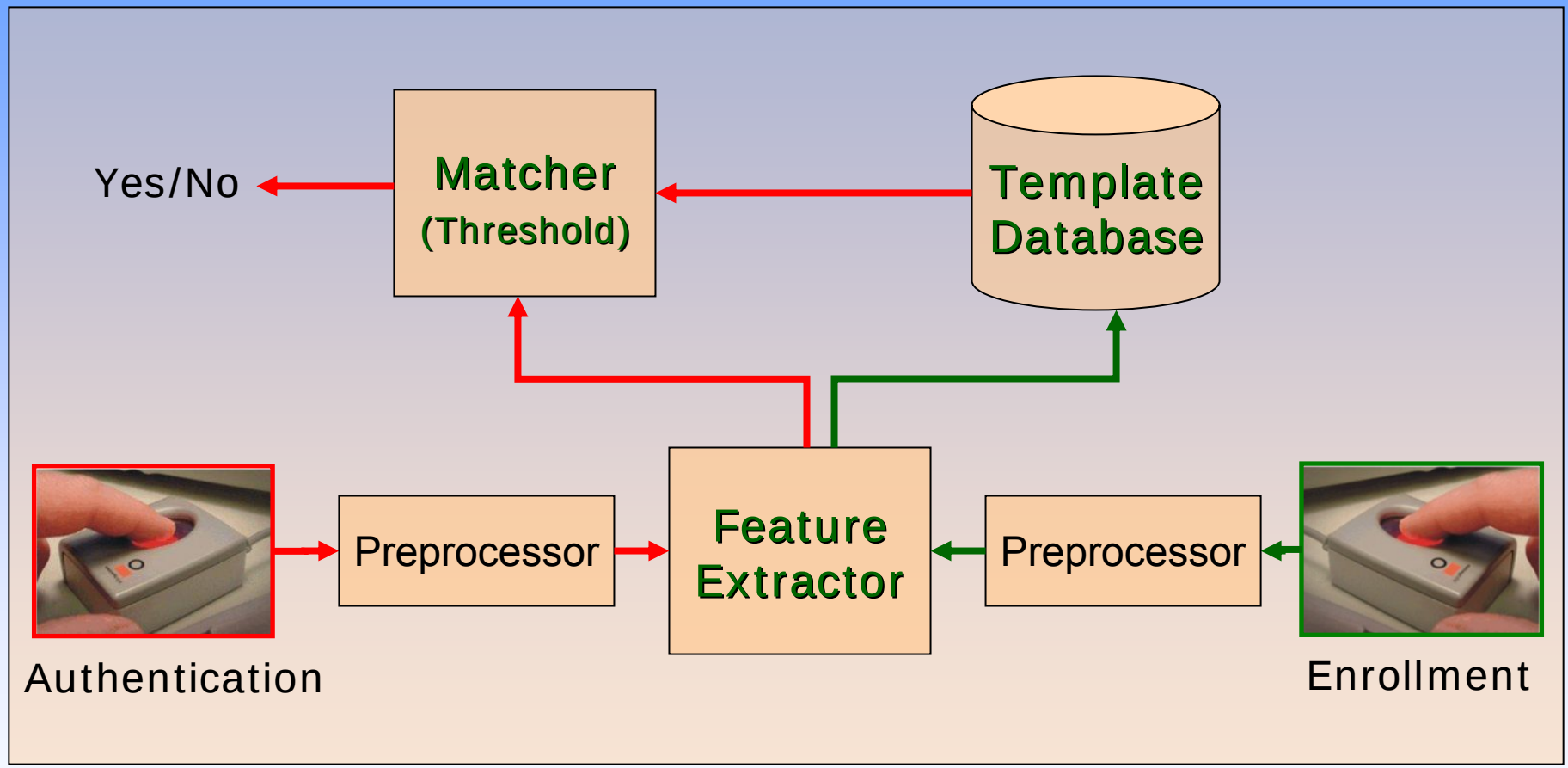
Cellular phone: Siemens

Grocery store payment: Indivos

Automobile: Audi A8

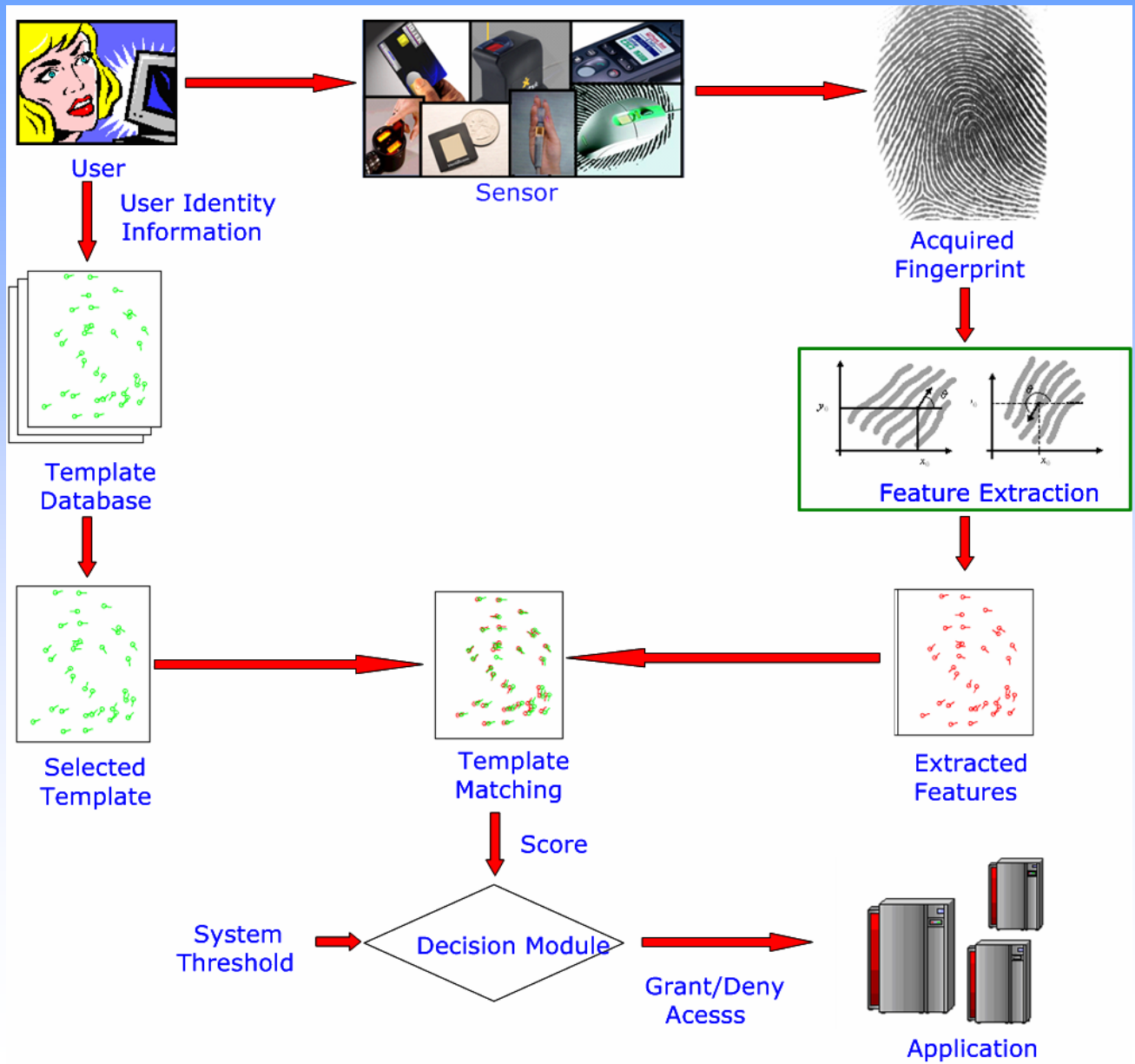
Disney World

Biometric Recognition System



- False accept rate (FAR): Proportion of imposters accepted
- False reject rate (FRR): Proportion of genuine users rejected
- Failure to enroll rate (FTE): portion of population that cannot be enrolled
- Failure to acquire rate (FTA): portion of population that cannot be verified

Fingerprint System



Challenges

- Accuracy
- Cost
- Speed
- Ease of Use
- Failure to Enroll
- Robustness
- Security
- Privacy

} Return on investment

"State-of-the-art" Error Rates

	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2004]	20 years (average age)	2%	2%
	FpVTE [2003]	US govt. ops. Data	0.1%	1%
Face	FRVT [2002]	Varied lighting, outdoor/indoor	10%	1%
Voice	NIST [2004]	Text independent, multi-lingual	5-10%	2-5%

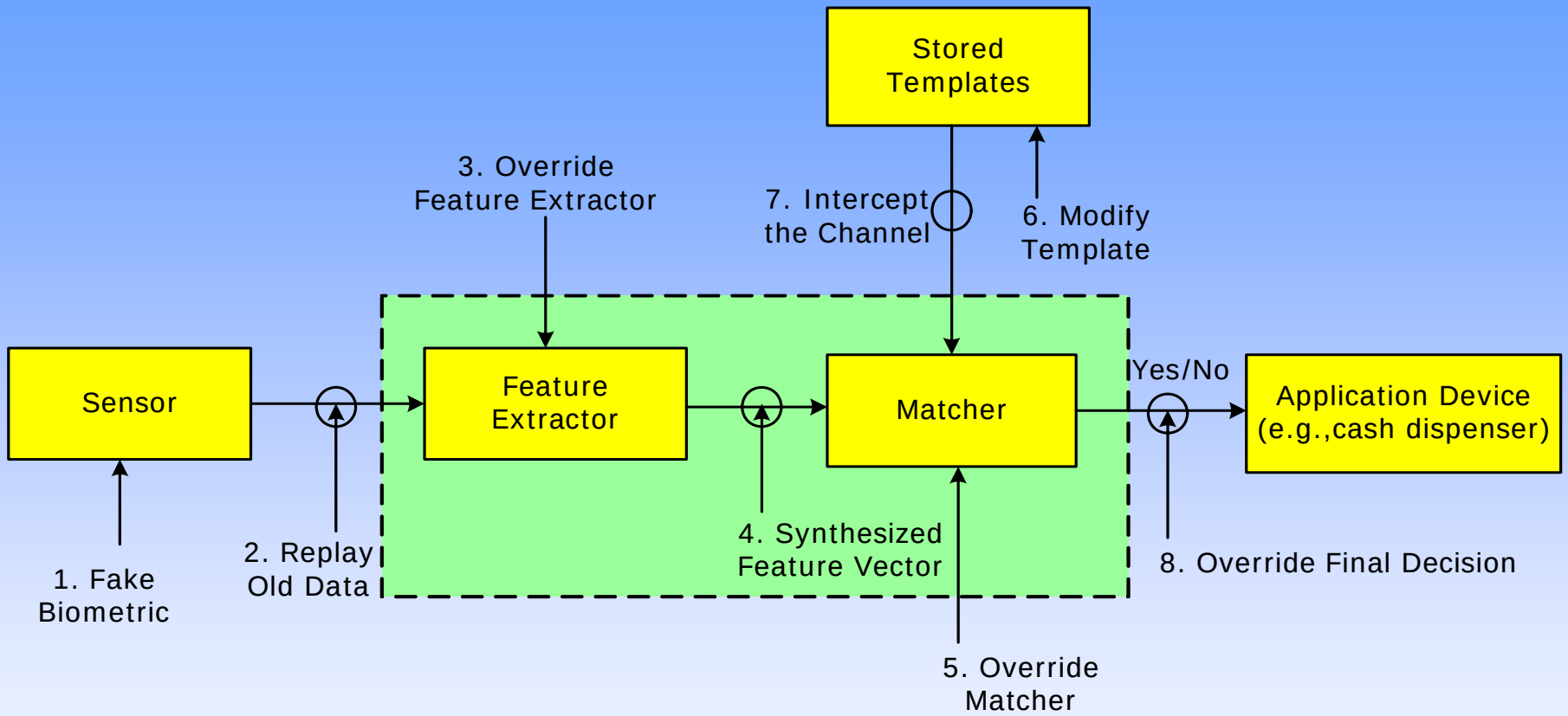
At NY airports, an average of ~ 200,000 passengers pass through daily. There would be 4,000 falsely rejected (and inconvenienced) passengers per day for fingerprints, 20,000 for face and 30,000 for voice. Similar numbers can be computed for false accepts

Biometric System Security

- Number of installed biometric systems in both commercial and government sectors is increasing
- Size of the population that uses some of these systems is extremely large (US VISIT program)
- New emerging applications in laptops, mobile phones, e-commerce, health care records,….

- What happens if the biometric system fails to recognize you or recognizes you as someone else?
- The potential damage resulting from security breaches in biometric systems can be enormous!

Biometric System Attacks



Type 1: A fake biometric is presented at the sensor; Type 2: Illegally intercepted data is resubmitted (replay); Type 3: Feature detector is replaced by a Trojan horse program; Type 4: Legitimate features are replaced with synthetic features; Type 5: Matcher is replaced by a Trojan horse program; Type 6: Templates in the database are modified; Type 7: Template is intercepted & altered in the channel; Type 8: Matching result (e.g., accept/reject) is overridden

Attack at the Sensor Level

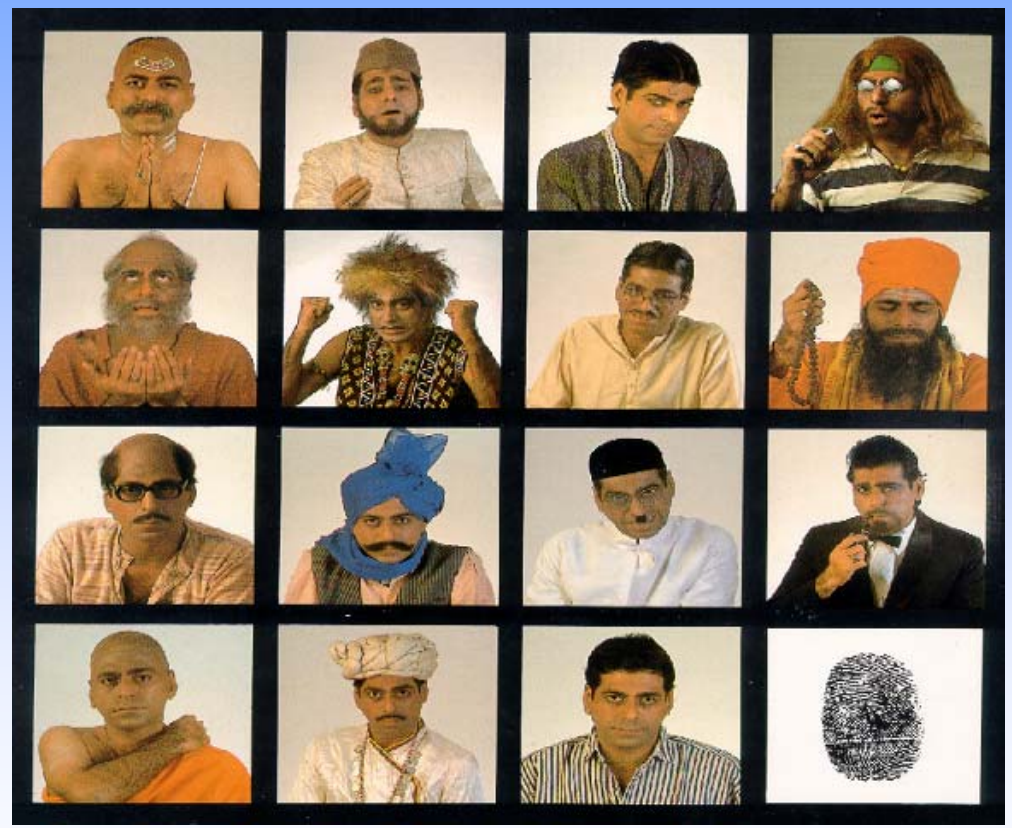
- Coercion
- Camouflage
- Synthetic biometric with/without user's cooperation

"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."

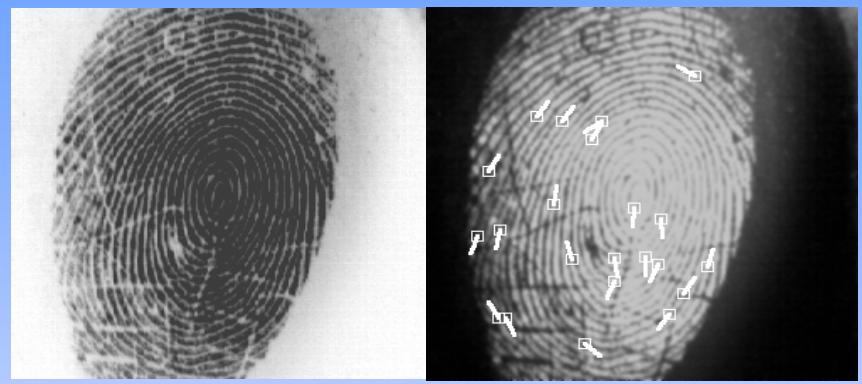
BBC News, 31 March, 2005

Camouflage

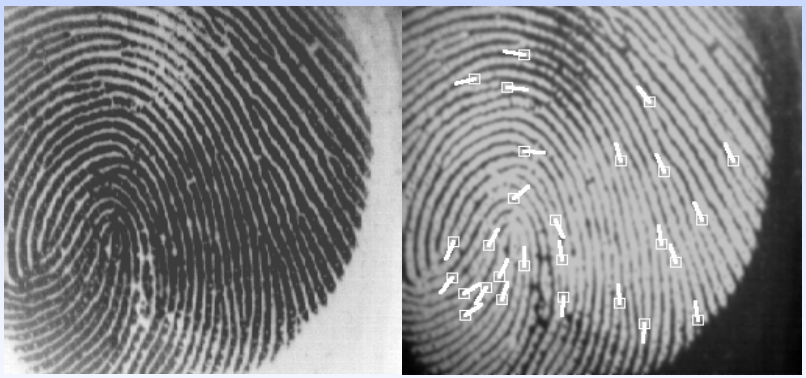

In response to the new TIA's Gait Identification Program, Americans take action to protect their Privacy
ANTONELLIS
5/22/03 ©2003 Tribune Media Services, Inc. All rights reserved ATelnaes@AOL.COM

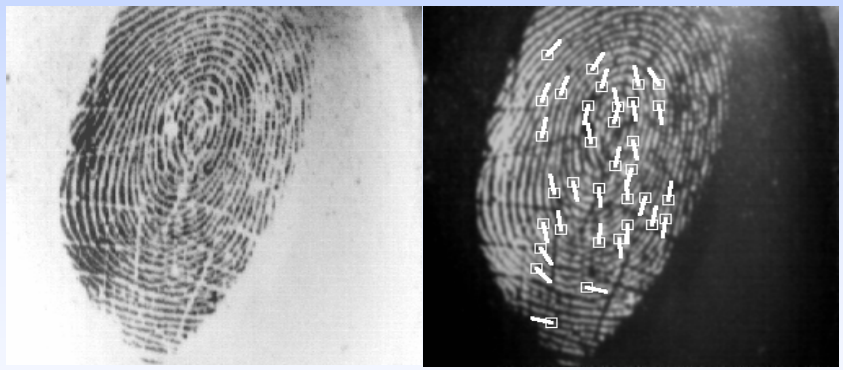


Fake Fingerprints



Live finger

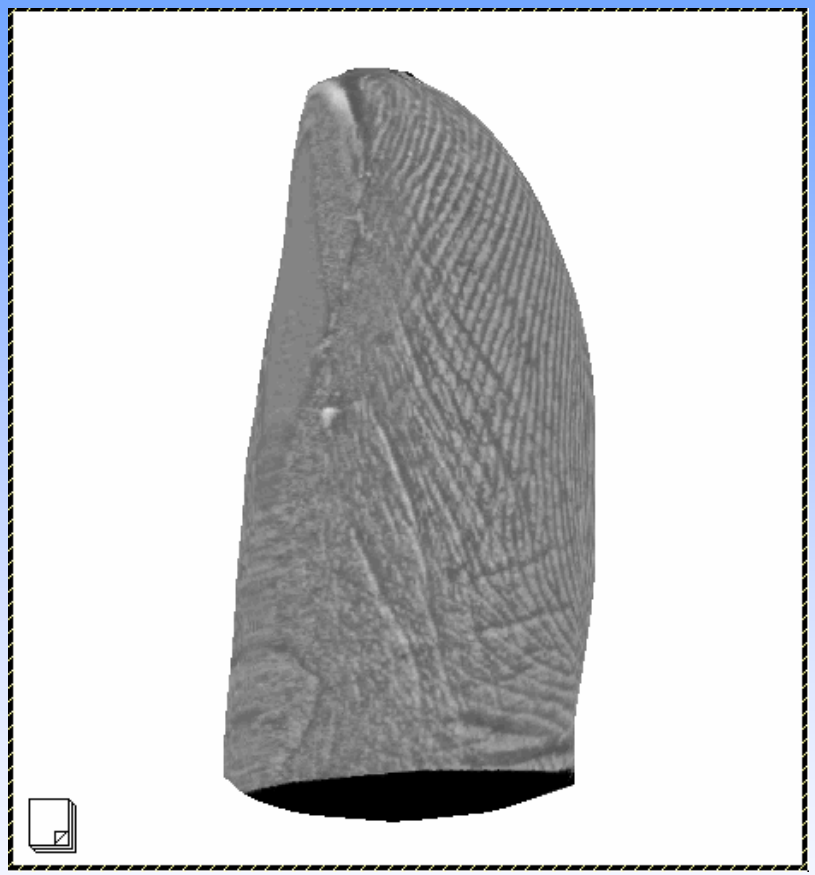




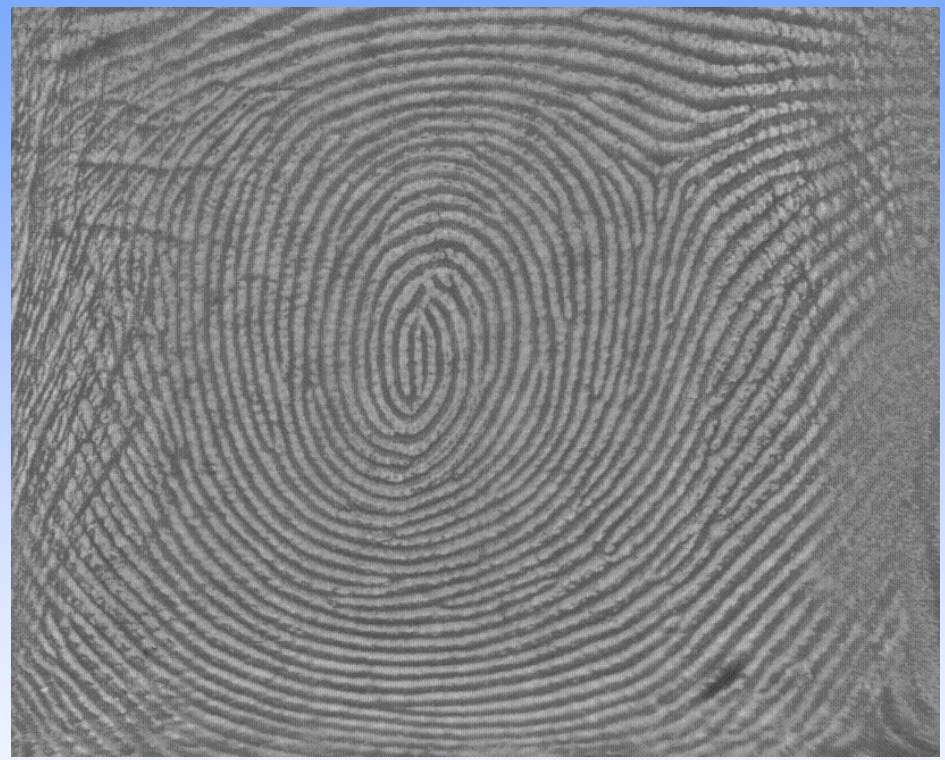
Gummy finger

Access was granted 75% of the time using gummy fingers

Touchless Sensors



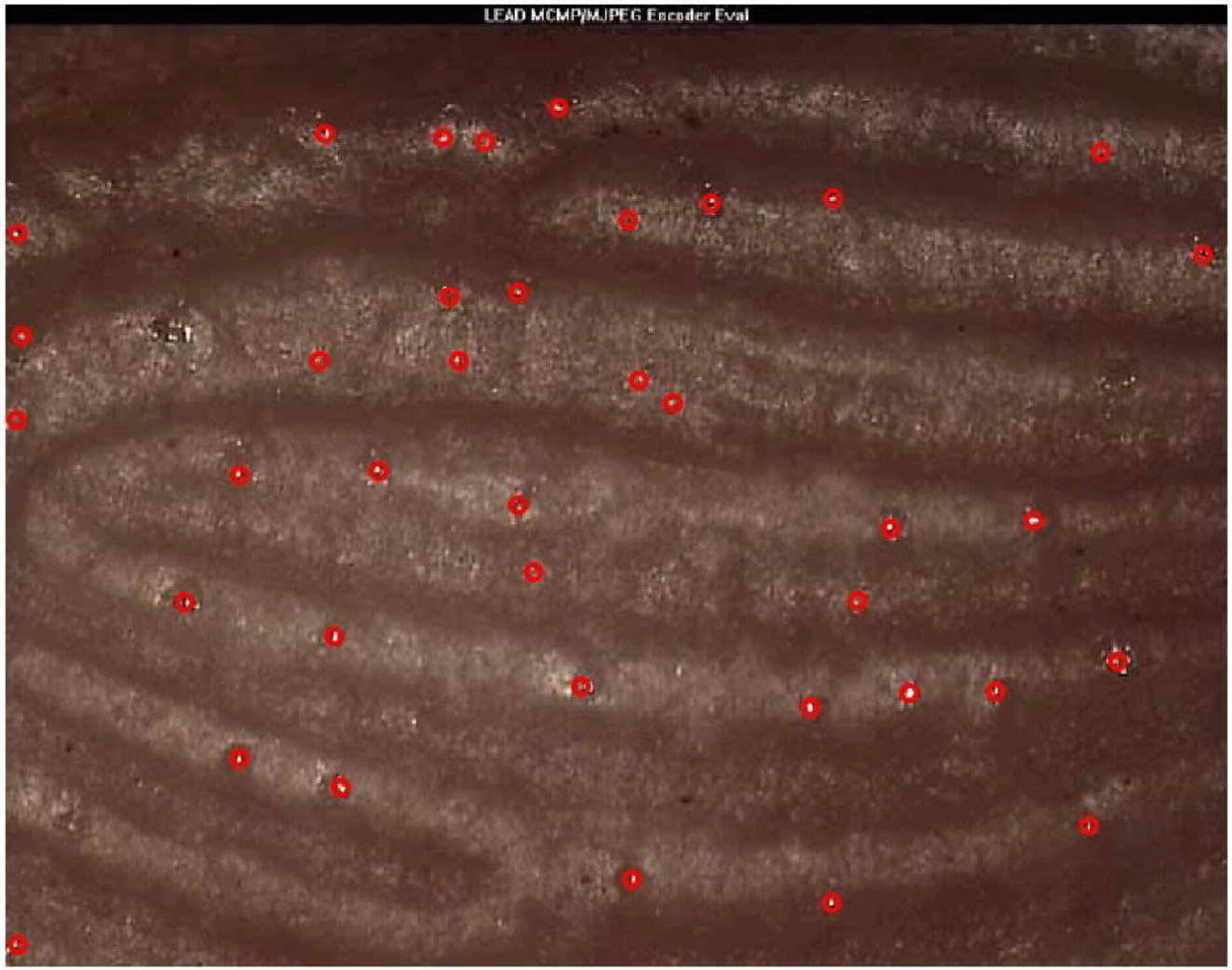
Touchless 3D image



Touchless “rolled” image

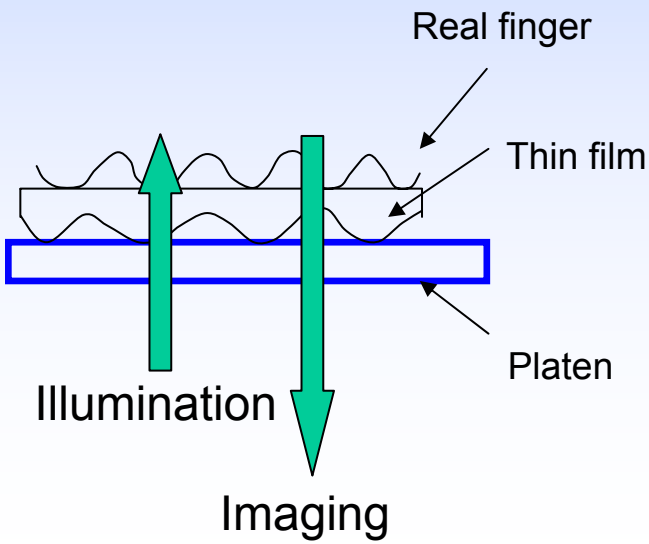
Courtesy: TBS North America, Inc.

High Resolution Sensors

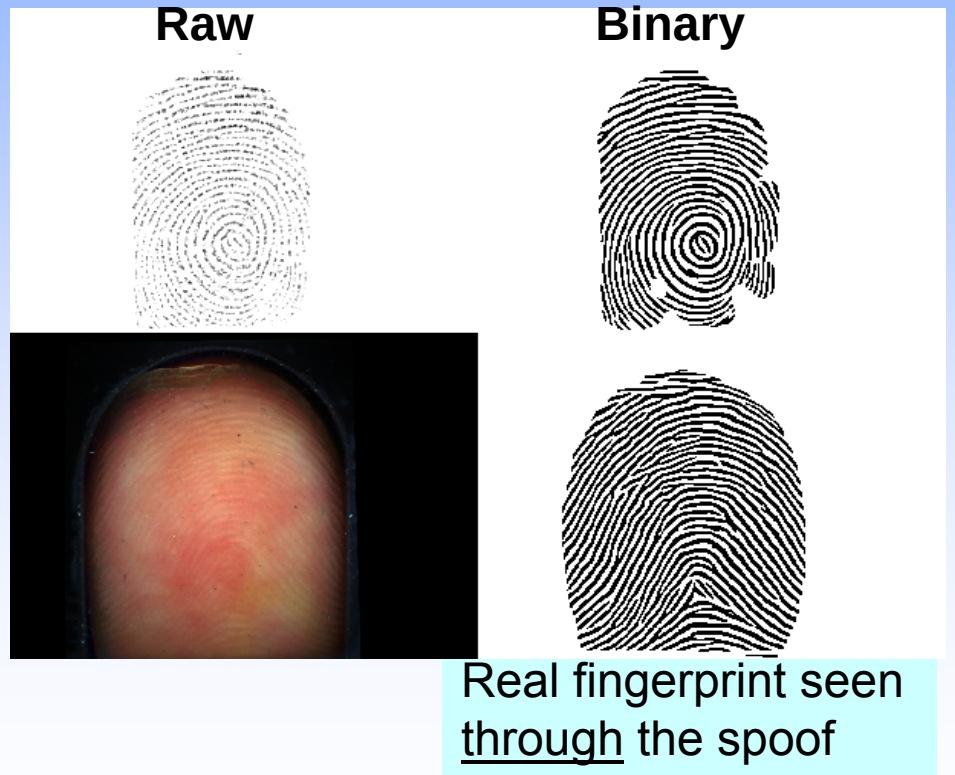


Spoof Detection With Multispectral Imaging

If a very thin latex membrane is placed over a real finger, optical readers only image surface topography but MSI can see through the membrane to image underlying fingerprint features.



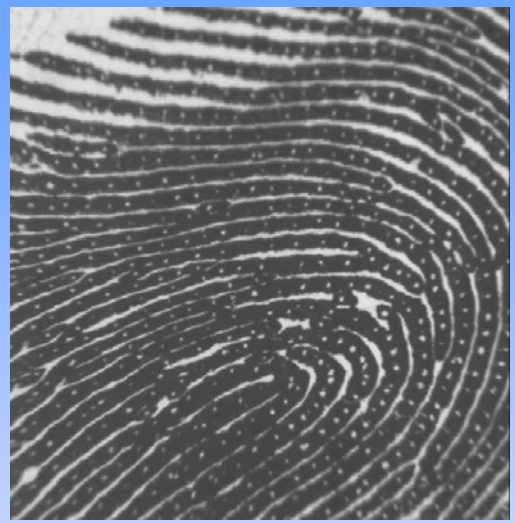
Lumidigm

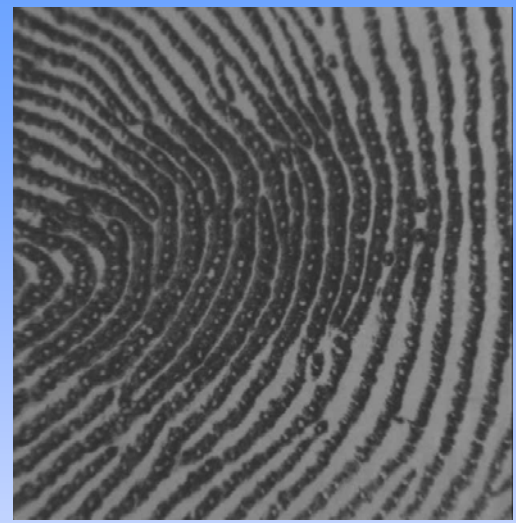


Real fingerprint seen through the spoof

Deformation-Based Spoof Detection

Live finger





http://www.cim.mcgill.ca/~vleves/homepage/

Gummy finger

Chen, Jain & Dass, “Fingerprint deformation for Spoof detection” Proc. Biometrics Research Symposium, Crystal City, Sept 2005

TPS: Estimating Deformation

Assume that (i) enrollment image is from a live finger and (ii) image quality is good for minutiae extraction and correspondence

- Source $U=\{u_1, u_2,\ldots u_n\}$, $u_i = (u_{xi}, u_{yi})$
- Target $V=\{v_1, v_2,\ldots v_n\}$, $v_i = (v_{xi}, v_{yi})$
- Deformation*

$$F(u_i) = \underbrace{c + Au_i}_{\text{Affine}} + \underbrace{W^T s(u_i)}_{\text{Non-Affine}} = v_i$$

Size of W: n x 2
Depends on the number of correspondences

Distance Vector:

$$s(u_i) = (\sigma(u_i - u_1), \sigma(u_i - u_2), \ldots, \sigma(u_i - u_n))^T$$

Radial Basis function:

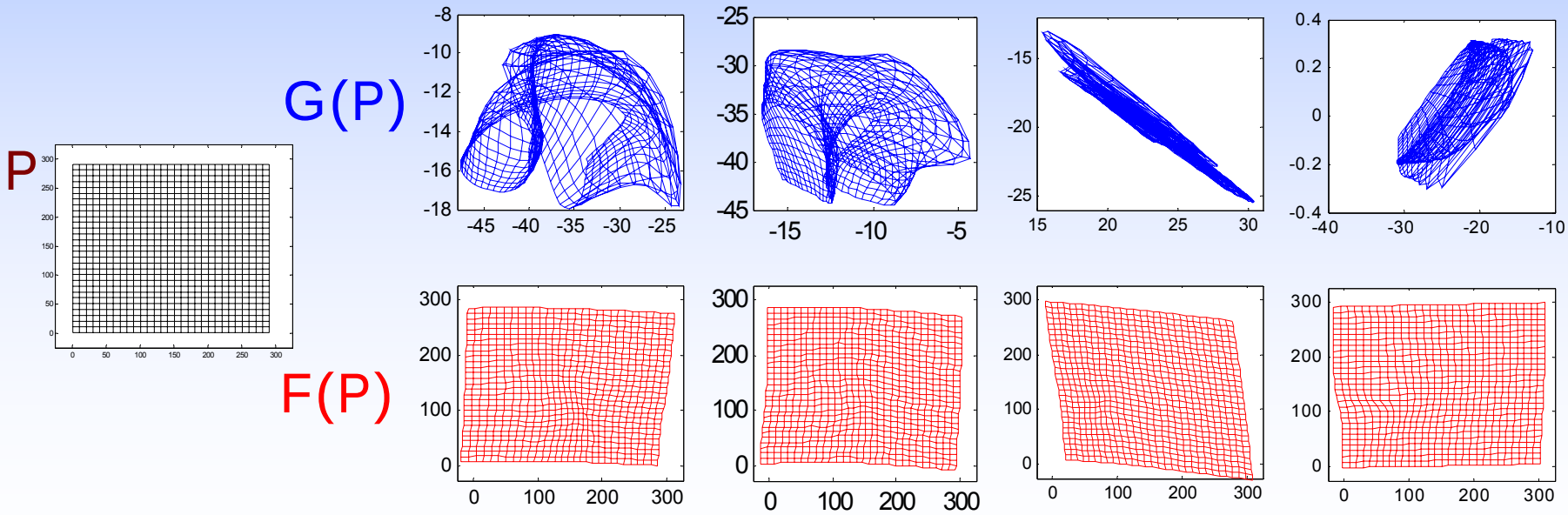
$$\sigma(u_i - u_j) = r^2 \log r, r = \| u_i - u_j \|$$

Fingerprint Liveness Detection

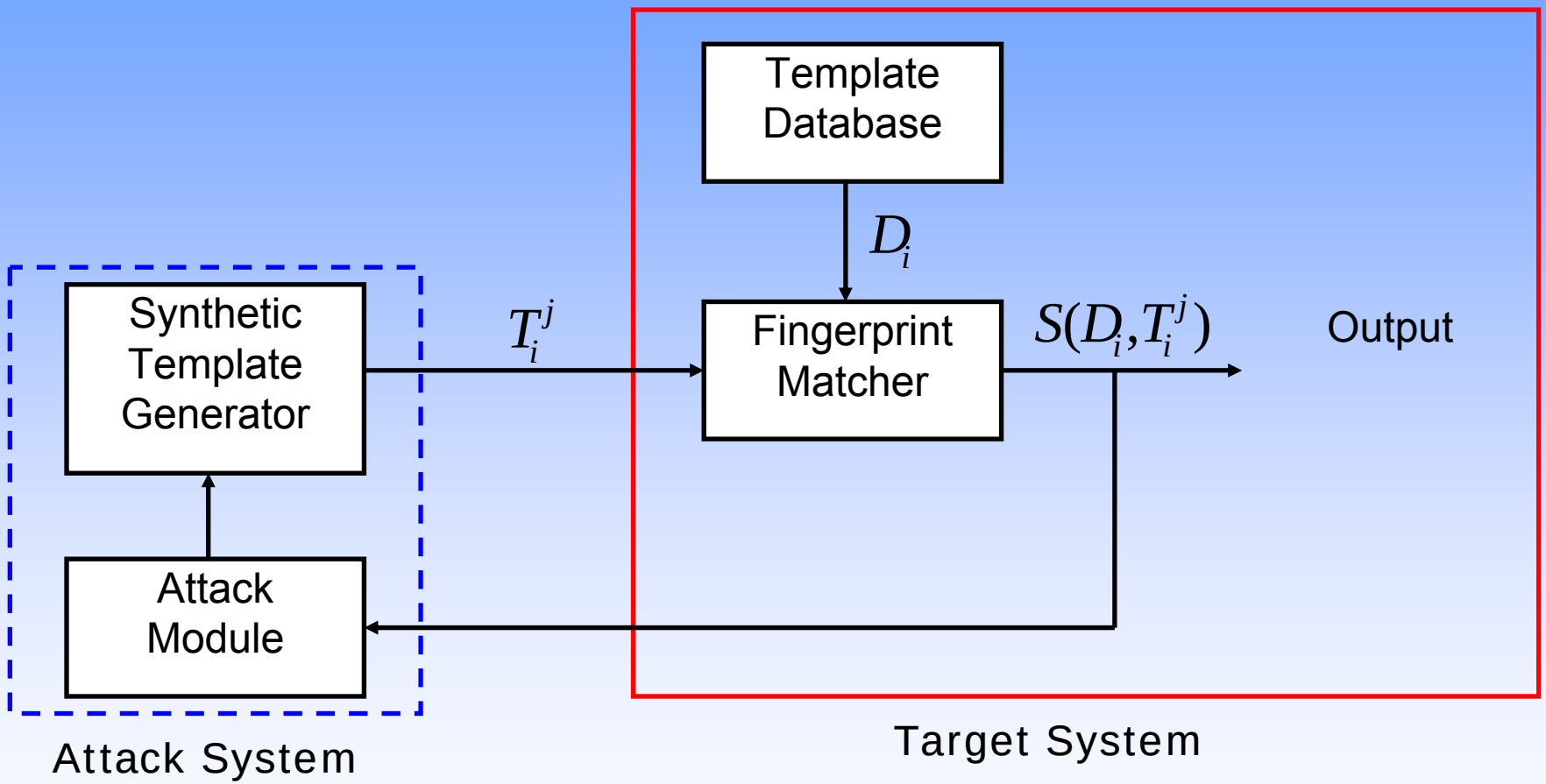
Estimate deformation (TPS) among all possible (genuine) *live vs. live* and *gummy vs. live pairs; ~82% accuracy*

$$G(p_i) = W^T s(p_i) \quad \text{(non-affine)}$$

$$F(p_i) = c + Ap_i + G(p_i) \quad \text{(affine+non-affine)}$$

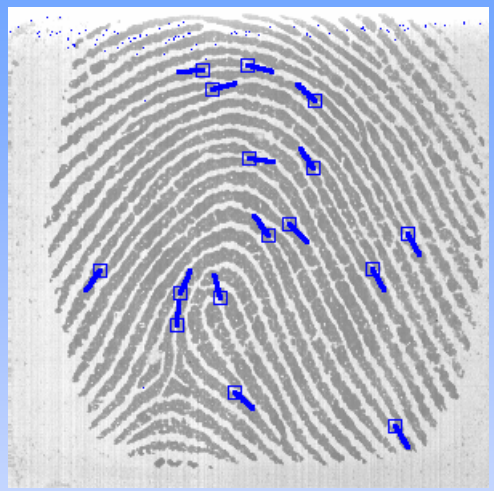


Hill-Climbing Attacks

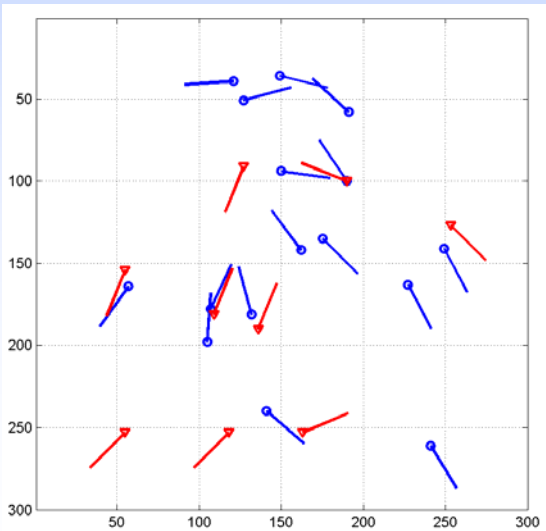


Bypass Feature Extractor: Inject random minutiae set and modify it iteratively to improve the matching score

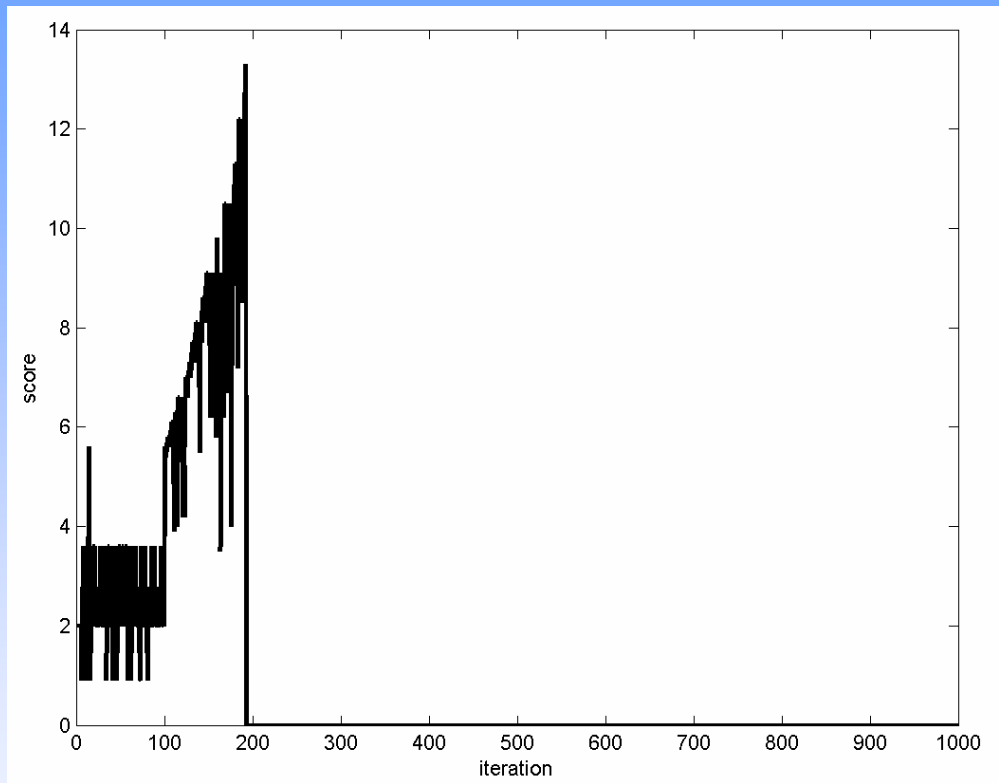
Injecting Random Minutiae Sets



Original image with minutiae



Synthetic (▽) and original (o) minutiae

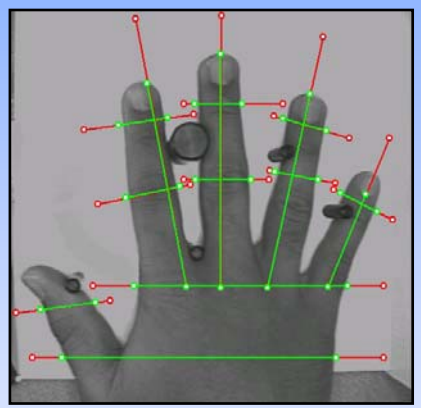


Progression of matching scores

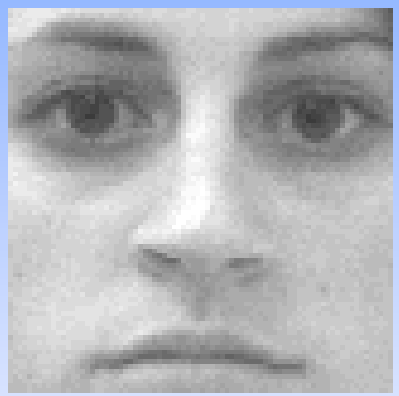
Account broken at iteration# 192: original template has 16 minutia; synthetic template has 10 minutia; 5 minutiae match; final matching score: 13.3

Biometric Template Protection

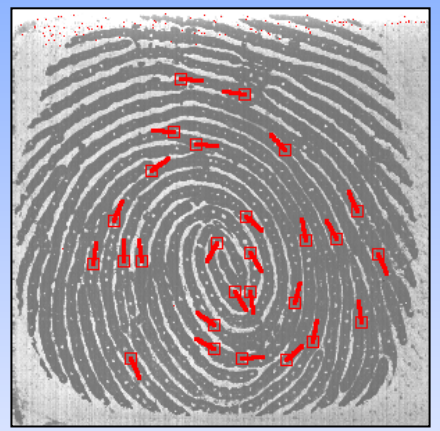
- A prototype of an individual's biometric that is stored in (i) database or (ii) smart card



Hand geometry



PCA coefficients



Minutiae features

"A true fingerprint image cannot be created from master template.."

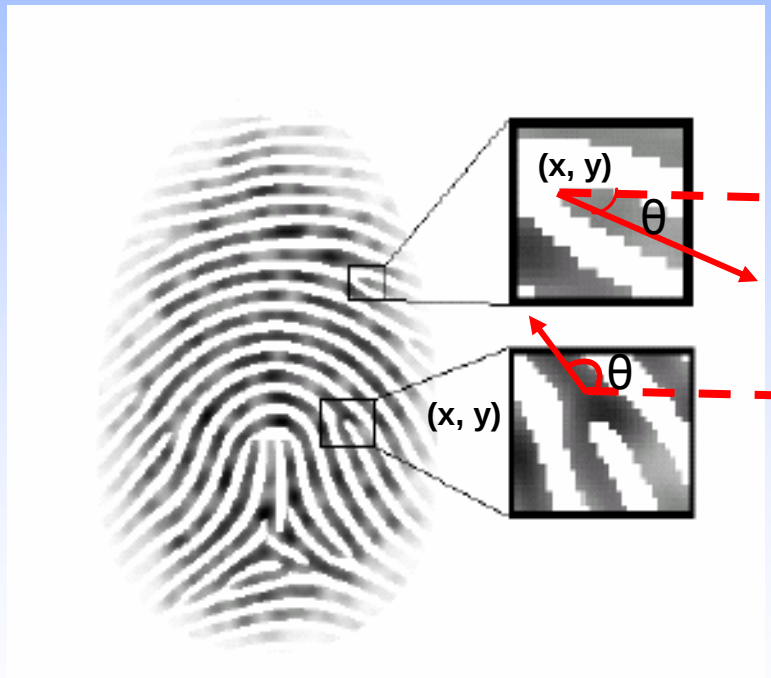
http://www.biometricaccess.com/support/bacfaq09.html
http://www.digitalpersona.com/support/faqs/privacy.html

Fingerprint Reconstruction From Minutiae Template

How much information does the minutiae distribution reveal about the original fingerprint?

Given a minutiae template (X_i, Y_i, θ_i):

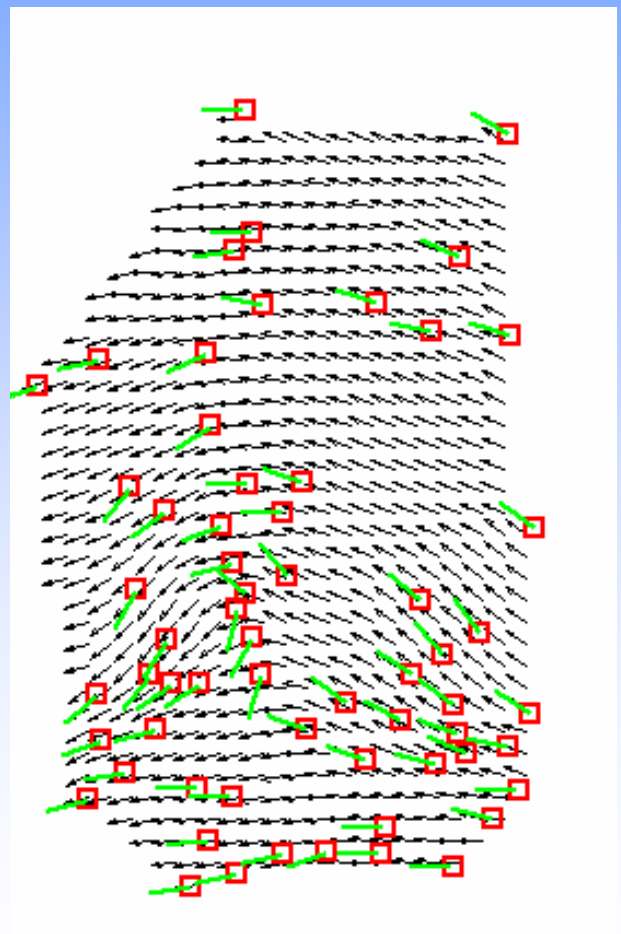
1. Estimate ridge flow
2. Predict class (A, L, R, W)
3. Reconstruct fingerprint



Orientation Estimation

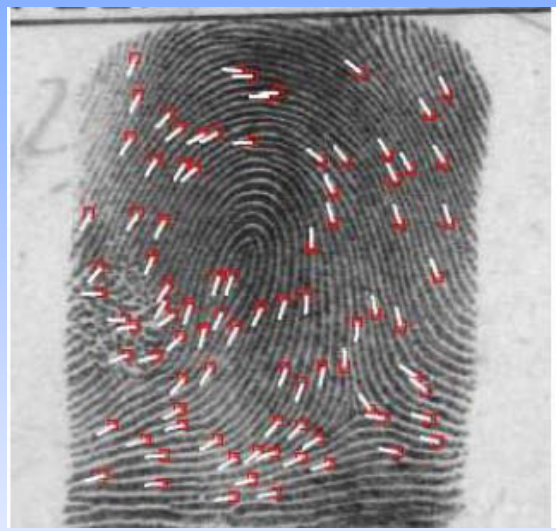
Minutiae orientations represent direction of ridge flow;
Interpolate ridge flow using group of minutiae

Original fingerprint

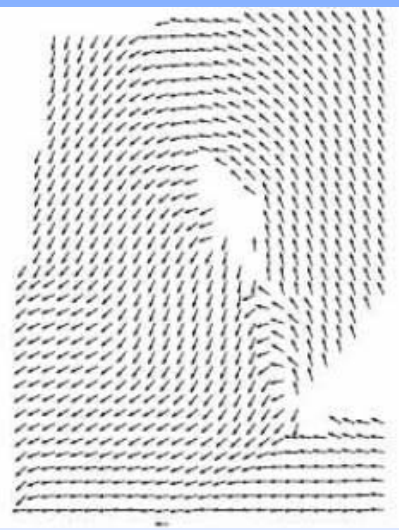


Estimated orientation field

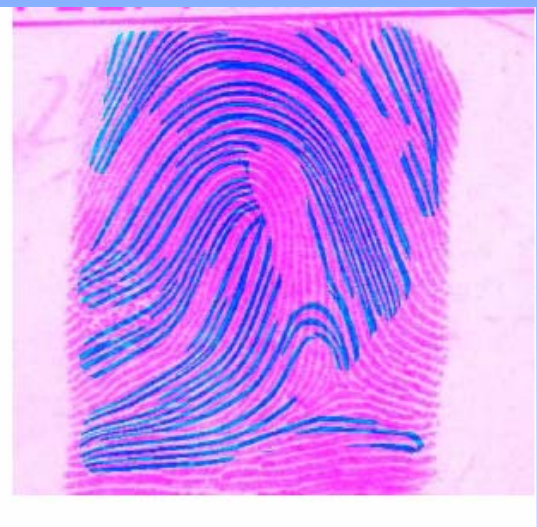
Fingerprint Reconstruction



Original fingerprint with minutiae



Orientation field estimated using minutiae



Reconstructed fingerprint overlaid on original

Reconstructed artifacts were matched with the true fingerprints with 23% success

Template Protection

Encryption

- Template is still vulnerable when it is decrypted

Watermarking

- Any tampering of the image can be identified

Steganography

- Hide the template in a carrier (cover) image

Transformed Template

- Store a (non-invertible) transformed version of the template

Template Encryption

- Store or transfer only encrypted template E, encrypted (e.g., using AES, RSA) with the secret key KE:

E = ENCRYPT(T, KE)

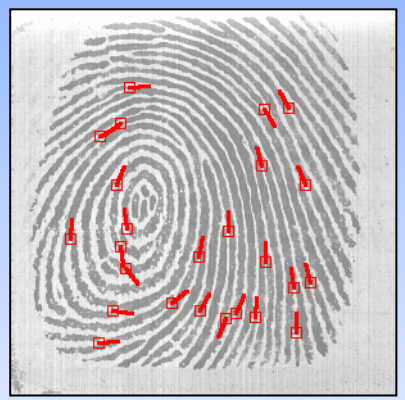
- Decrypt the template only when necessary with the appropriate decryption key, KD:

T = DECRYPT(E, KD)

- Template is secure while encrypted: Without KD, E can not be converted back to T

- But, Matcher needs the original template and decrypted templates are still vulnerable to attacks!

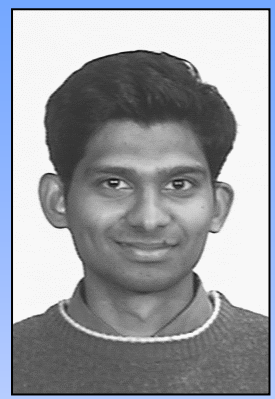
Hiding Minutiae in Face



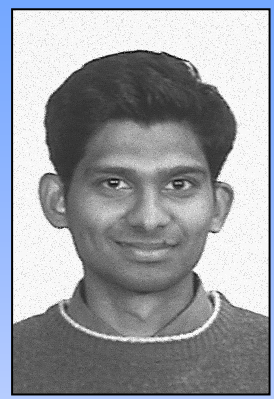
Minutiae

x	y	θ
76	216	242
121	195	255
136	82	292
136	229	248
170	90	262
172	169	270
178	46	274
184	85	82
192	146	281
196	198	270
201	89	52
212	233	255
216	220	262
228	125	321
234	79	8
234	147	298
236	175	295
240	167	112
259	68	356
60	92	356
77	197	58
88	85	144
98	69	332
239	190	274
251	222	270

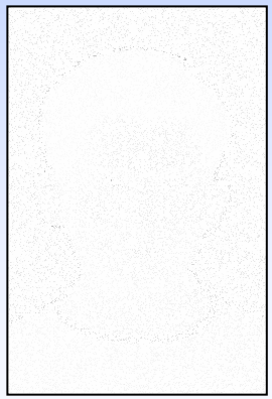
Minutiae attributes



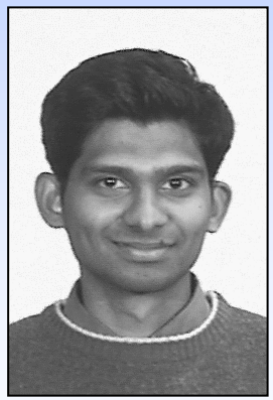
Host face image



Marked face image



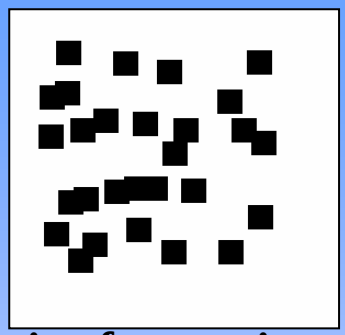
Negative of difference image



Reconstructed face image

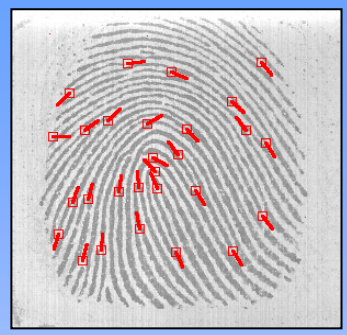
Hiding Eigenfaces in Fingerprints

input face



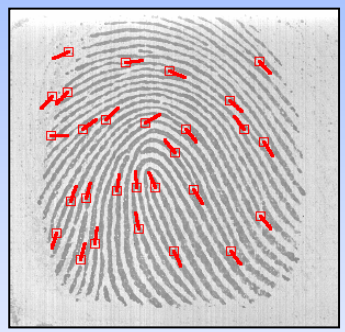
minutiae feature image

watermarked image

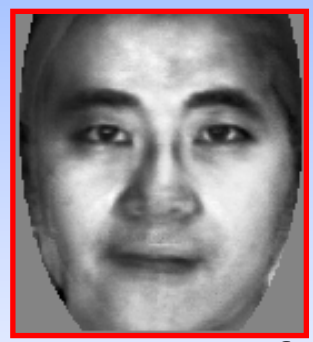


-39.06
-29.71
17.44
-49.33
-12.07
19.66
-0.42
-2.10
4.07
-6.49
4.44
2.31
-13.24
2.74

14 eigen-face coefficients



minutiae overlaid host fingerprint



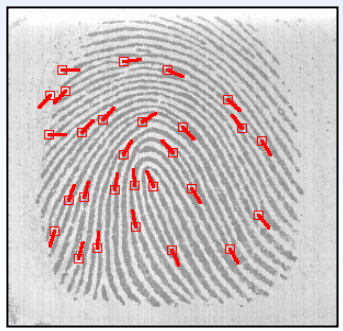
reconstructed face

minutiae overlaid reconstructed fingerprint

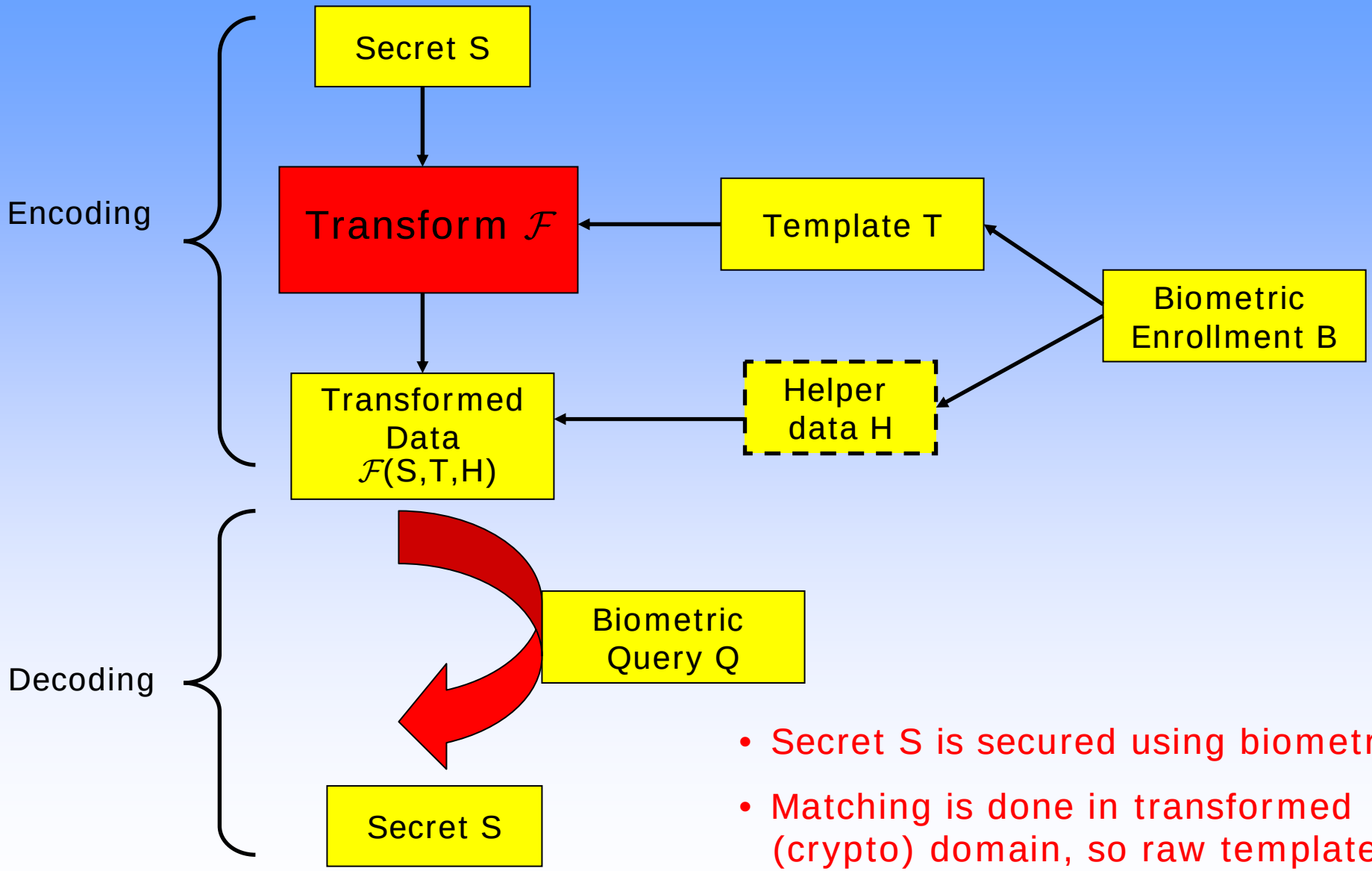
watermark face

ridge feature image

watermarked image



Biometric Cryptography

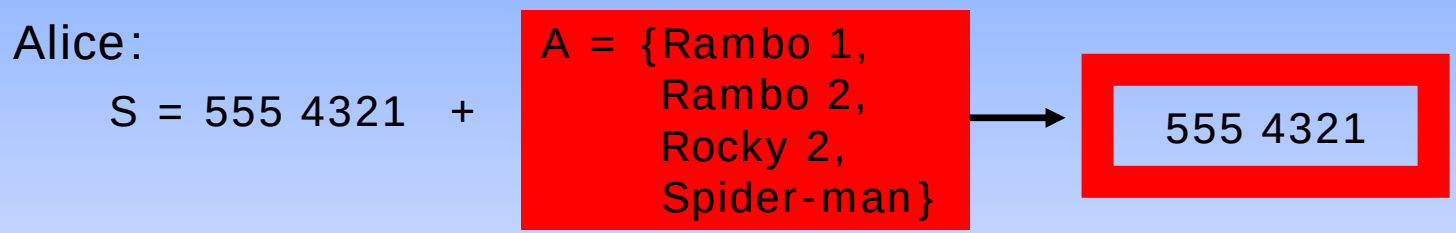


- Secret S is secured using biometric
- Matching is done in transformed (crypto) domain, so raw template is not stored

Fuzzy Vault

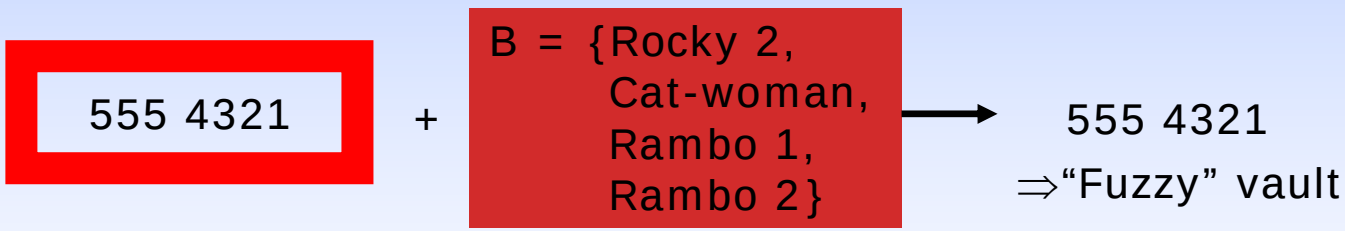
- Alice places a secret S in a vault and locks it using a set A
- Bob uses an unordered set B to unlock the vault: successful iff B and A overlap substantially

Alice locks her phone no. in the vault using her favorite movies:

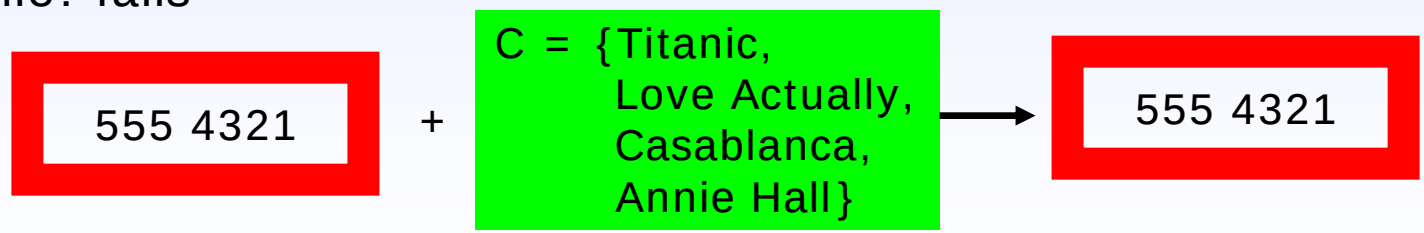


Unlocking attempts:

Bob: succeeds



Charlie: fails



Juels and Sudan, “ A Fuzzy Vault Scheme”, Proc. Symp. Inf. Th, 2002

Fuzzy Vault: Challenges

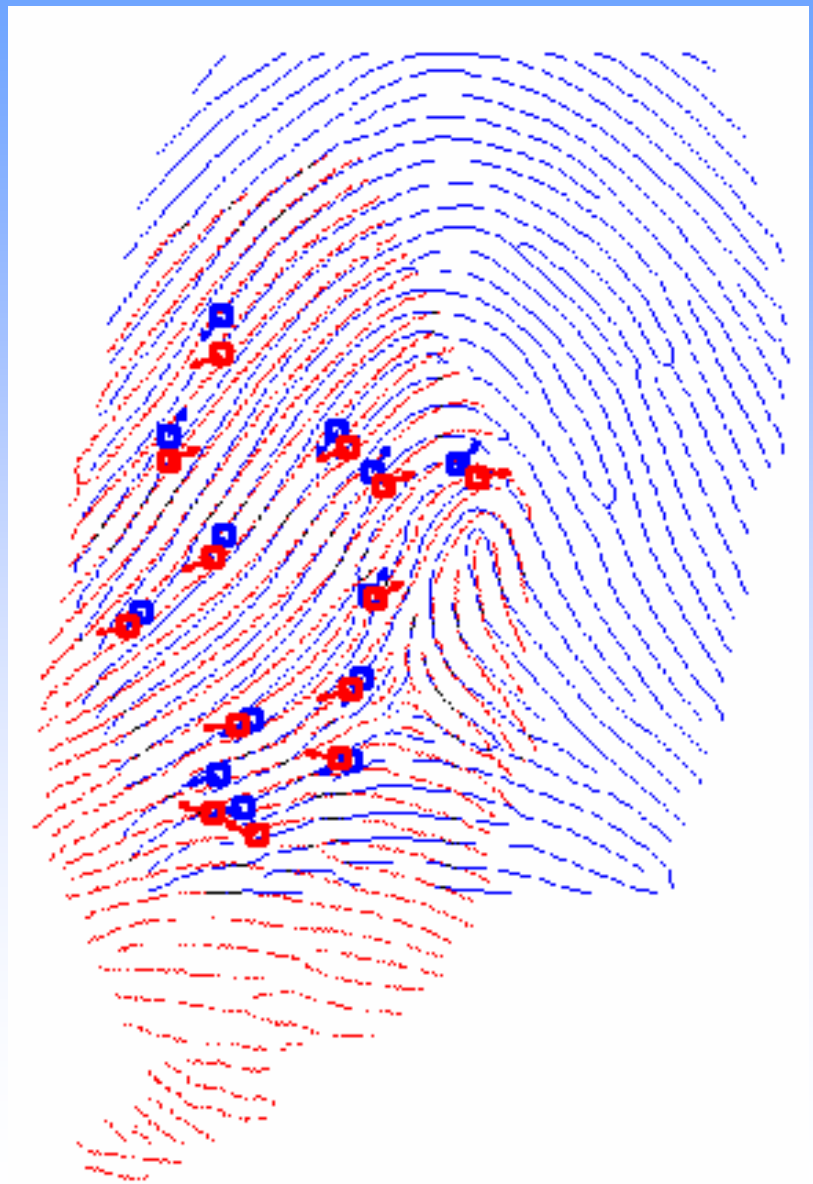
- Intra-class Variability
  - Images may differ w.r.t. rotation, translation, deformation & no. of minutiae
- Alignment of Template & Query
  - How to align template & query since the template is not available at decoding time!

Intra-class Variability

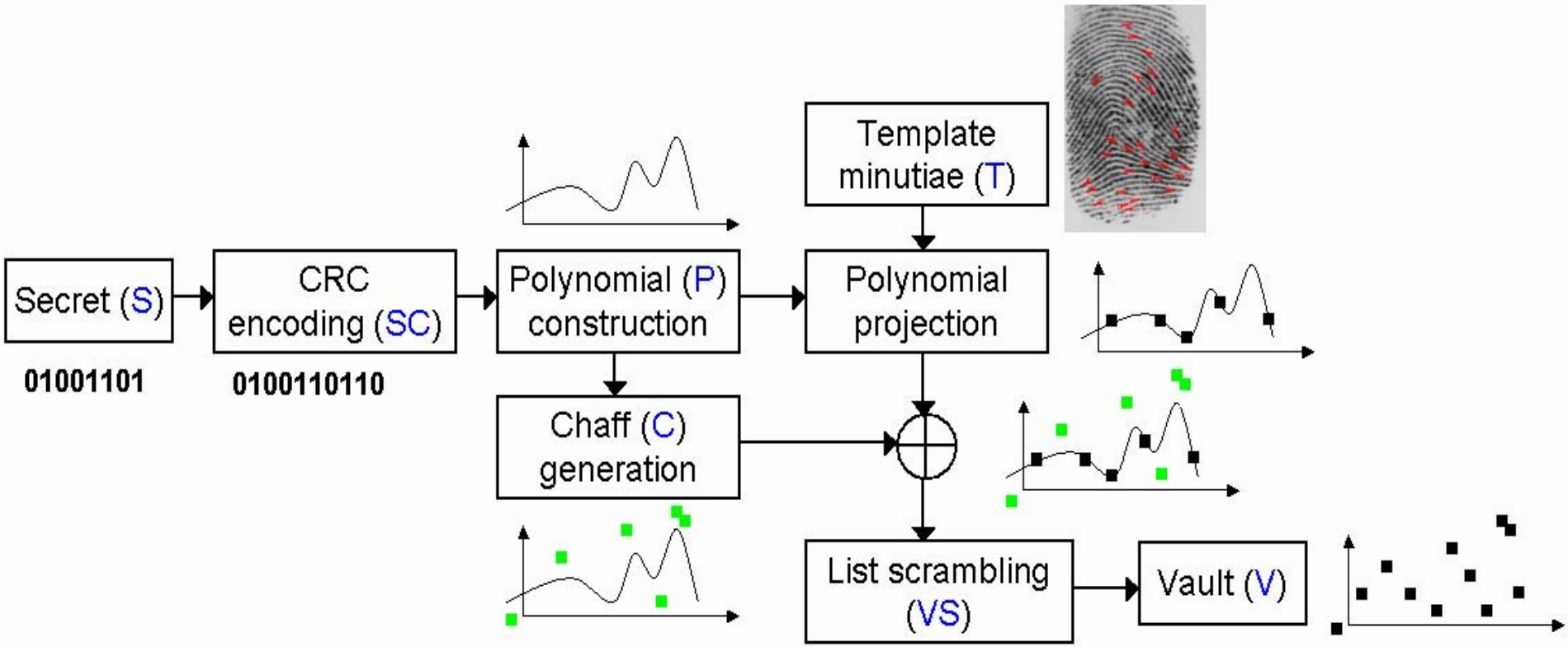
y

x

Alignment

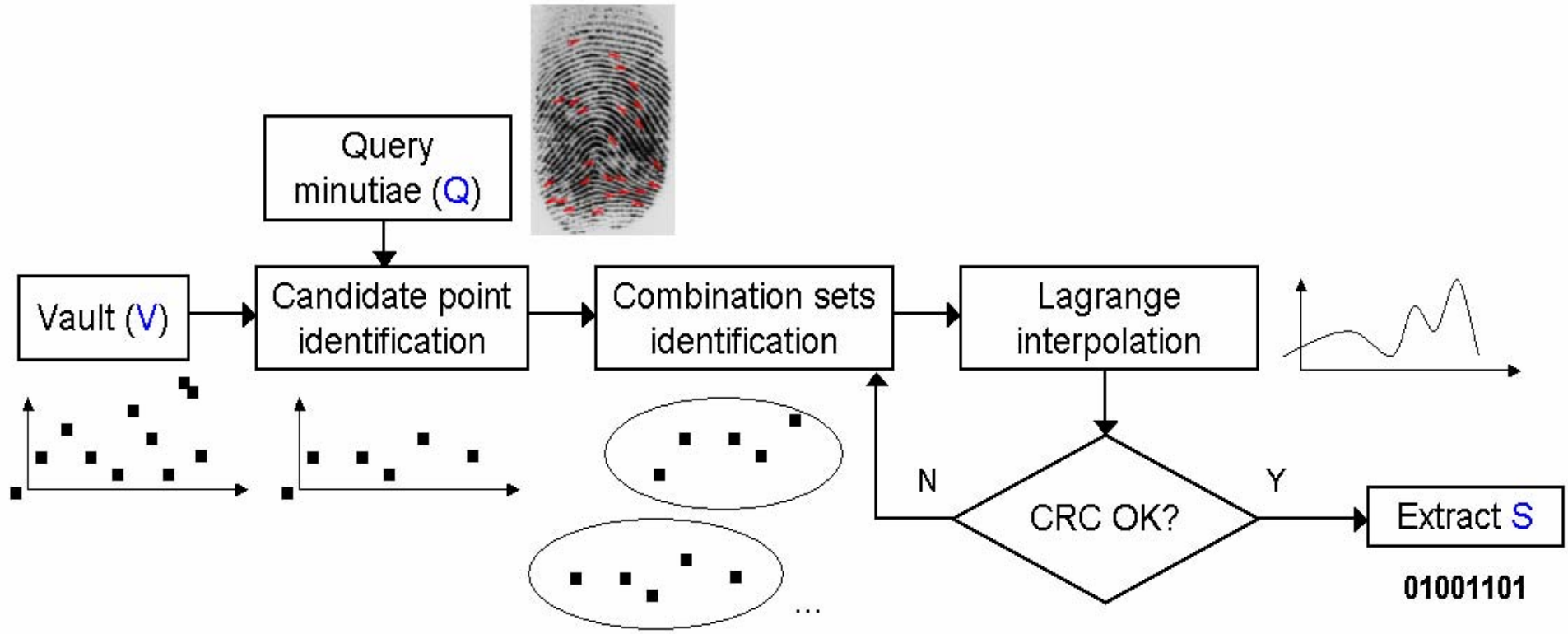


Fuzzy Fingerprint Vault Encoding



- Secret S is secured using template minutiae T:
  - T generates points on the polynomial P, chaff points are also added to this point list to increase security
  - Cyclic Redundancy Check is used for error detection during decoding
- Final vault is a 2D point list, with no minutiae vs. chaff point separation

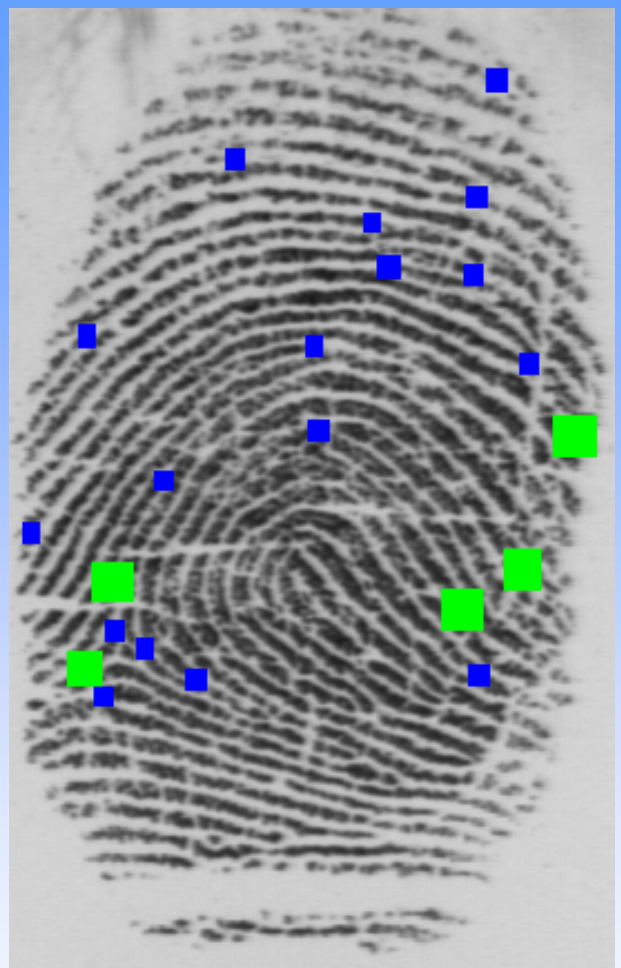
Fuzzy Fingerprint Vault Decoding



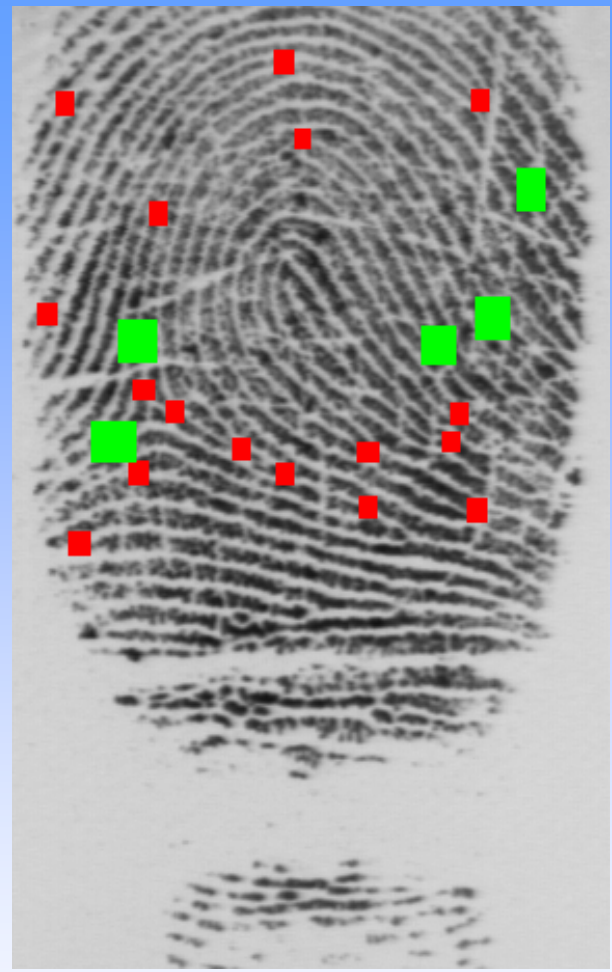
- Query minutiae Q extracts the secret S from the vault:
  - Q picks candidate points from the vault to be used in decoding
  - Lagrange interpolation using subsets of this candidate list results in the decoded polynomial (and the secret S)

Performance of Fingerprint Vault

- Fingerprint database (229 300x400 pairs)
  - Minutiae correspondences manually established
    - 16-bit minutiae locations are used for securing the vault; secret S: 128-bit AES key
    - Polynomial degree p=8, # minutiae= 22, #chaff points = 200
- Genuine Accept Rate: 85%
  - 34 out of 229 query templates could not separate sufficient no. of (≥9) genuine points from chaff points
- False Accept Rate: 0%



template fingerprint
(marked: 22 locking minutiae, **5 common**)

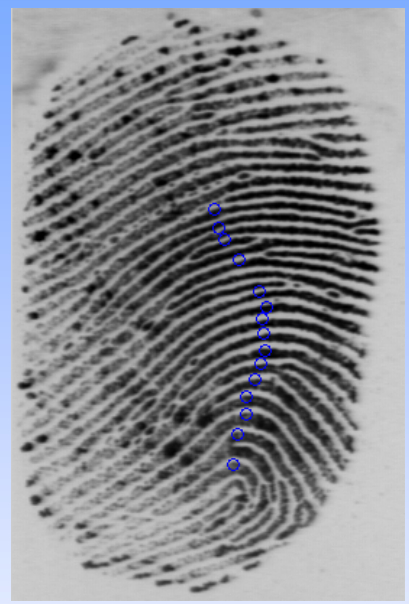


query fingerprint
(marked: 22 unlocking minutiae, **5 common**)

False Reject: Only 5 genuine points found during decoding; this is due to large intra-class variations

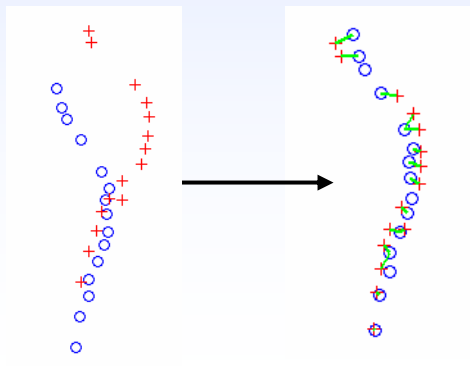
Automatic Fingerprint Alignment

- Align query fingerprint with template helper data (points of maximum curvature on Orientation Field Flow curves)



Template helper data

Query → Helper data extraction → ICP alignment → Vault decoding



Britain's Identity Crisis

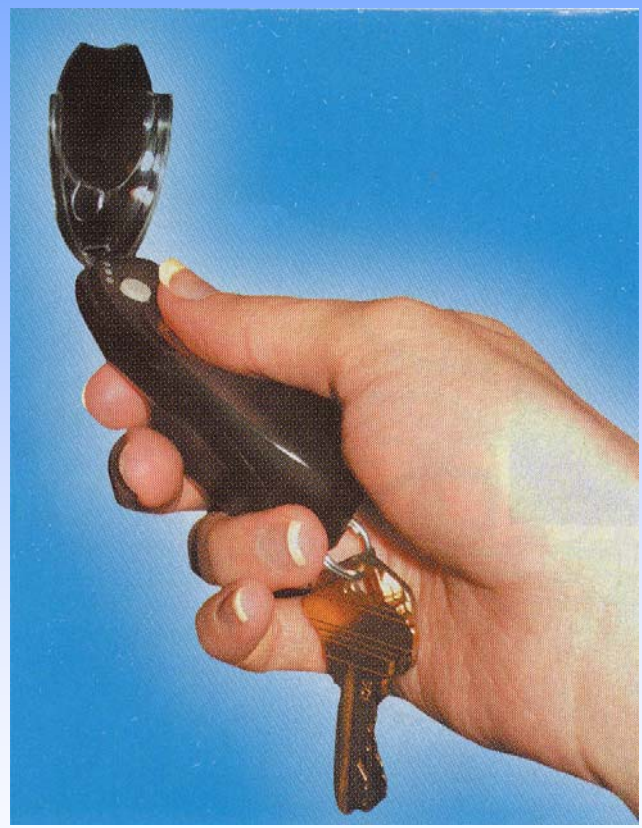
Proposed biometric ID cards won't prevent fraud or terrorism (IEEE Spectrum, Jan 2006)

- Proposal: Issue everyone an ID card with a microchip containing personal and biometric data. Data will also be stored in a central database
- Proponents: Card-database combination will provide a foolproof ID check
- Critics: (i) How much will ID cards cut down identity theft and terrorism? (ii) Total cost: 10-20 billion pounds, (iii) central database subject to failure and denial-of-service attacks, (iv) identification accuracy may not be adequate to handle ~50 million users
- Central database is "poor security and poor privacy practice"

Decentralization of Templates

Fingerprint ID For Wireless Keys, IEEE Spectrum, Jan 2006)

- A fingerprint scanner is placed in a battery-powered device that fits like a fob on a key chain. It can communicate with either RFID readers or Bluetooth radios
- A typical use is as an RFID key for access control
- Fingerprint matching takes place inside the device, so fingerprint never leaves the device; fob can be reprogrammed only by the machine that set it up.



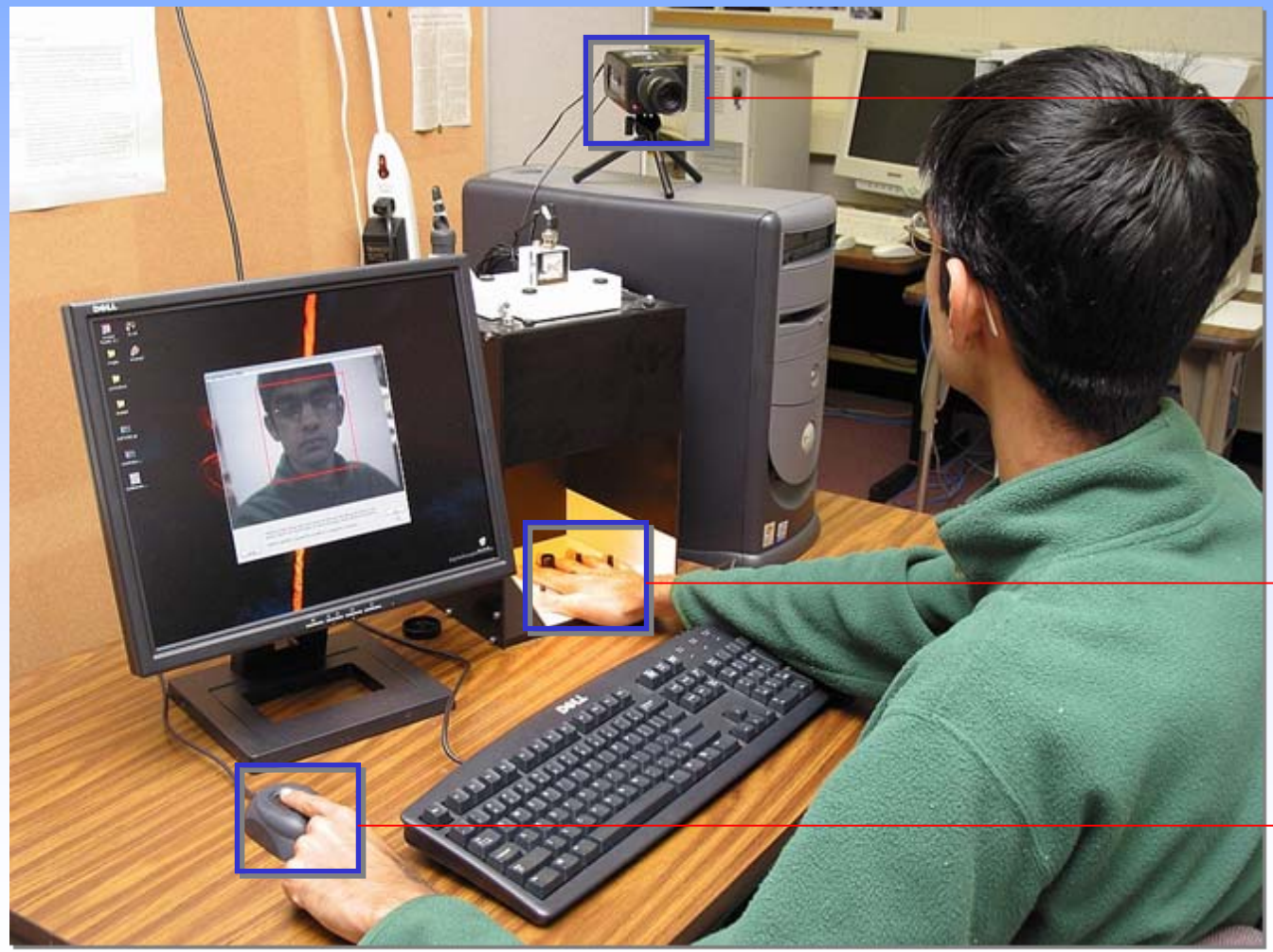
www.privaris.com

Other Attacks

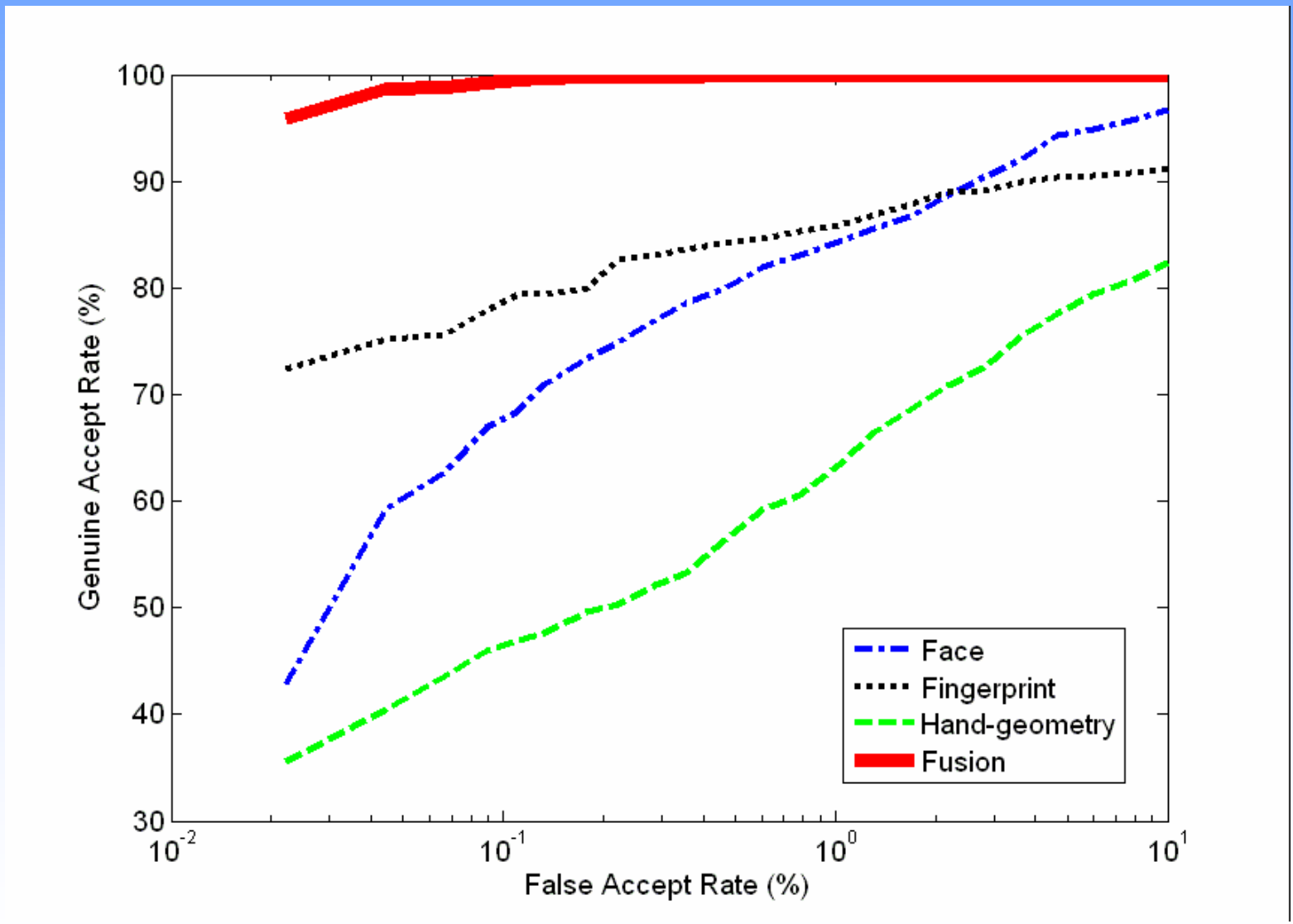
- Insider attacks
- Integrity of the enrollment process
- Once initial access is granted, an impostor can spoof the system in the absence of real-time continuous authentication
- Exception handling may introduce a weak link
- By providing poor quality images at input
- Biometrics is made ineffective by attacking other components of the security system

Multibiometrics

Provides resistance against spoof attacks; also improves matching accuracy and population coverage



Multibiometric System Performance



Securing Wireless Devices With Multibiometric

- AuthenTec has sold 4 million fingerprint sensors world-wide to provide secure authentication for mobile commerce and mobile banking applications

Summary

- Biometrics are an essential component of any identity-based system, but they themselves are vulnerable
- Some of these attacks are simple to execute; solutions to these attacks have been identified, but there is still room for improvement
- Attacks on biometric systems can result in loss of privacy and monetary damage, so the users need to be convinced about the system protection
- New security issues with biometric systems may arise as their use becomes more widespread
- In spite of this, biometric systems are being deployed for securing international borders, controlling access and eliminating identity theft