Biometric System Security

Anil K. Jain

Dept. of Computer Science and Engineering

Michigan State University

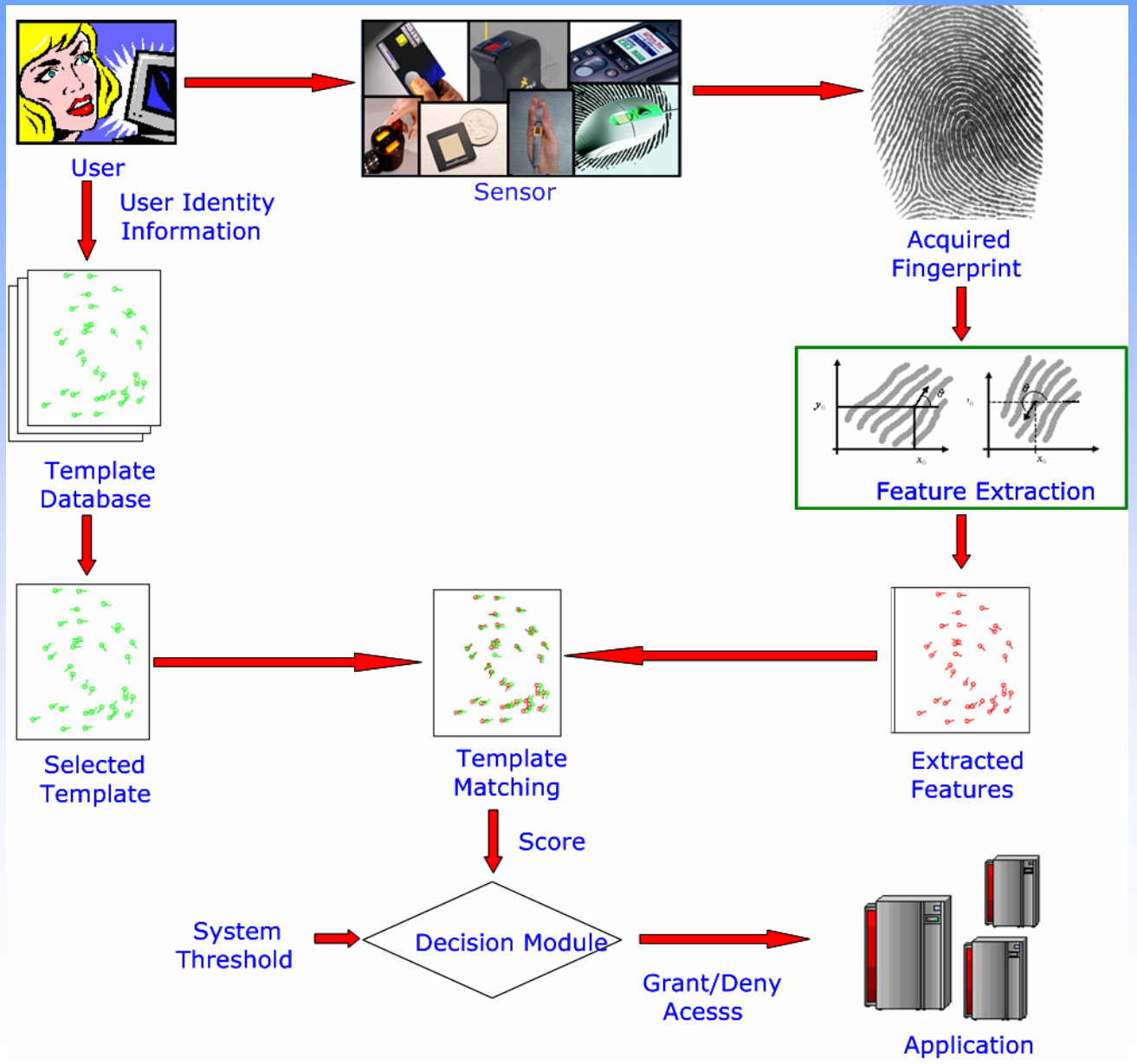
http://biometrics.cse.msu.edu

Biometric System Security

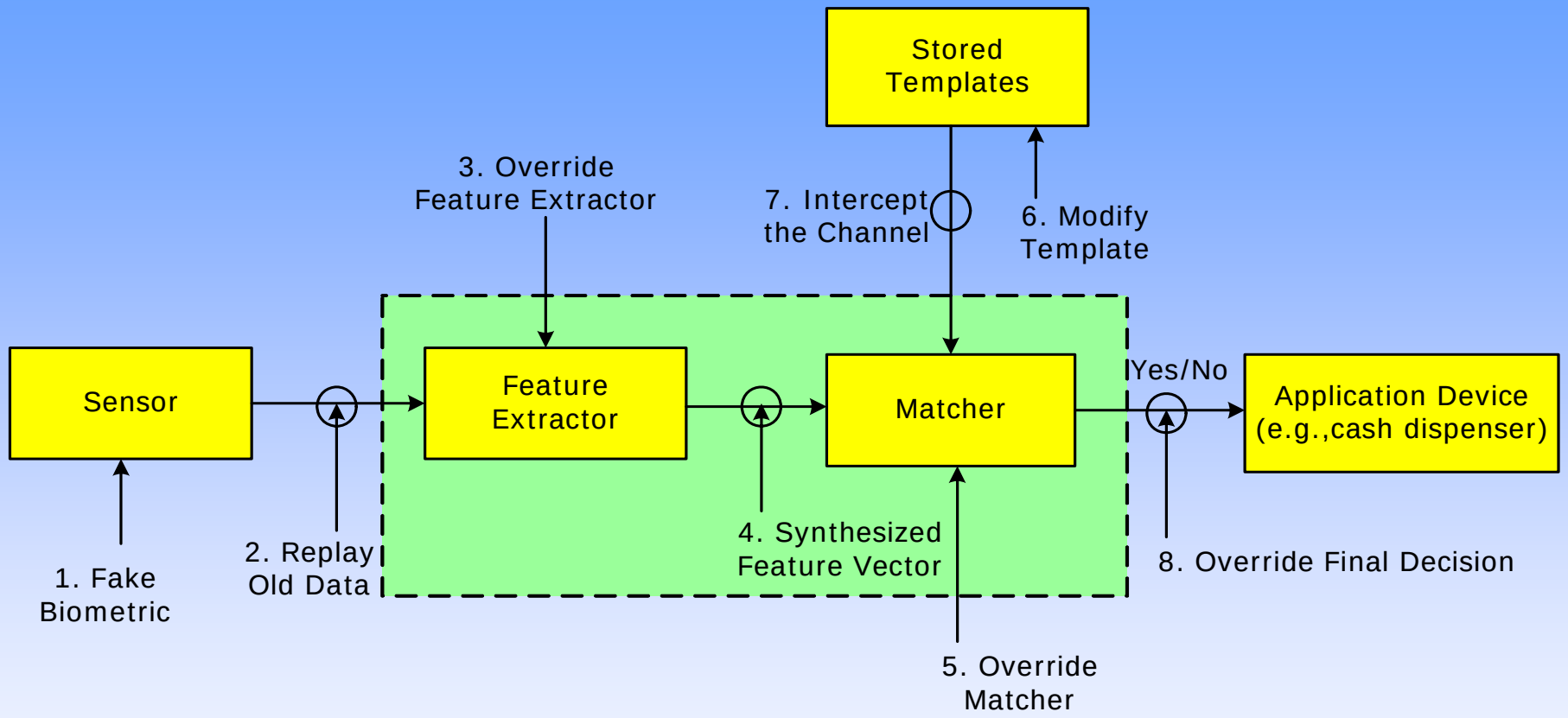
- Number of installed biometric systems in both commercial and government sectors is increasing
- Size of the population that uses some of these systems is extremely large (US VISIT program)
- New emerging applications in laptops, mobile phones, e-commerce, health care records,….

- 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!

Fingerprint System



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

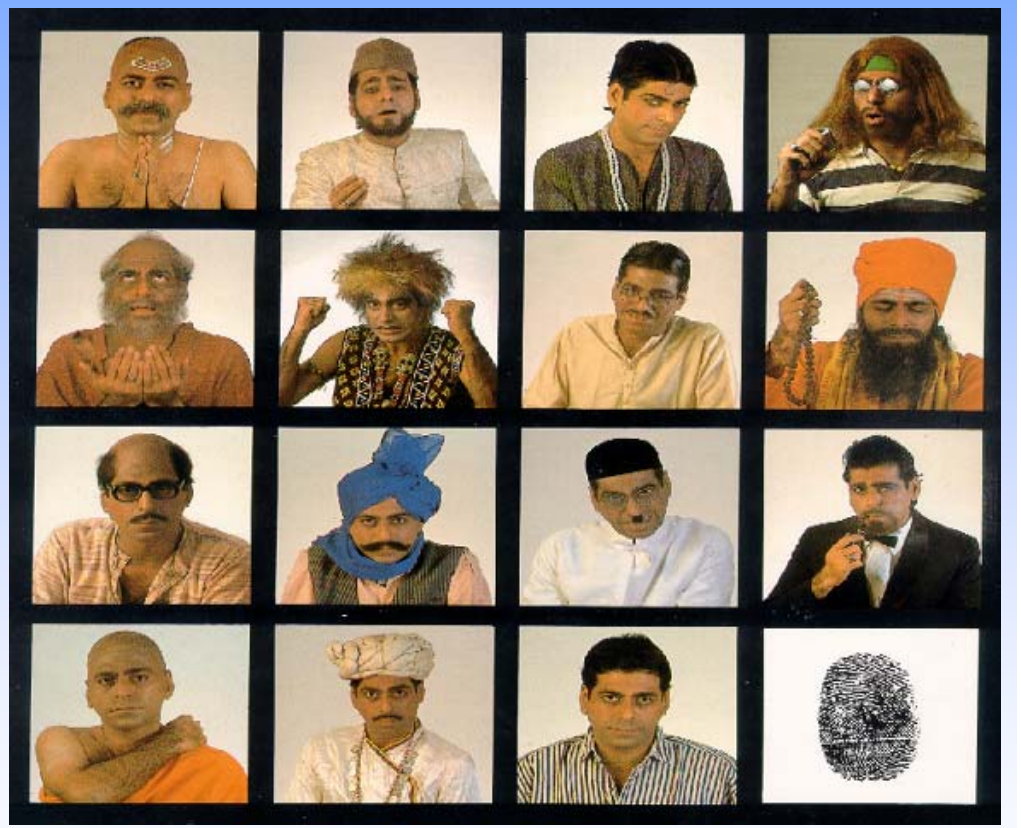
- Coercion
- Camouflage
- Synthetic biometric with/without user's cooperation

"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."

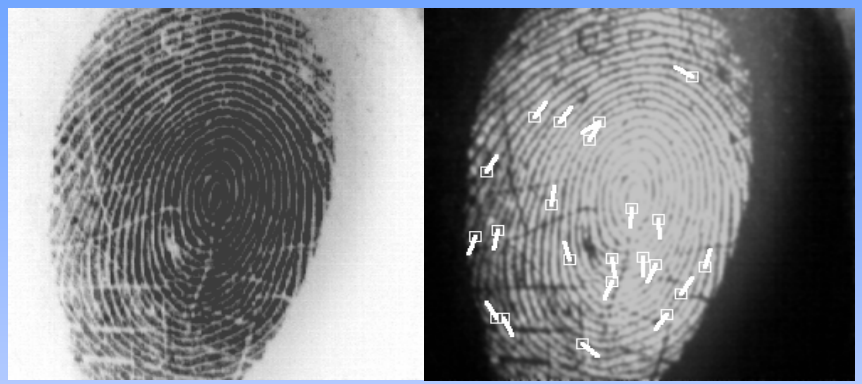
BBC News, 31 March, 2005

Camouflage

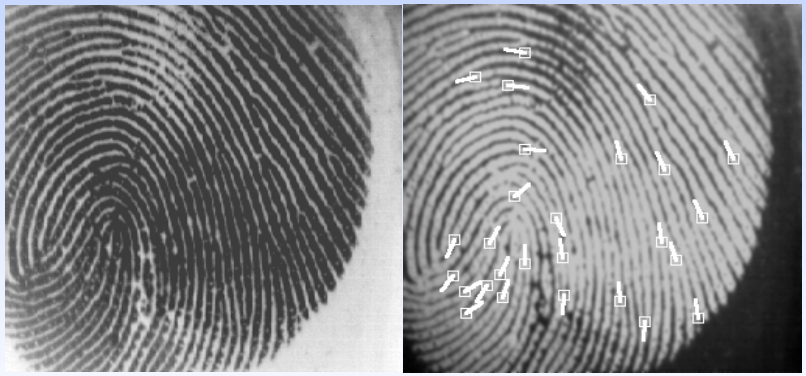

In response to the new TIA's Gait Identification Program, Americans take action to protect their Privacy
ANTELMES
5/22/03 ©2003 Tribune Media Services, Inc. All rights reserved ATelmaes@AOL.COM

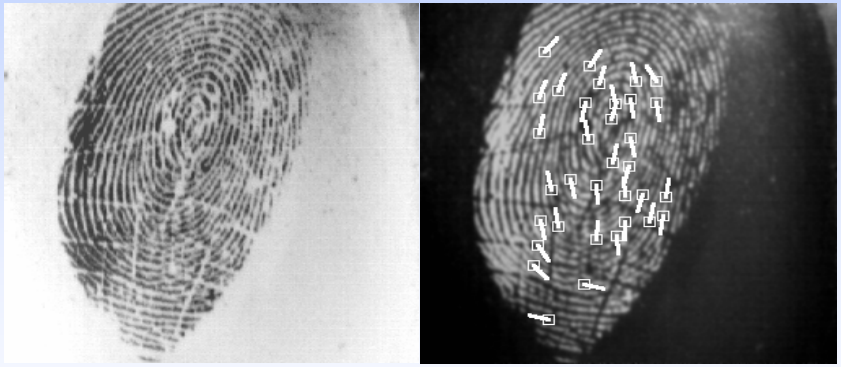


Fake Fingerprints



Live finger





Gummy finger

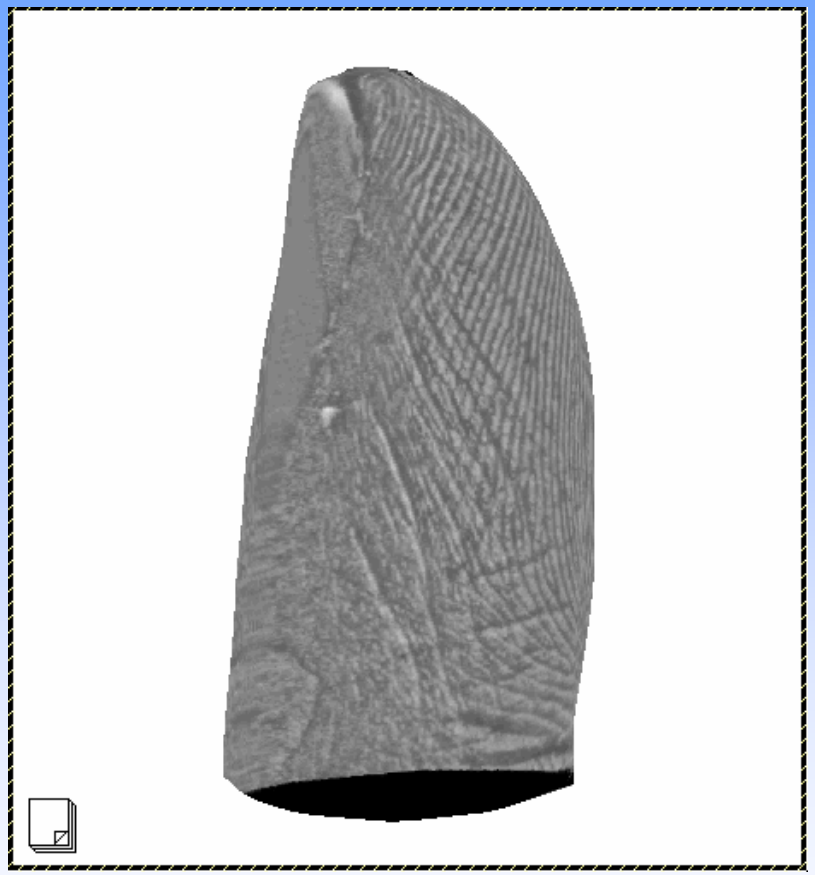
Access was granted 75% of the time using gummy fingers

New Sensing Technologies

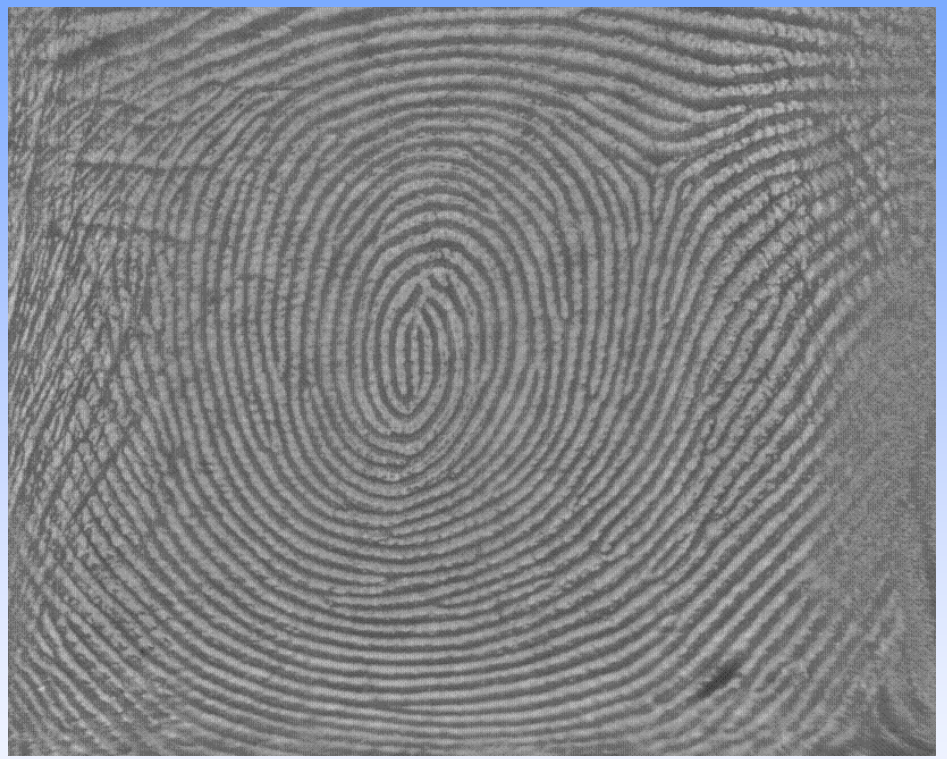
- Touchless
- High Resolution
- Multispectral

These sensors provide higher quality image and are resistant to spoof attacks

Touchless Sensors



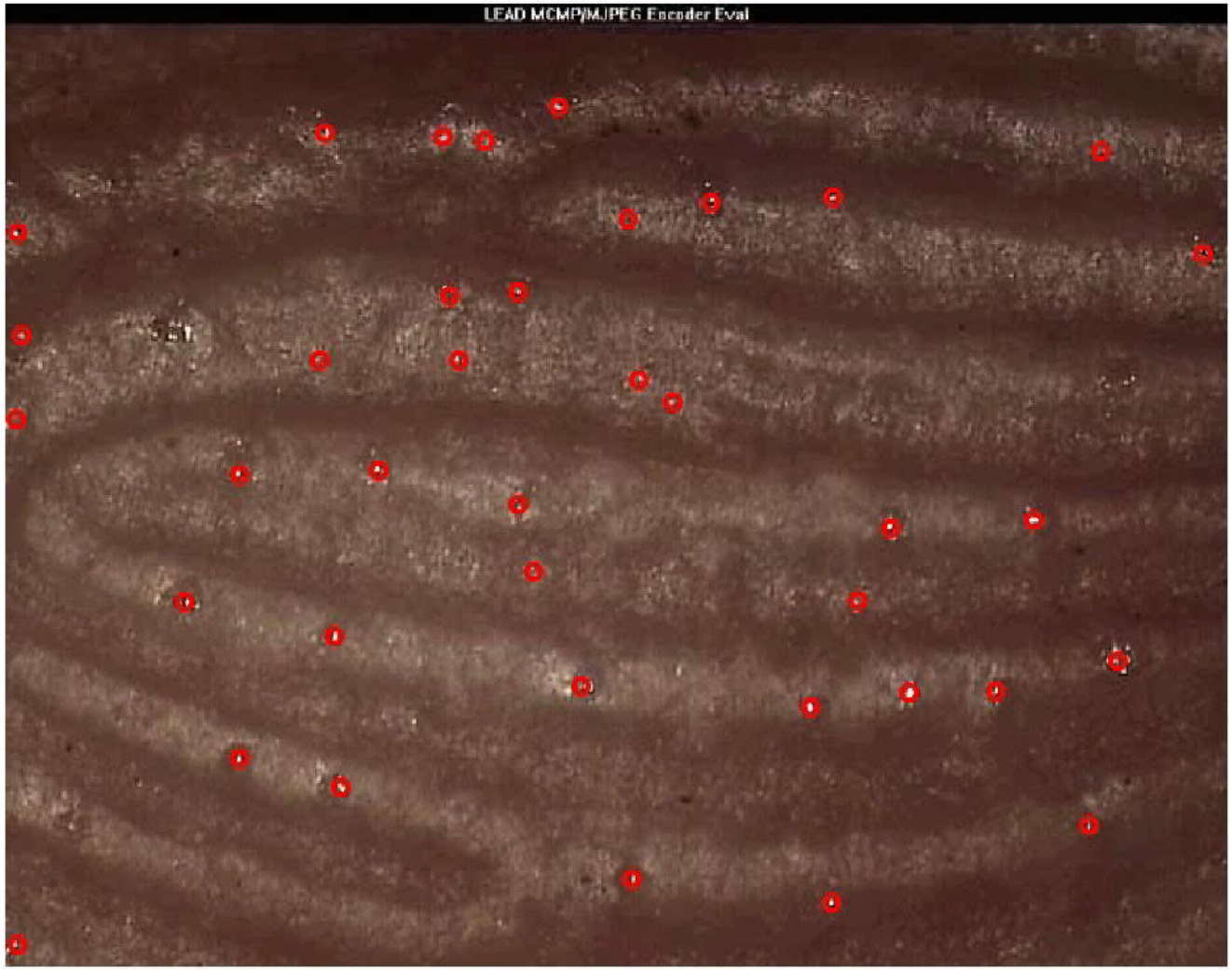
Touchless 3D image



Touchless “rolled” image

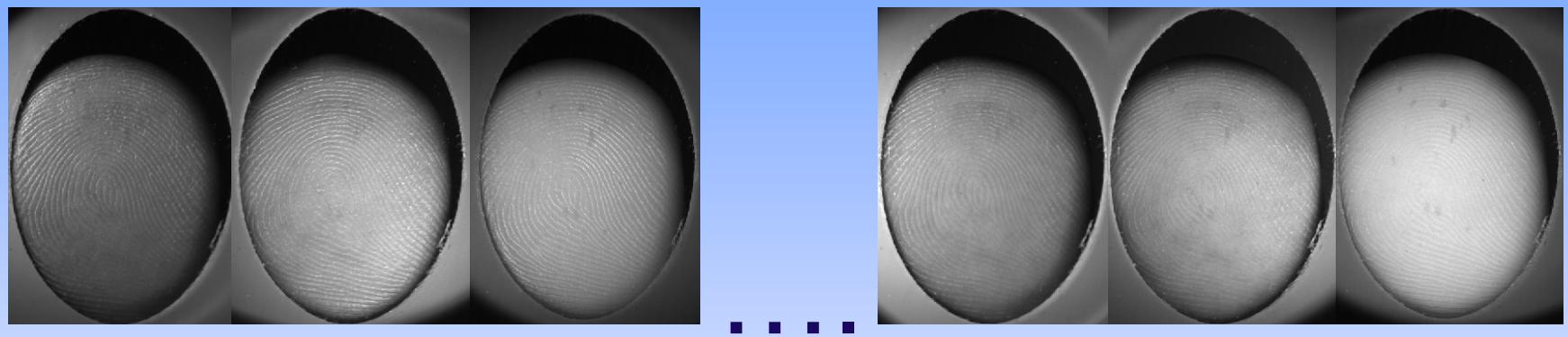
Courtesy: TBS North America, Inc.

High Resolution Sensors



Multispectral Fingerprint Imaging

Multiple wavelengths capture features at different depths (surface and subsurface) of the finger tissue

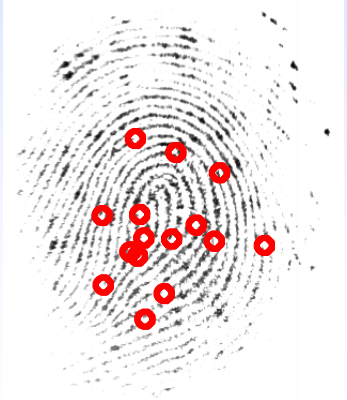


430 Non-polarized (Blue) | 530 Non-polarized (Green) | 630 Non-polarized (Red) | .... | 430 Polarized (Blue) | 530 Polarized (Green) | 630 Polarized (Red)

Jupiter 1.10
Combined Image - MSI

VS.

Cross Match Verifier
Model 300 - TIR



Courtesy: Lumidigm

Spoof Detection With MSI

Spoof finger
made of glue

Optical Sensor MSI Sensor

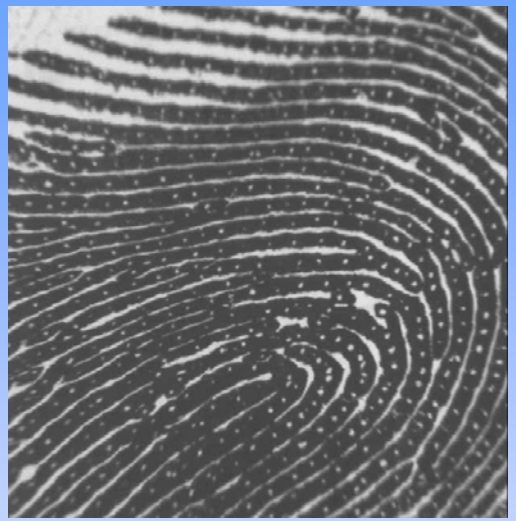
True Finger

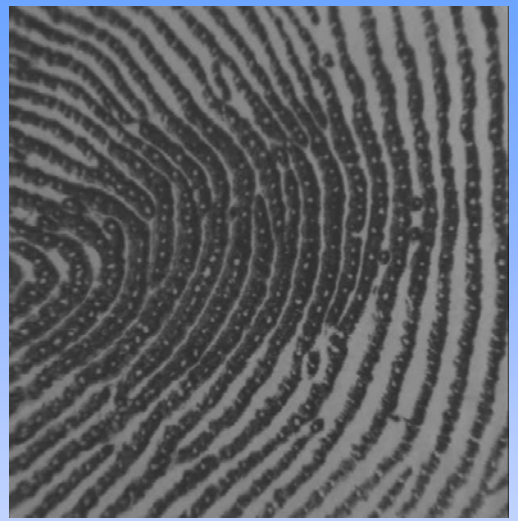
Finger with
glue spoof

MSI sensor can see 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

Estimating Deformation Using TPS

- Given two point sets $U=\{u_1, u_2,\ldots u_n\}$ and $V=\{v_1, v_2,\ldots v_n\}$ that are in correspondence, estimate deformation

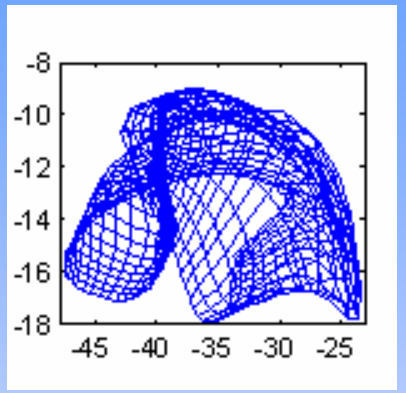
$$F(u_i) = \underbrace{c + Au_i}_{\text{Affine}} + \underbrace{W^T s(u_i)}_{\text{Non-Affine}} = v_i$$

- Thin Plate Spline (TPS) model is used to estimate the deformation among all possible (genuine) *live vs. live* and *gummy vs. live pairs*

- Features from the deformation model provide ~82% accuracy

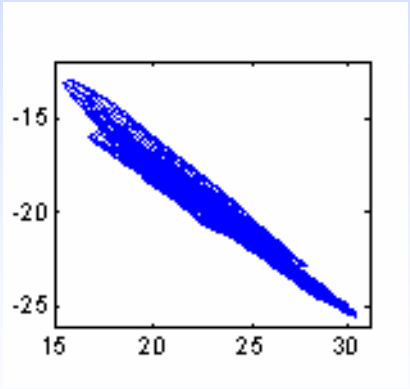
Fingerprint Liveness Detection

Live finger vs. Live finger

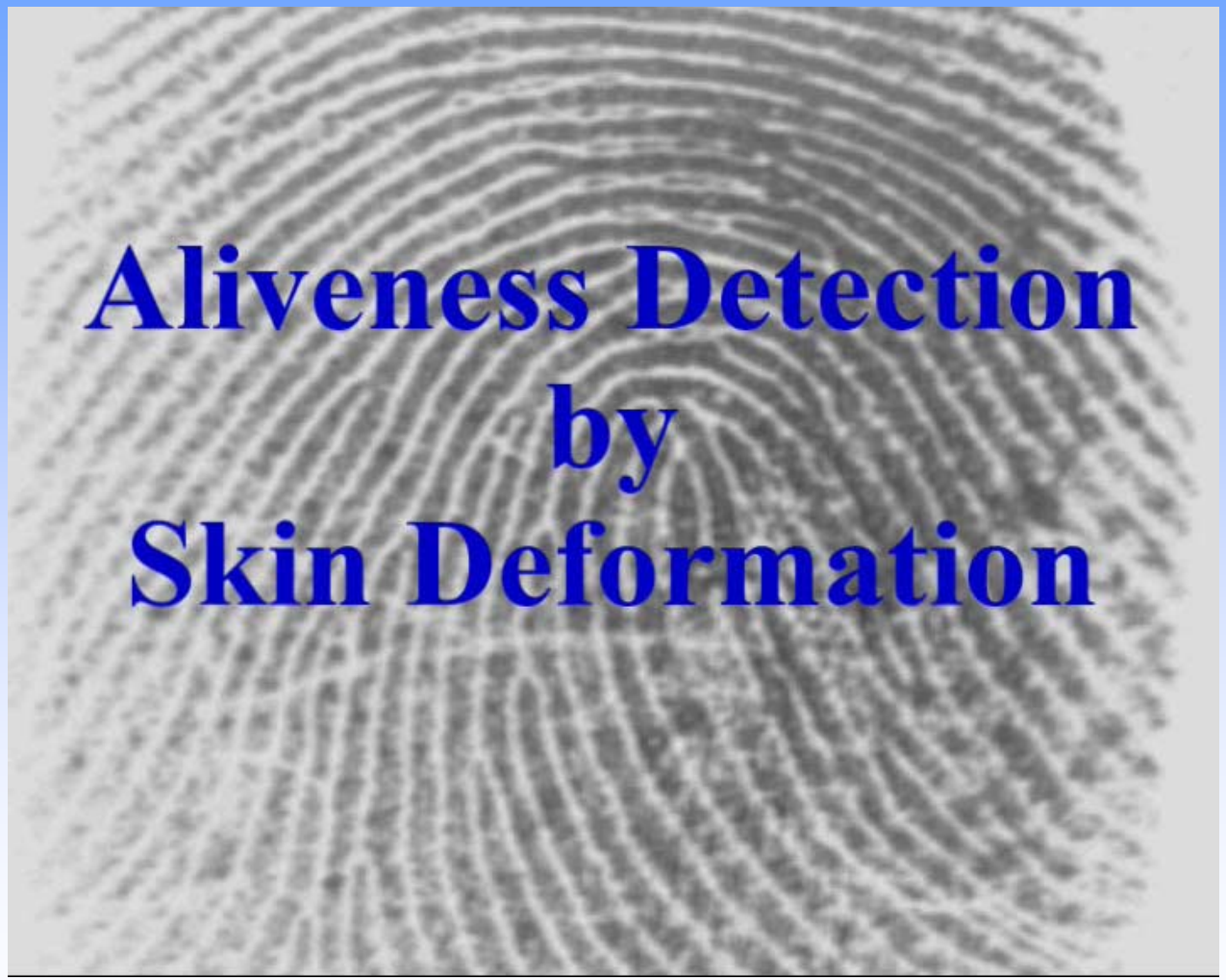


Estimated deformation

Live finger vs. Gummy finger

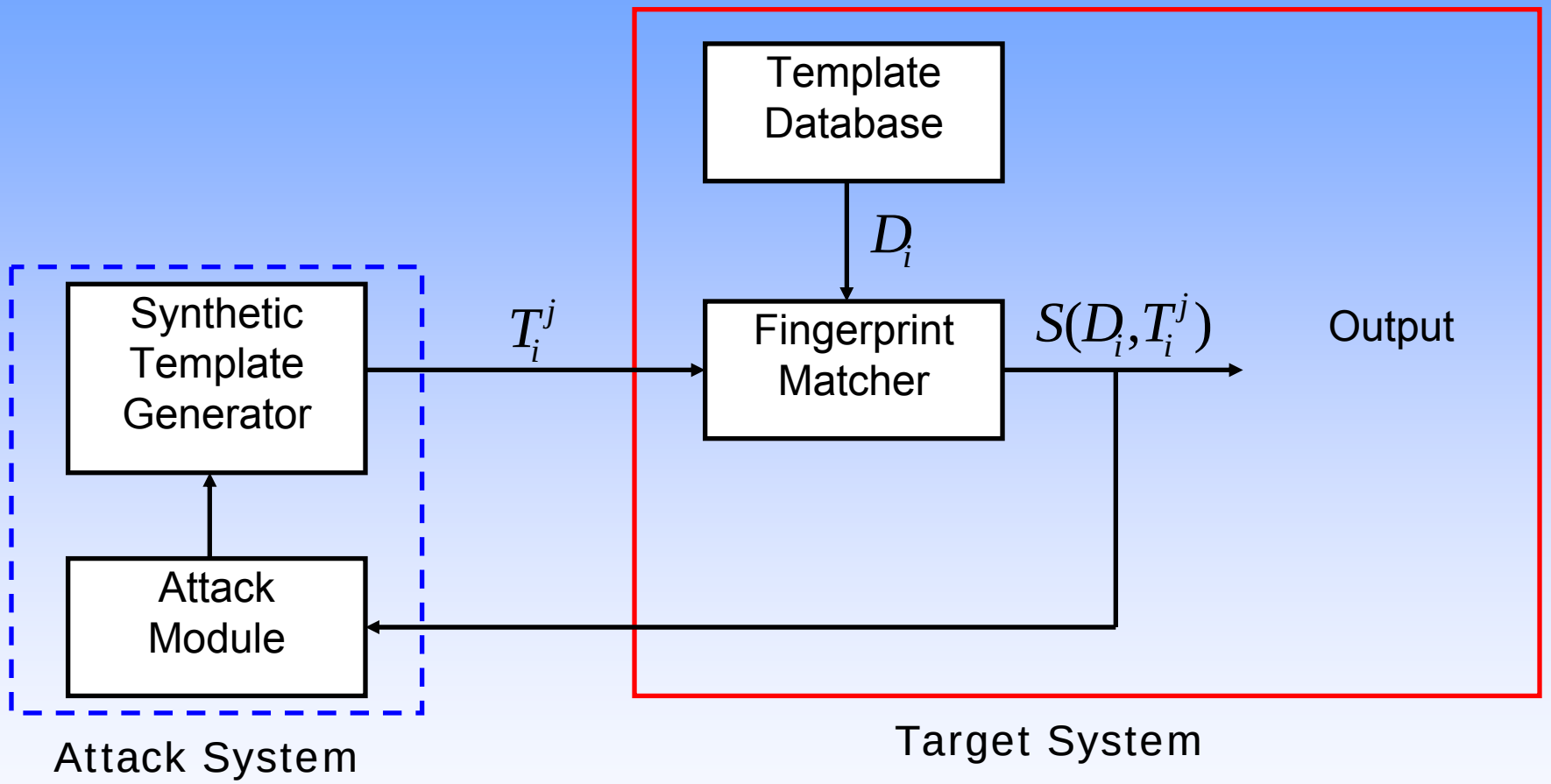


Spoof Detection Using Distortion Code



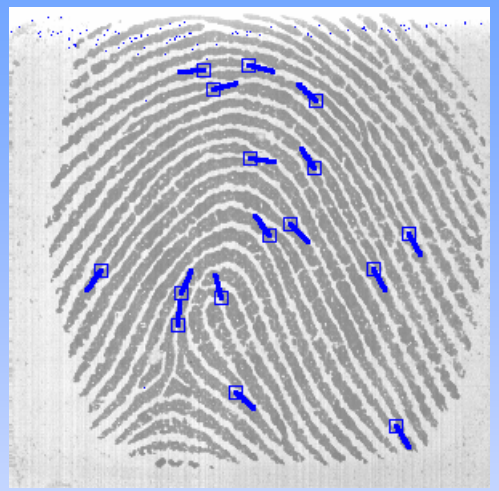
Antonelli et al., “Fake Finger Detection by Skin Distortion Analysis”, IEEE Trans. on TIFS, Vol. 1, No. 3, pp. 360-373, Sept. 2006

Hill-Climbing Attacks

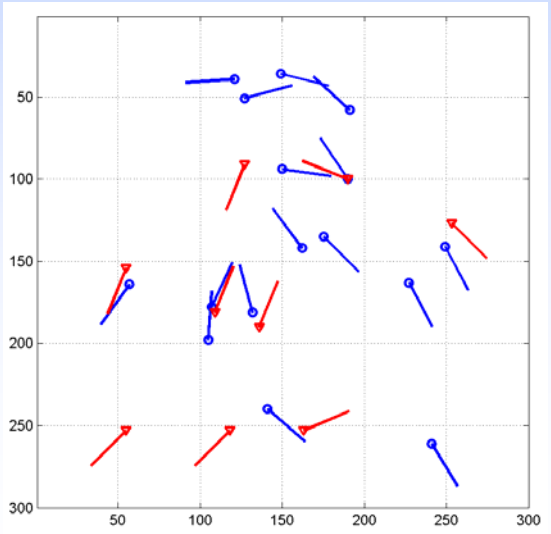


Bypass Feature Extractor: Inject random minutiae set and modify it iteratively to improve the matching score

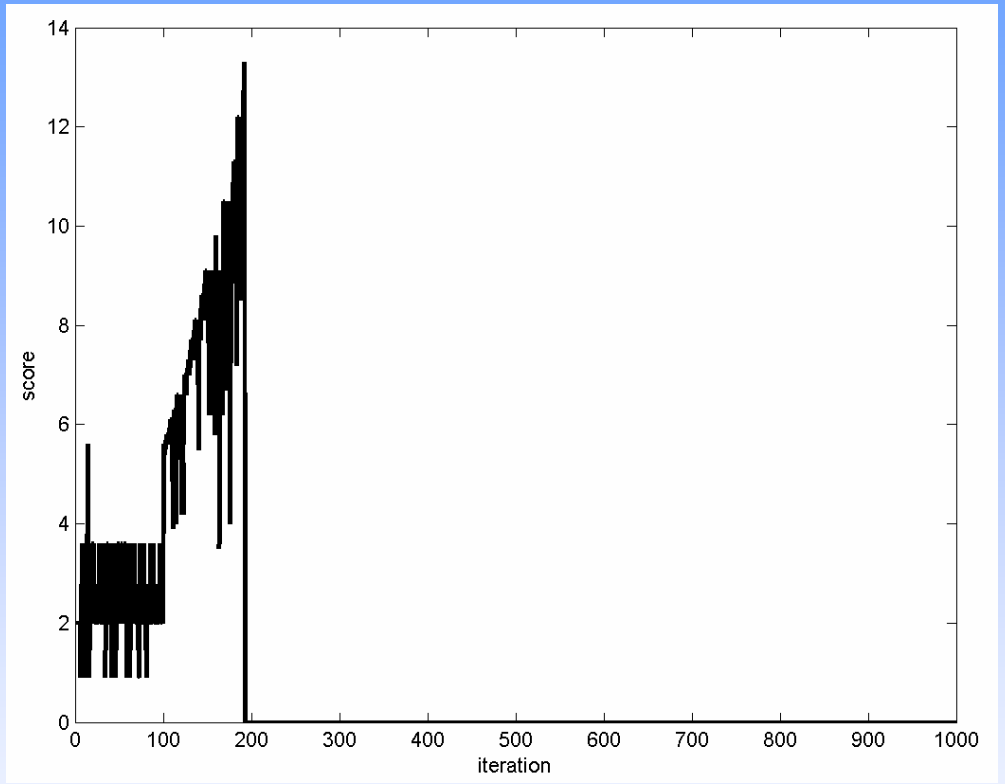
Injecting Random Minutiae Sets



Original image with minutiae



Synthetic (▽) and original (o) minutiae

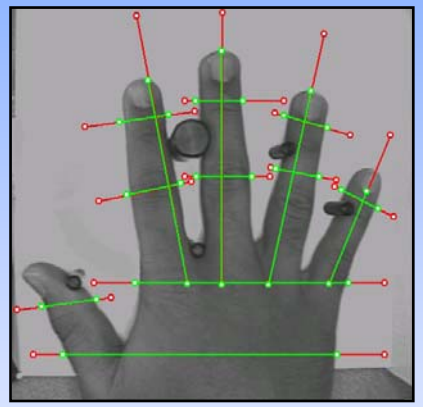


Progression of matching scores

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

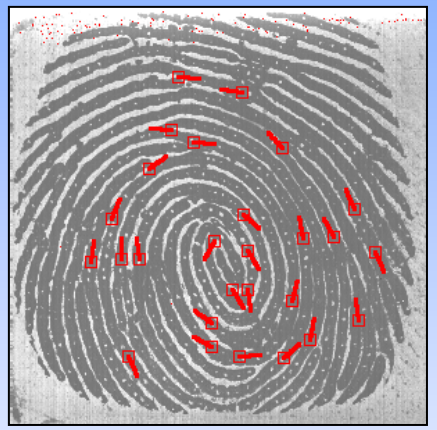
Biometric Template Protection

- 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.."

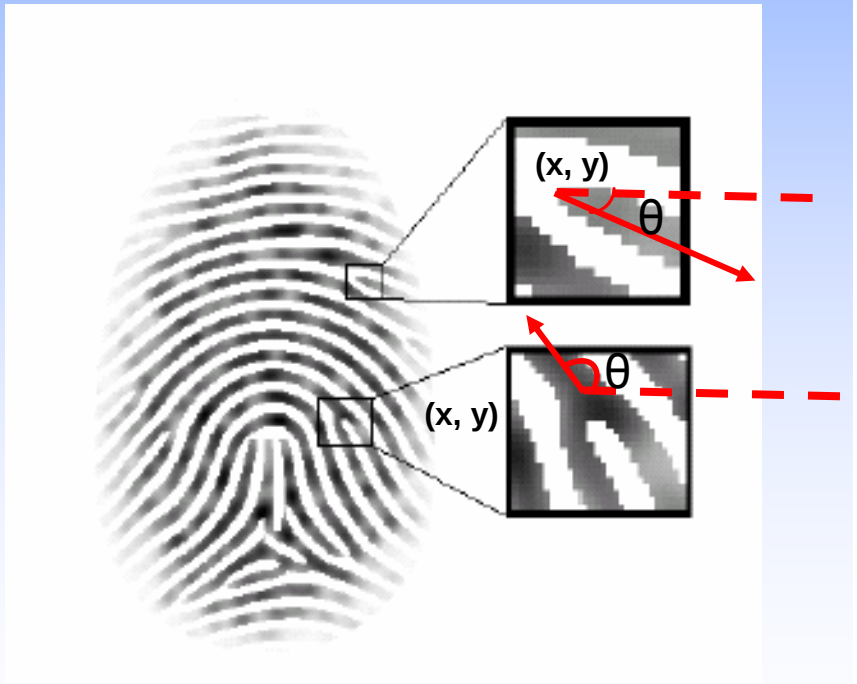
http://www.biometricaccess.com/support/bacfaq09.html
http://www.digitalpersona.com/support/faqs/privacy.html

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):

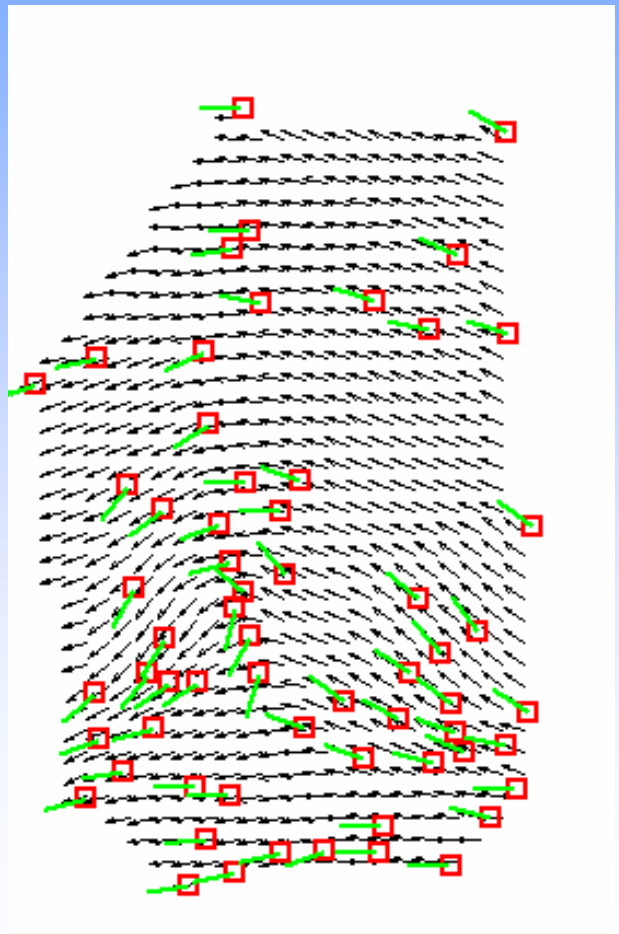
1. Estimate ridge flow
2. Predict class (A, L, R, W)
3. Reconstruct fingerprint



Orientation Estimation

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

Original fingerprint



Estimated orientation field

Fingerprint Reconstruction

Reconstructed images matched true fingerprints 23% of the time

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)

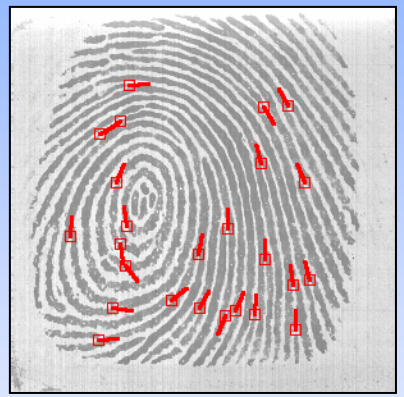
- Decrypt the template only when necessary with the appropriate decryption key, KD:

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!

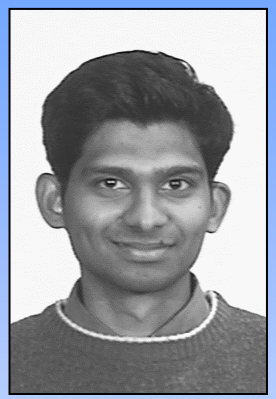
Hiding Minutiae in Face



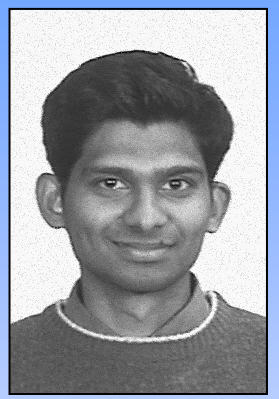
Minutiae

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

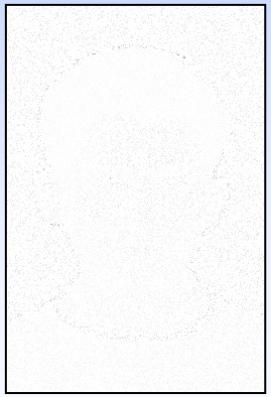
Minutiae attributes



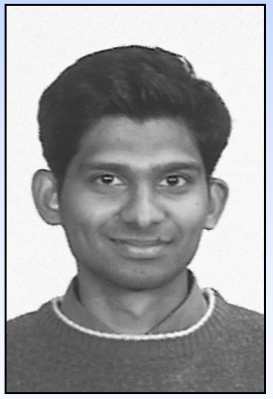
Host face image



Marked face image



Negative of difference image



Reconstructed face image

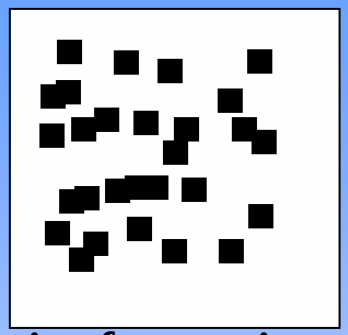
Hiding Eigenfaces in Fingerprints

input face

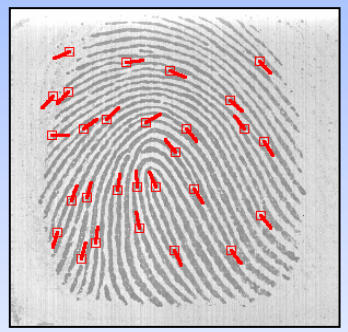
watermark face

-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 feature image



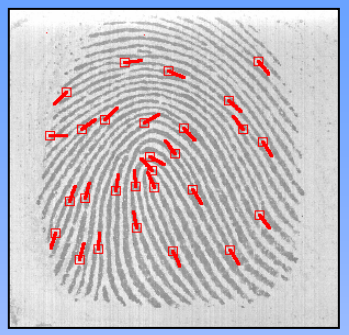
minutiae overlaid host fingerprint

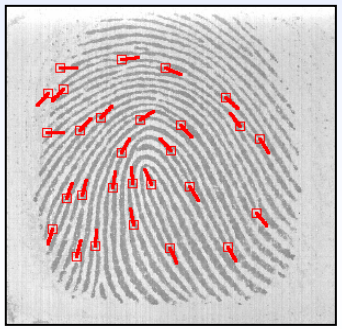
ridge feature image

watermarked image

reconstructed face

watermarked image

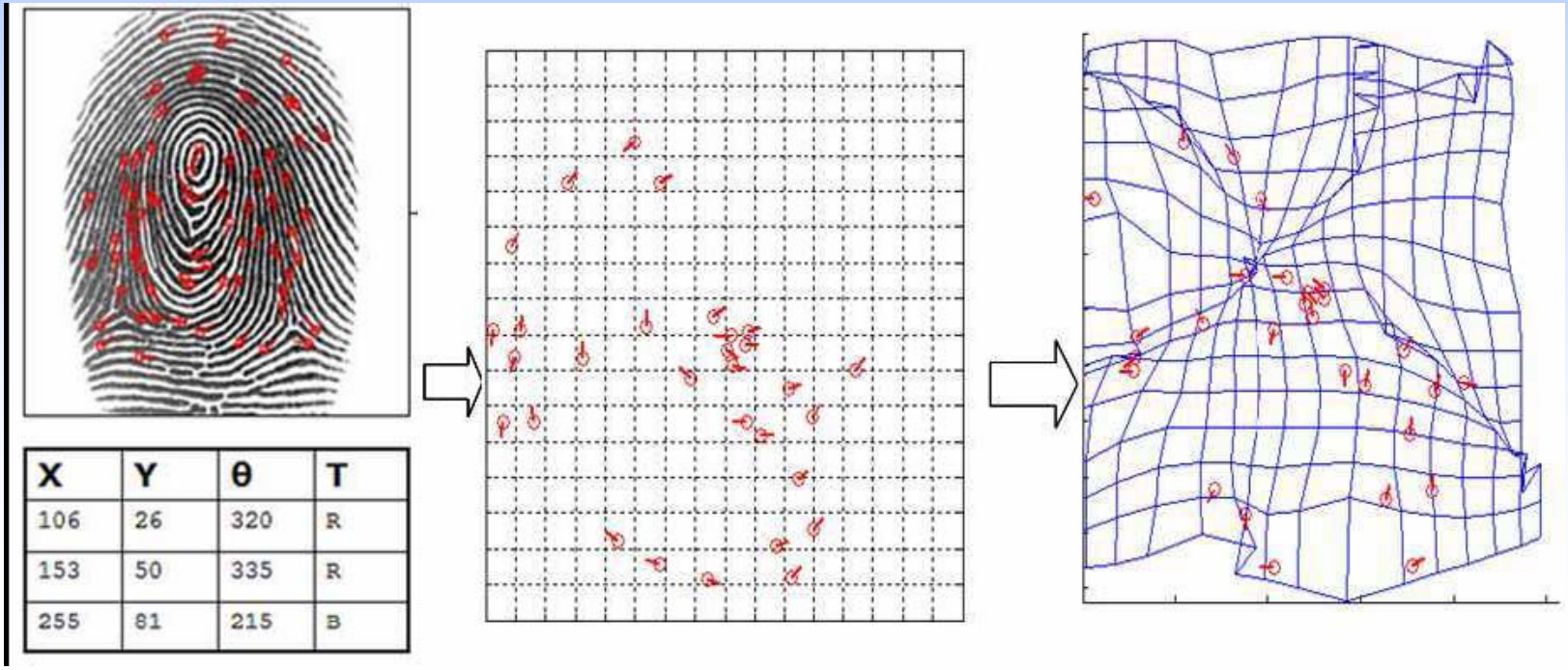




minutiae overlaid reconstructed fingerprint

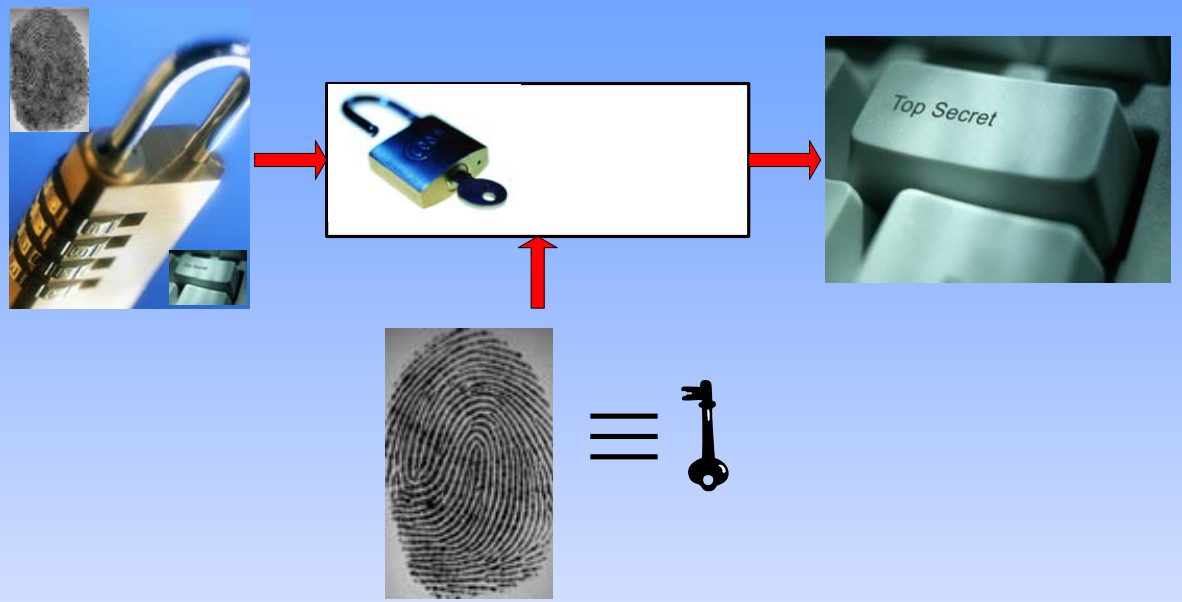
Cancelable Biometric Templates

- Apply repeatable but non-invertible transformations to the biometric template
- Every application can use different transformation parameters; this prevents functional creep (matching across databases) and improves privacy



X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B

Biometric Cryptosystems

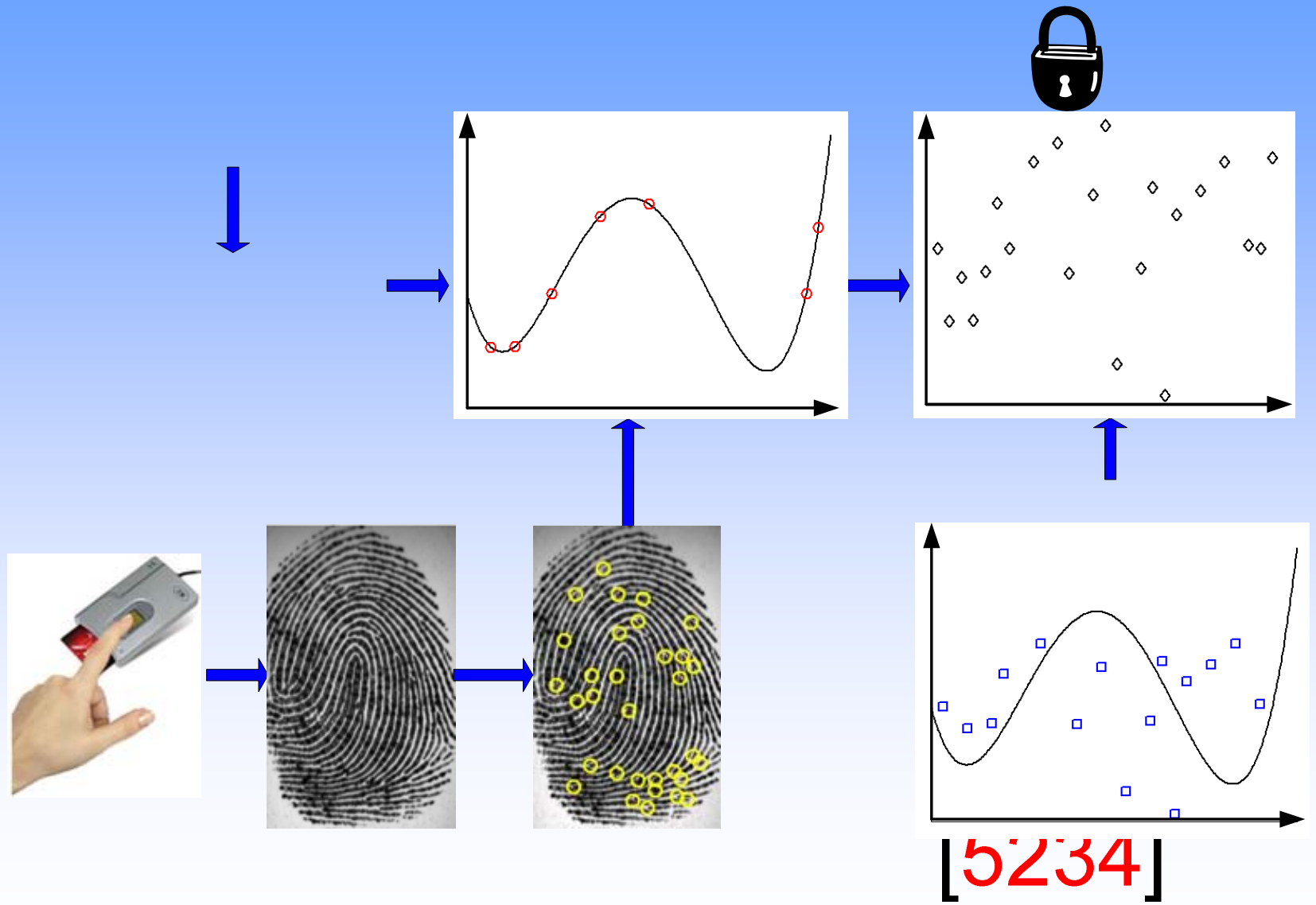


- Biometric template and secret key are monolithically bound within a cryptographic framework
- Infeasible to recover key or template without any knowledge of user's biometric data
- Key release implies successful authentication

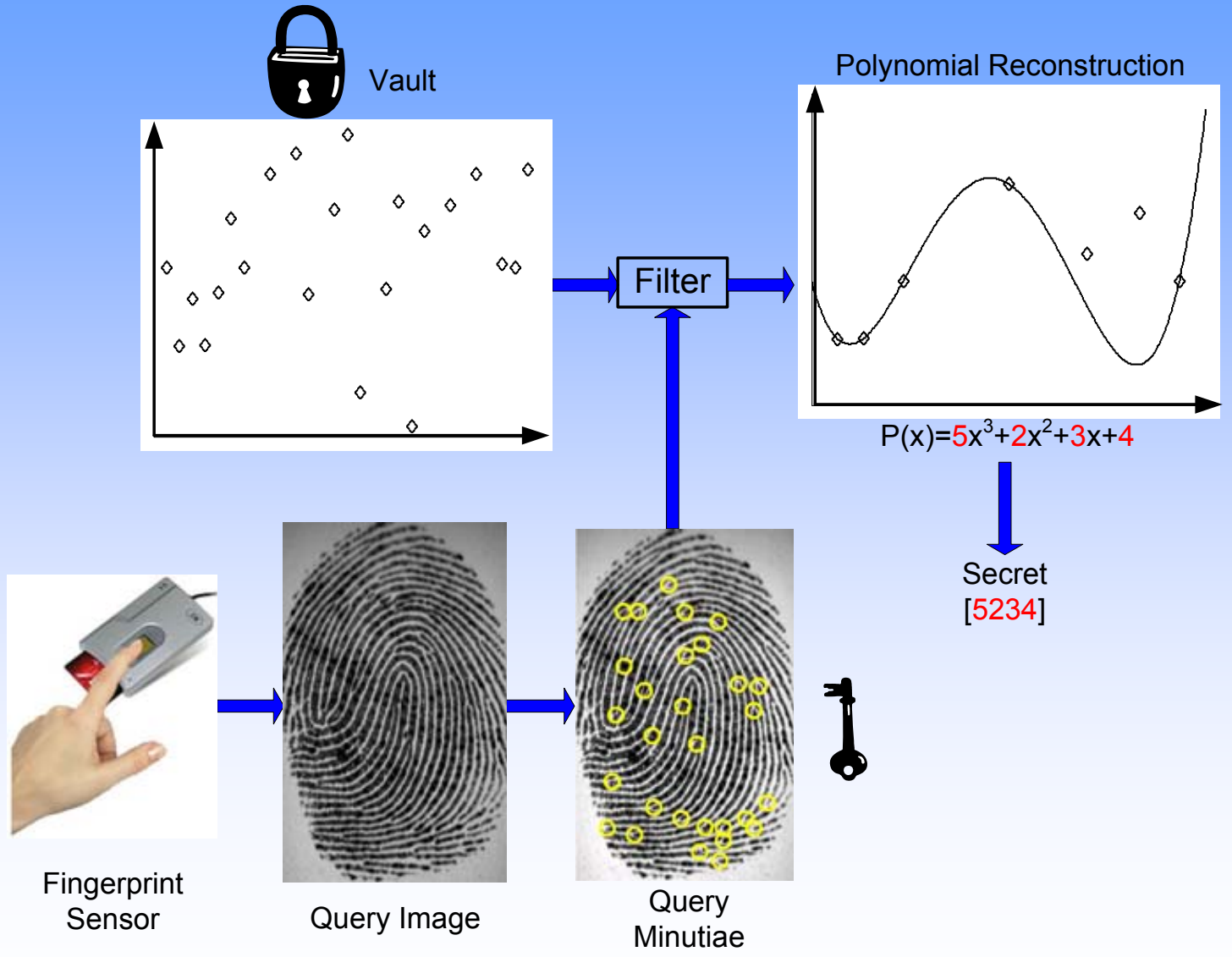
Fuzzy Vault (Juels & Sudan, 2002)

- Operates in the key binding mode
- The secret S is locked by a user's biometric (set X), resulting in a vault V
- To enhance security, set X is hidden in a large number of "chaff" points
- The decryption algorithm opens the vault if the presented biometric (set X') is sufficiently close to X
- In a fingerprint-based fuzzy vault, sets X and X' correspond to minutiae of template and query

Fuzzy Vault: Encoding



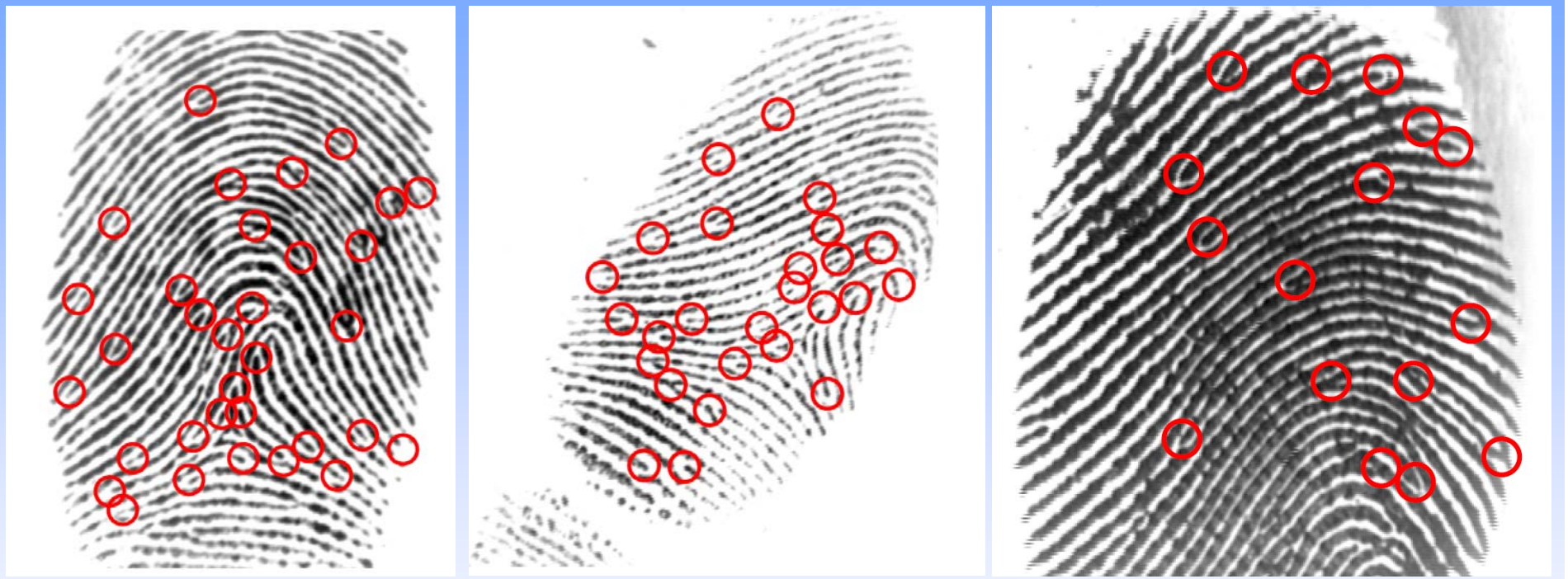
Fuzzy Vault: Decoding



Fingerprint-based Fuzzy Vault: Challenges

- Intra-class Variability
  - Query and template 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



Three different impressions of the same finger

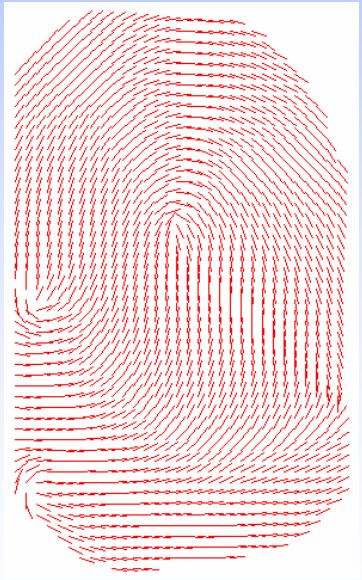
Alignment without Original Template

- Fuzzy vault stores only the transformed template; helper data needed for alignment
- Choice of helper data:
  - should not lead to template reconstruction
  - carry sufficient information for alignment
- Helper data: Attributes of high curvature points

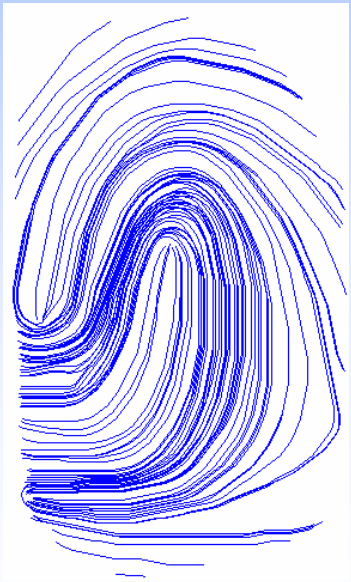
Helper Data Extraction

- Orientation field flow curve (OFFC): a set of piecewise linear segments whose tangent direction at each point is parallel to the orientation field direction
- Helper data: Local maxima of OFFC curvatures

Fingerprint Image



Orientation Field



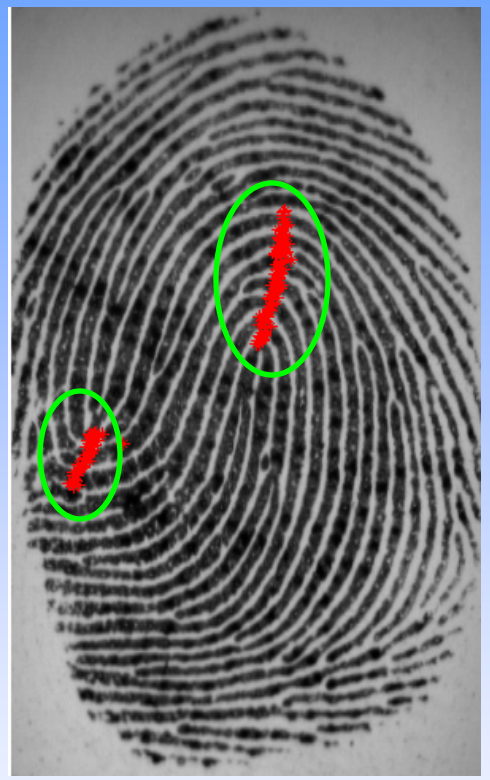
Flow Curves

High Curvature Points

Helper Data Examples

Row	Col	Curv
212	138	1.68
208	141	1.51
206	142	1.42
205	140	1.47
⋮		

Template



Query

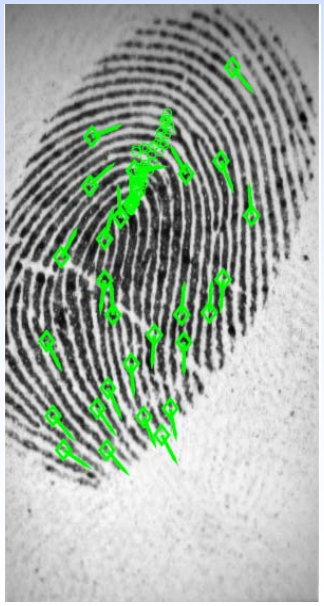
228	155	1.57
228	157	1.55
226	159	1.46
⋮		
318	40	0.77
316	37	0.76
317	43	0.75
⋮		

Clustering identifies multiple clusters in helper data

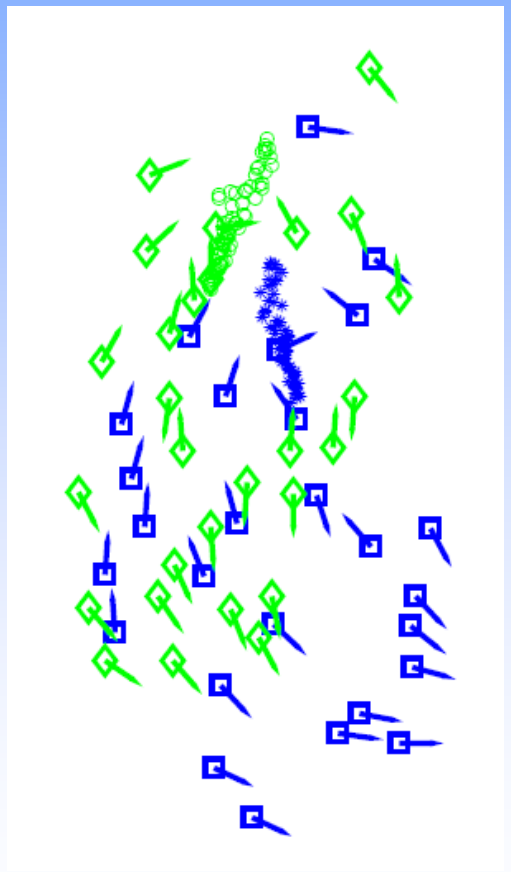
Alignment Using Helper Data

Template

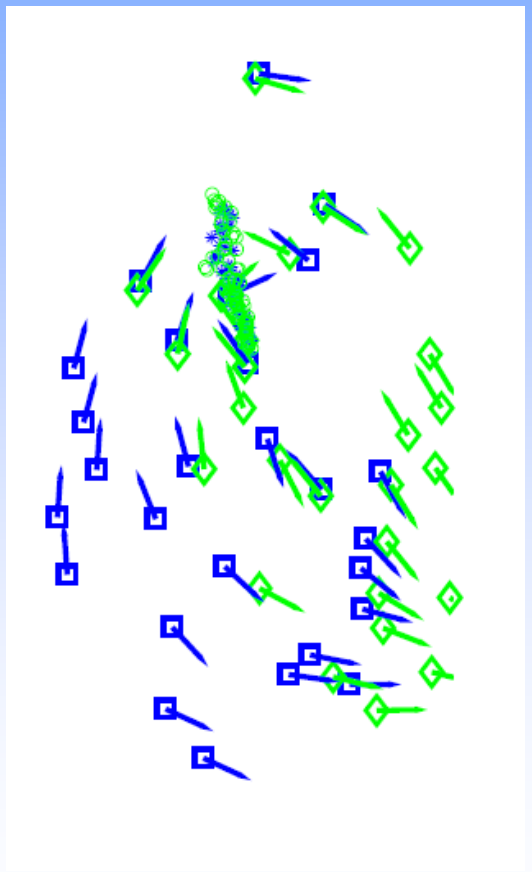
Query



Before alignment

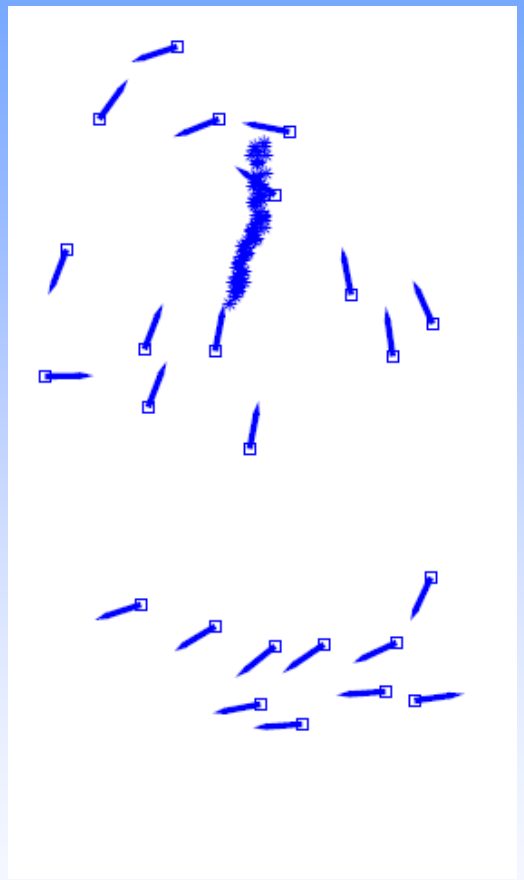


After ICP alignment

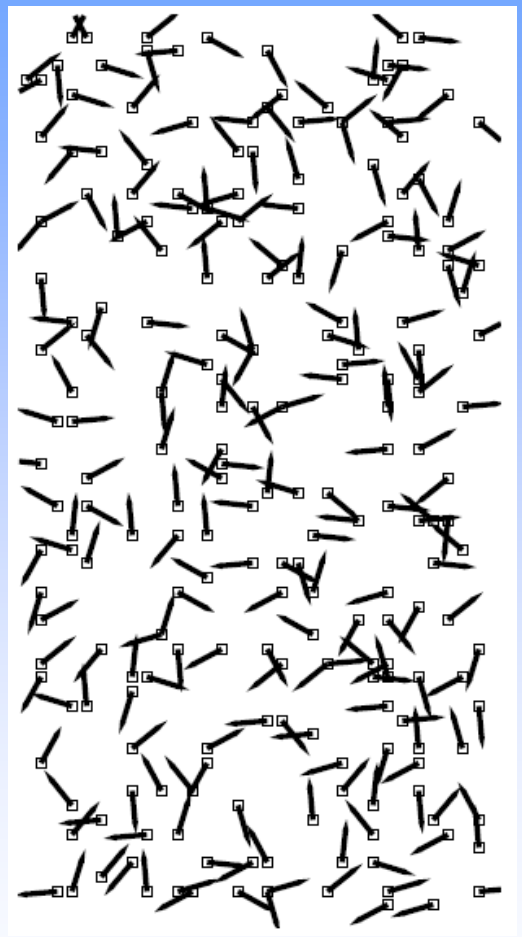


Fingerprint Vault Encoding

Template
Fingerprint Image
With Minutiae



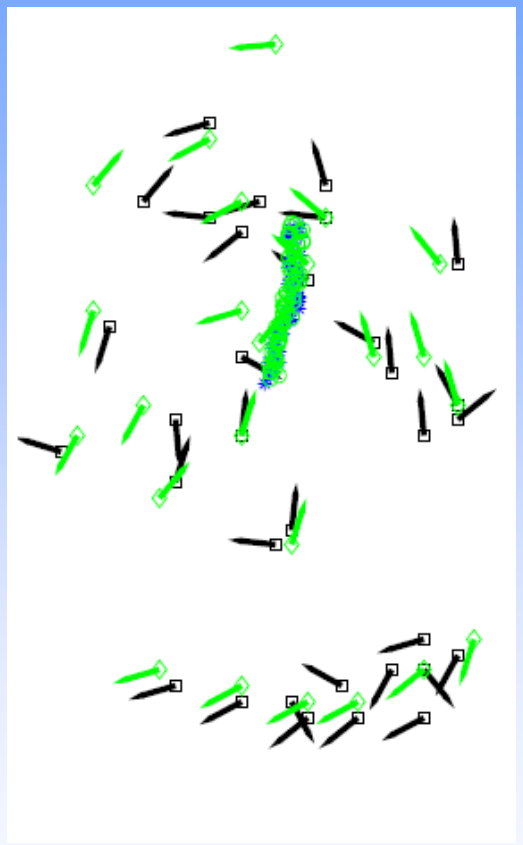
Selected Template
Minutiae and
Helper Data



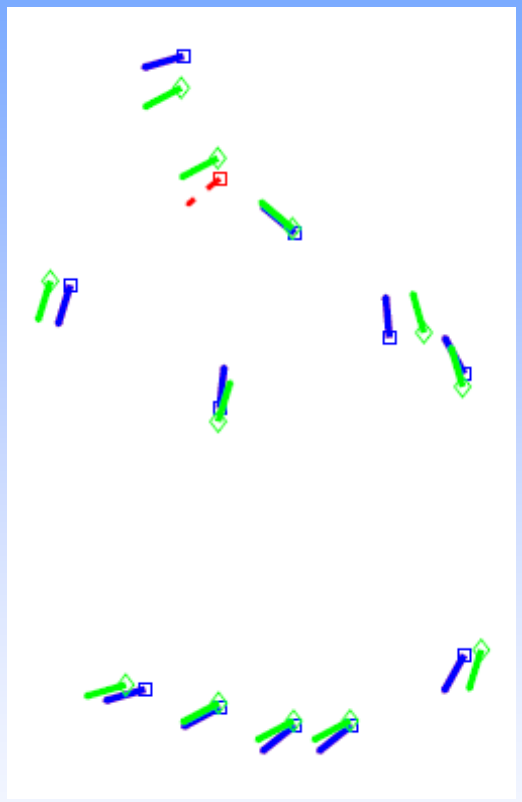
Selected Template
Minutiae Hidden
Among Chaff Points

Fingerprint Vault Decoding

Query Fingerprint
Image With Minutiae



ICP Alignment and
Coarse Filtering



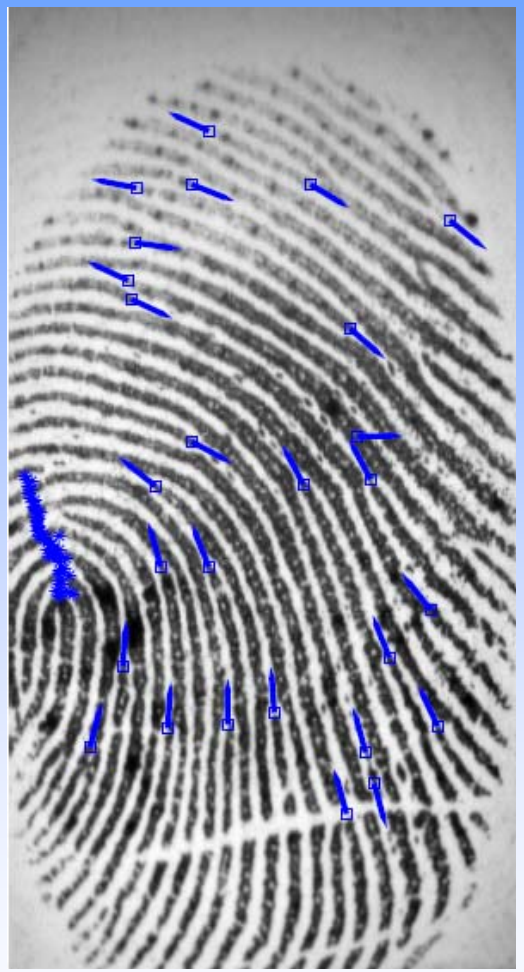
Unlocking Set After
Minutiae Matching

Fingerprint Fuzzy Vault Performance

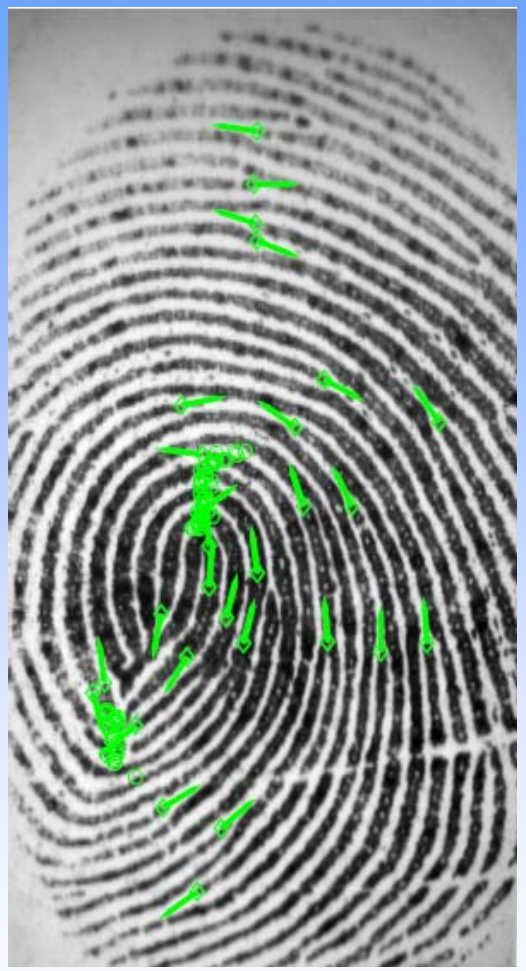
- FVC 2002 Database 2: 569 dpi images (optical); 18-24 genuine minutiae, > 200 chaff points

		Key Size = 128 bits		Key Size = 160 bits	
Scenario	FTAR (%)	GAR (%)	FAR (%)	GAR (%)	FAR (%)
1 Template, 1 Query	2	91	0.01	86	0
Mosaiced Template, 1 Query	1	94	0.02	88	0
Mosaiced Template, 2 Queries	1	96	0.04	90	0

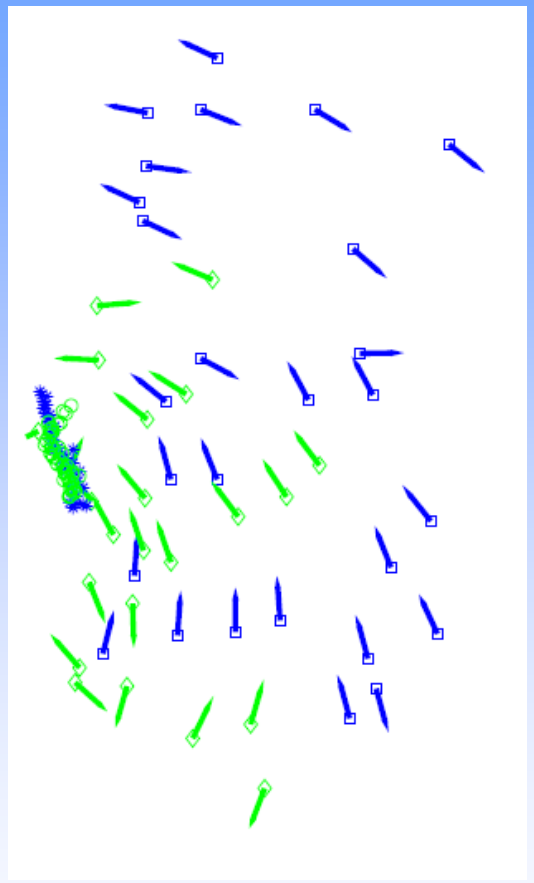
False Reject - Incorrect Helper Data



Template



Query



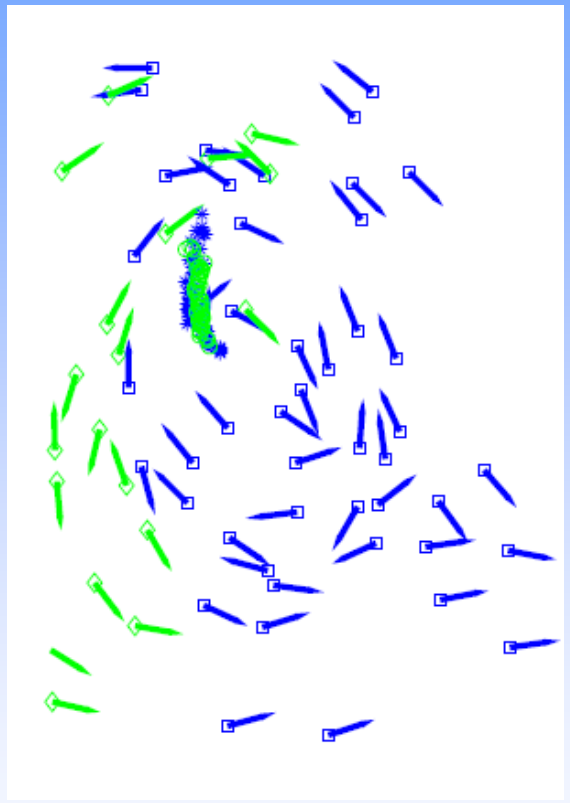
After ICP alignment

Helper data incorrectly extracted in template because core is near the image boundary

False Reject – Partial Overlap

Template

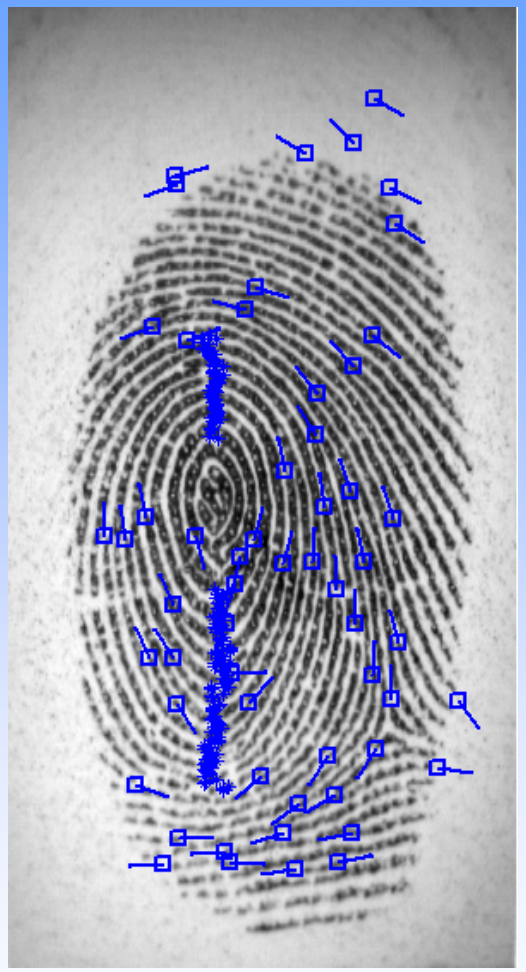
Query



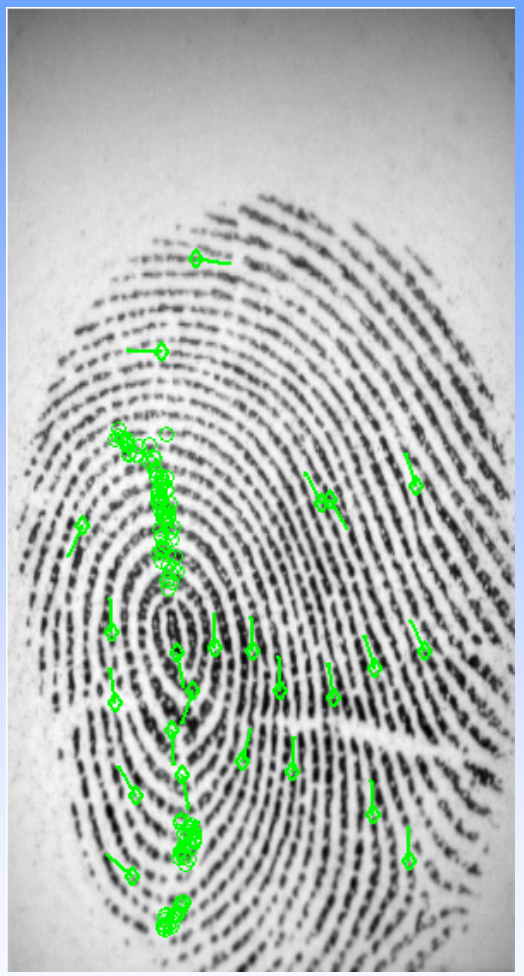
After ICP alignment

Template and query have small number of overlapping minutiae

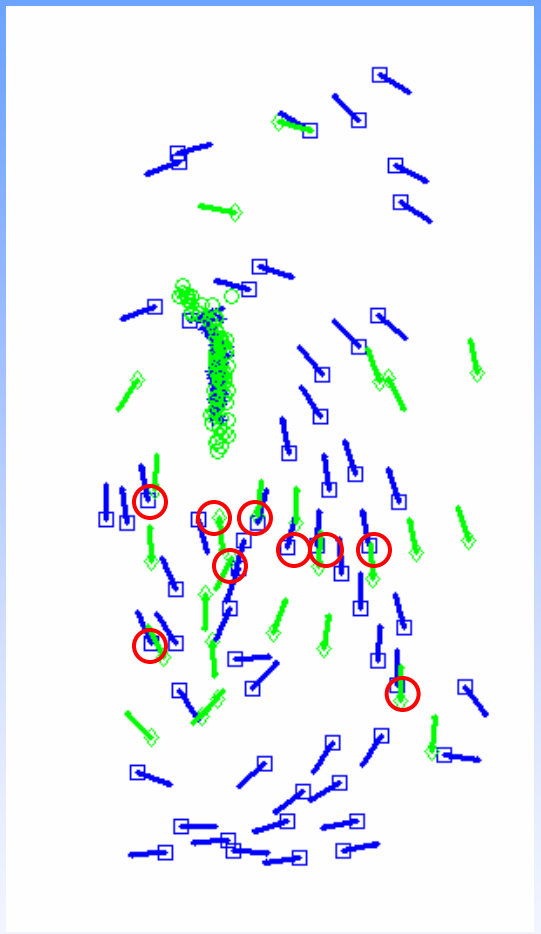
Example of False Accept



Template



Query



After ICP alignment

Template and query have 9 overlapping minutiae

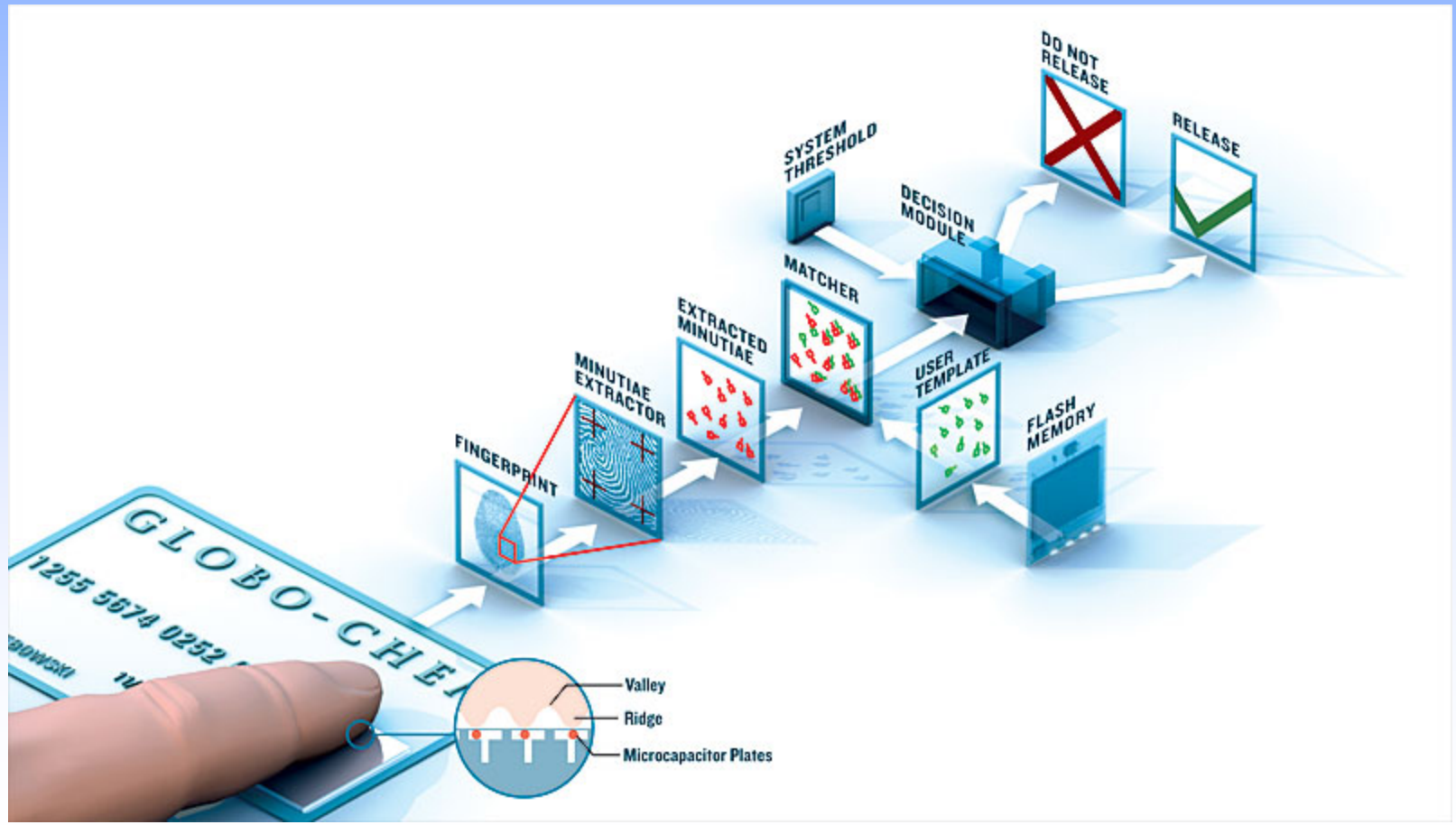
Britain's Identity Crisis

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"

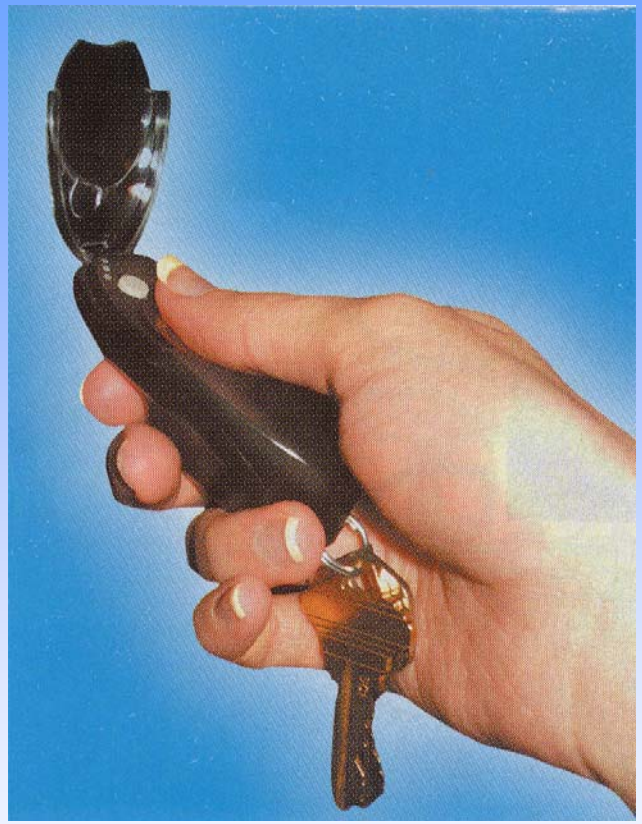
Match on Card

Complete system (sensor, feature extractor, matcher, template) resides on card; template is never transmitted or released from card



Decentralization of Templates

Biometric Smart Card
(UPEK Inc.)



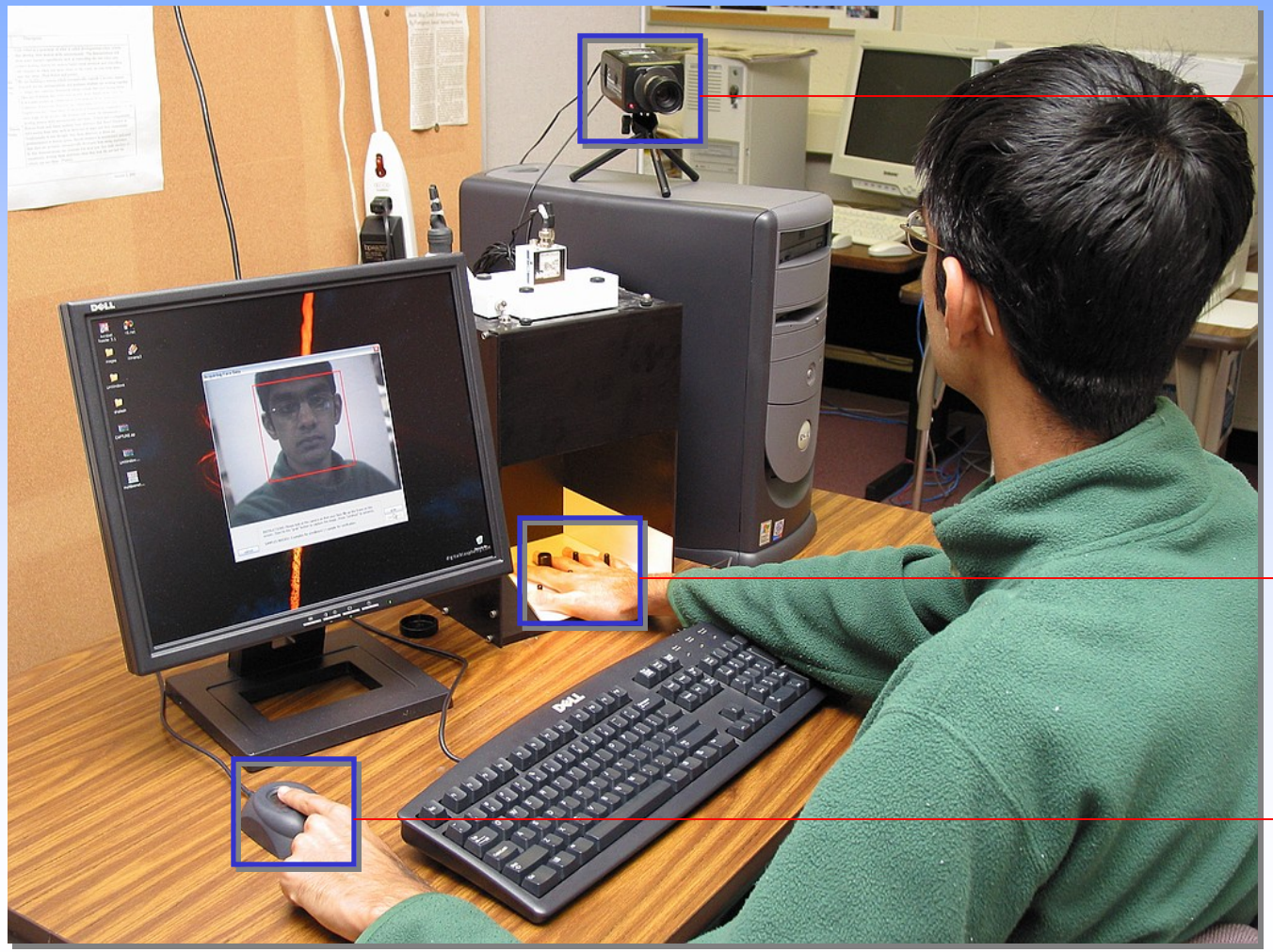
Biometric Key Chain
(Privaris, Inc.)

Other Attacks

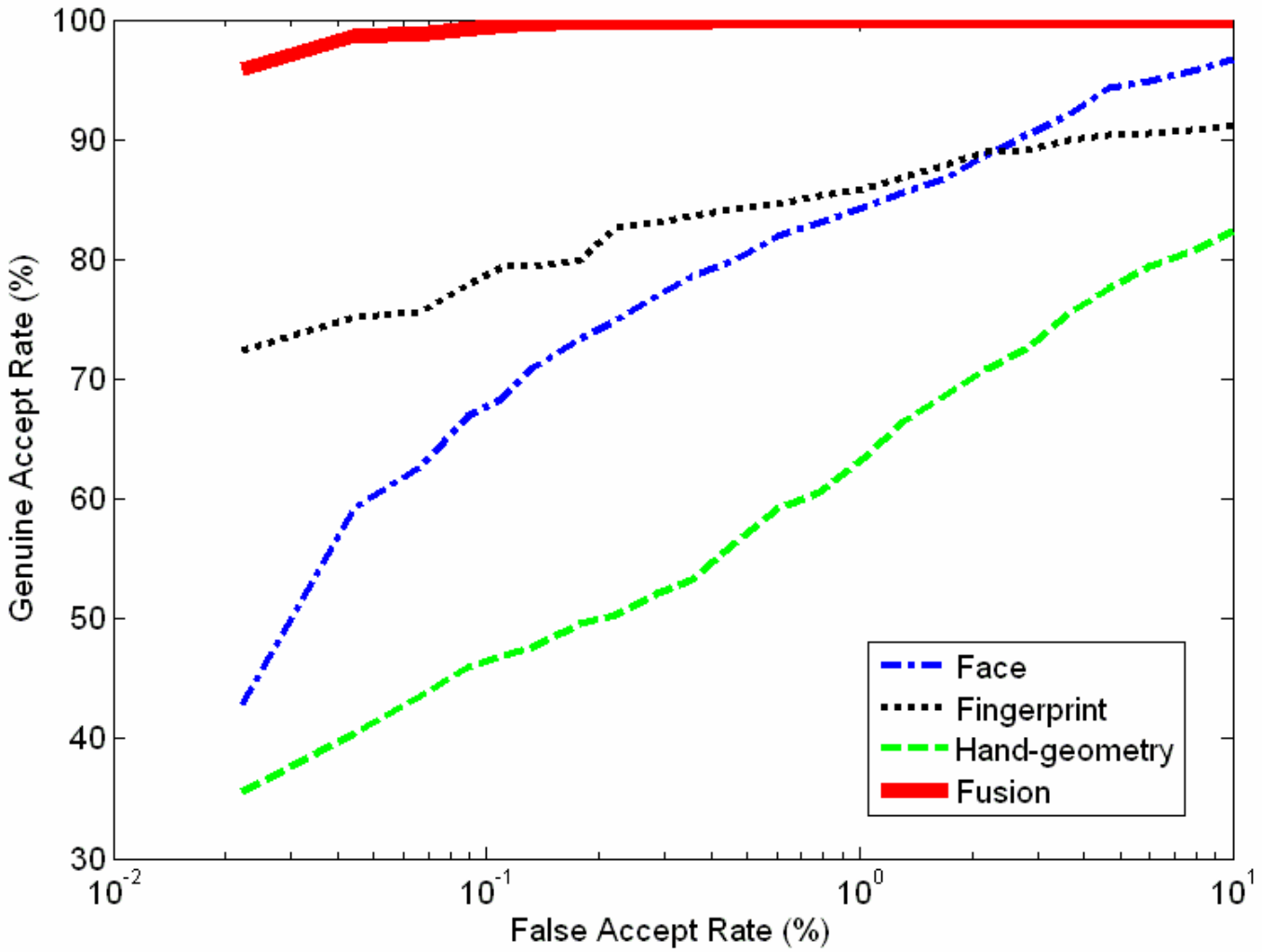
- Insider attacks
- Integrity of the enrollment process
- Once initial access is granted, an impostor can spoof the system in the absence of real-time continuous authentication
- Exception handling may introduce a weak link
- By providing poor quality images at input
- Biometrics is made ineffective 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 10 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