Biometric Authentication: How Do I Know Who You Are?

Anil K. Jain

Dept. of Computer Science and Engineering

Michigan State University

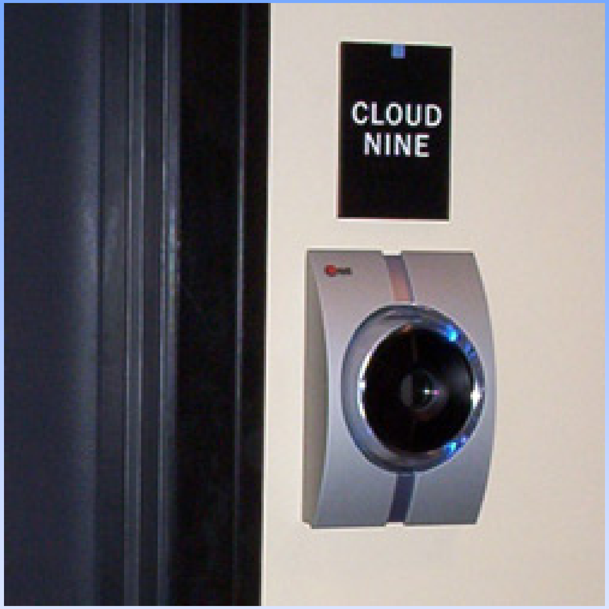
http://biometrics.cse.msu.edu

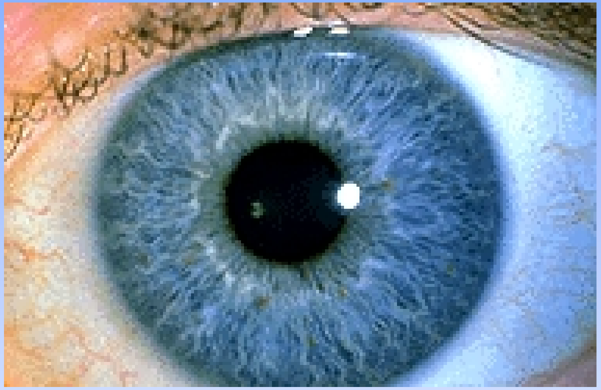
Fingerprint System at Gas Stations

“Galp Energia SGPS SA of Lisbon won the technology innovation award for developing a payment system in which gasoline-station customers can settle their bills simply by pressing a thumb against a glass pad. Scanning technology identifies the thumbprint and sends the customer's identification information into Galp's back-office system for payment authorization.”

THE WALL STREET JOURNAL, November 15, 2004

Using Iris Scans to Unlock Hotel Rooms





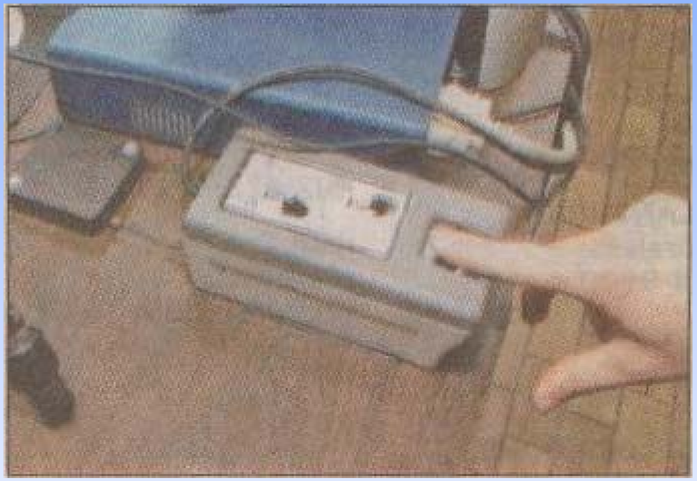
The Nine Zero hotel in Boston just installed a new system which uses digital photos of the irises of employees, vendors and VIP guests to admit them to certain areas, the same system used in high-security areas at airports such as New York's JFK.

USA TODAY 7/22/2004

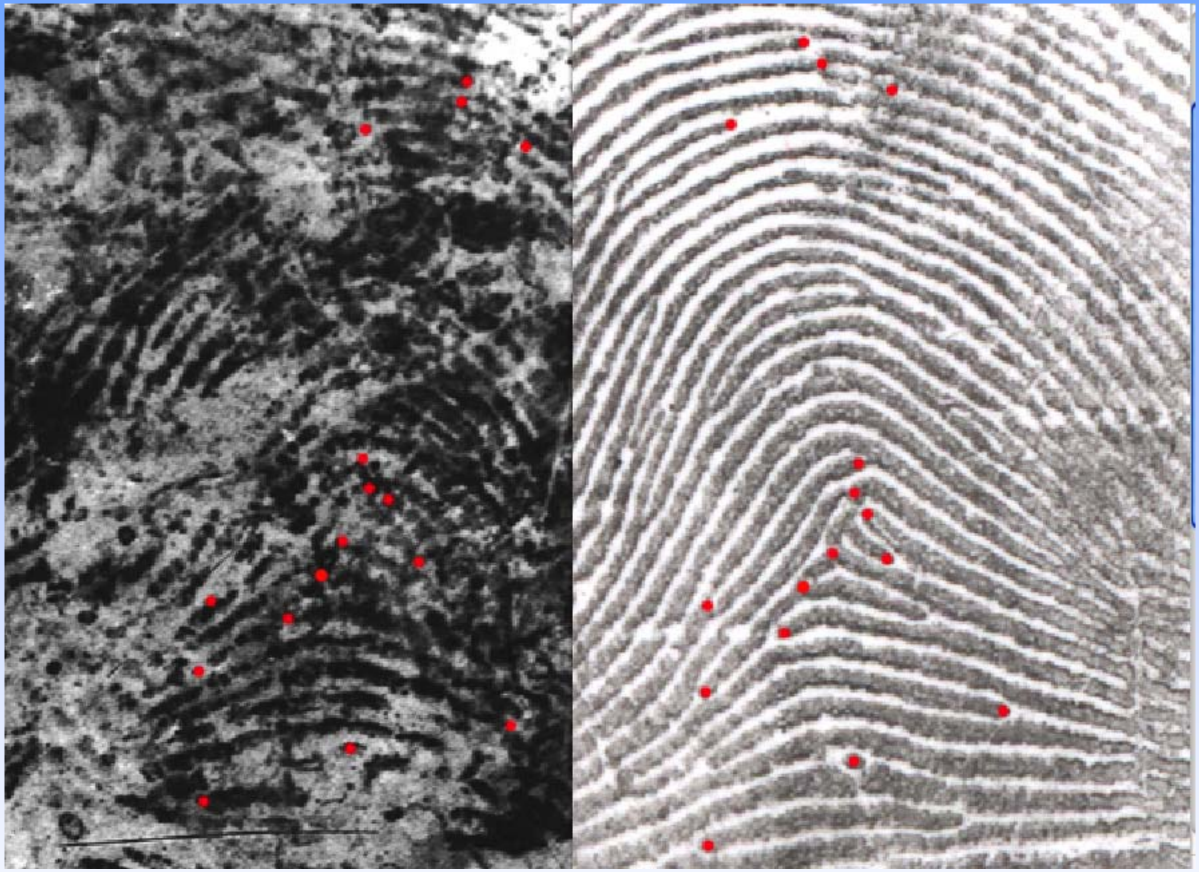
Fingerprint System at Border Crossings

"Foreigners entering the United State in three cities, including Port Huron, were fingerprinted, photographed and subjected to background checks on Monday in a test of a program that will eventually be extended to every land border crossing nationwide."

Lansing State Journal, Nov. 16, 2004



Mayfield Fingerprint



U.S. and Spanish authorities told reporters Mayfield's fingerprints matched those found on a bag discovered near the bombing site in Spain. Mayfield was later released after Spanish law enforcement officials said they had matched fingerprints on the plastic bag to an Algerian man

Outline

- Identity Problems
- Biometric Recognition
  - Applications
  - Modalities
  - Challenges
- Fingerprint Recognition
  - Representation
  - Matching
  - Individuality
- Multimodal Biometrics
- Biometric System Vulnerabilities

Identity Problems

Security Threats:

We now live in a global society of increasingly desperate and dangerous people whom we can no longer trust based on identification documents which may have been compromised

Senator? Terrorist? A Watch List Stops Kennedy at Airport: Senator Edward M. Kennedy, Democrat of Mass., discussed the problems faced by ordinary citizens mistakenly placed on terrorist watch lists. Between March 1 and April 6, airline agents tried to block Mr. Kennedy from boarding airplanes on five occasions because his name resembled an alias used by a suspected terrorist who had been barred from flying on airlines in the United States. RACHEL L. SWARNS, NY Times, Aug 20, 2004

Identity Problems

Identity Theft: Identity thieves steal PIN (e.g., date of birth) to open credit card accounts, withdraw money from accounts and take out loans

3.3 million identity thefts in U.S. in 2002; 6.7 million victims of credit card fraud

Surrogate representations of identity such as passwords and ID cards no longer suffice

Too Many Passwords to Remember!

Copyright 1996 Randy Glasbergen. www.glasbergen.com
GLASBERGEN
"Sorry about the odor. I have all my passwords tattooed between my toes."

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

Biometrics

- AAutomatic recognition of people based on their distinctive anatomical (e.g., face, fingerprint, iris, retina, hand geometry) and behavioral (e.g., signature, gait) characteristics

- RRecognition of a person by their body, then linking that body to an externally established "identity", forms a very powerful tool

↔ *John Smith*

Biometric Functionalities

- Positive Identification

  Is this person truly known to the system?

  Provide log-in access to a valid user

- Large Scale Identification

  Is this person in the database?

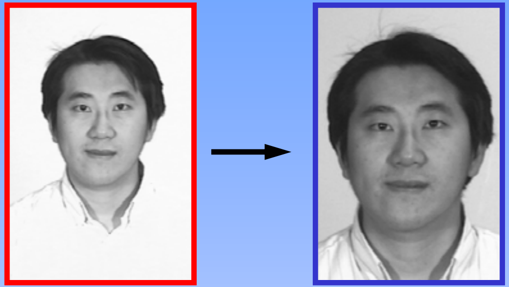
  Prevent issuing multiple driver licenses to the same person

- Screening

  Is this a wanted person?

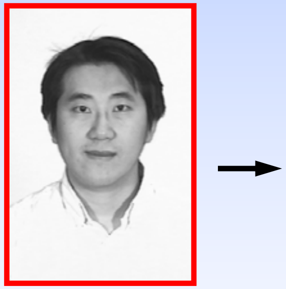
  Airport watch-list

Only biometrics can provide negative identification (i.e., I am not he) capability

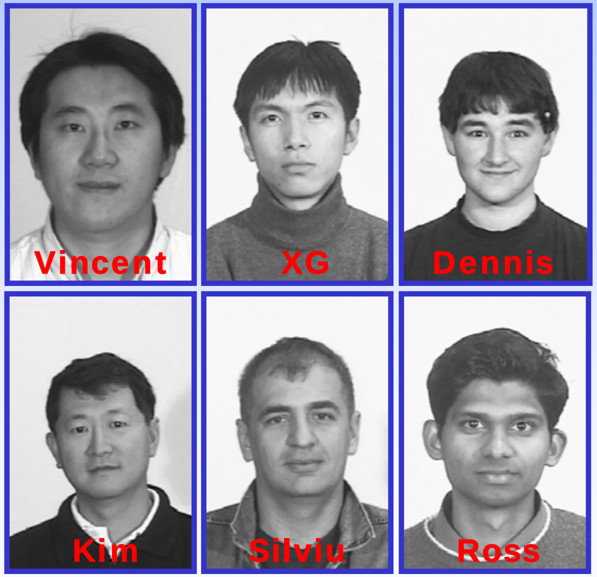


Query image (Vincent)

Template image (Vincent)



Query image



Biometrics is Not New!

- Bertillon system (1882) took a subject's photograph, and recorded height, the length of one foot, an arm and index finger
- Galton/Henry system of fingerprint classification adopted by Scotland Yard in 1900
- FBI set up a fingerprint identification division in 1924
- AFIS installed in 1965 with a database of 810,000 fingerprints
- First face recognition paper published in 1971 (Goldstein et al.)
- FBI installed IAFIS in ~2000 with a database of 47 million 10 prints; average of 50,000 searches per day; ~15% of searches are in lights out mode; 2 hour response time for criminal search

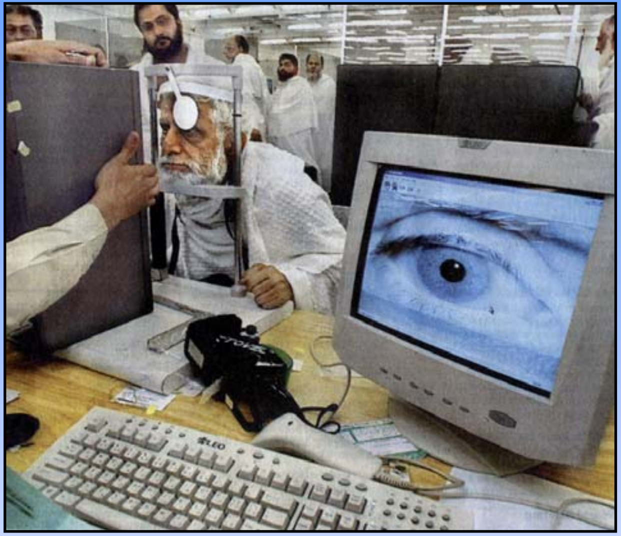
Emphasis now is to automatically perform reliable person identification in unattended mode, often remotely (or at a distance)

Biometric Applications

Forensic	Government	Commercial
Corpse Identification	National ID Card Biometric passport	ATM Internet Banking
Criminal Investigation	Driver's License Voter Registration	Access Control Computer Login
Parenthood Determination	Welfare Disbursement	Cellular Phone
Missing Children	Border Crossing* US-VISIT program	E-commerce Smart Card

* There are ~500 million border crossings/year in the U.S.

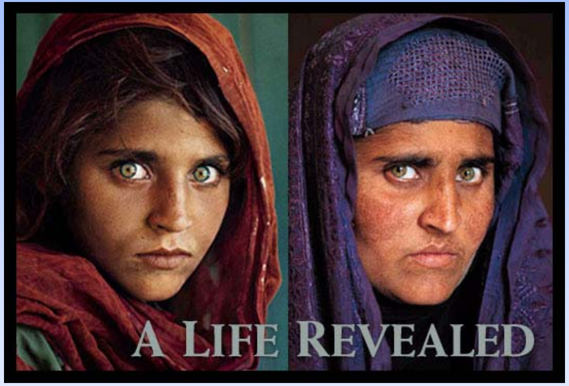
Biometric Applications



Haj pilgrims in Saudi Arabia

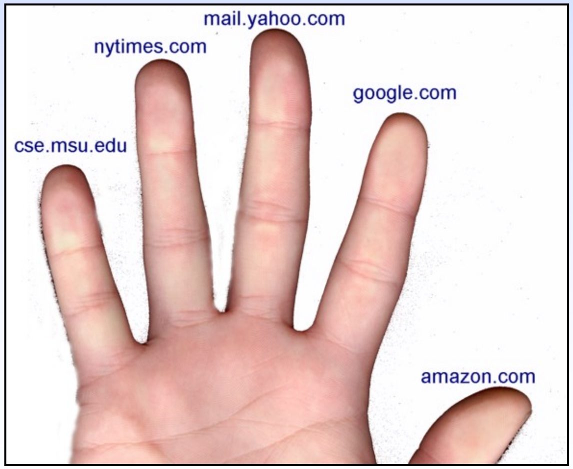
Point of sale

Disney World



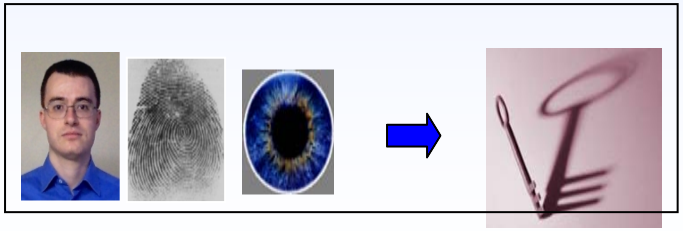
Sharbat Gula in 1985, 1992

Iris-based ATM



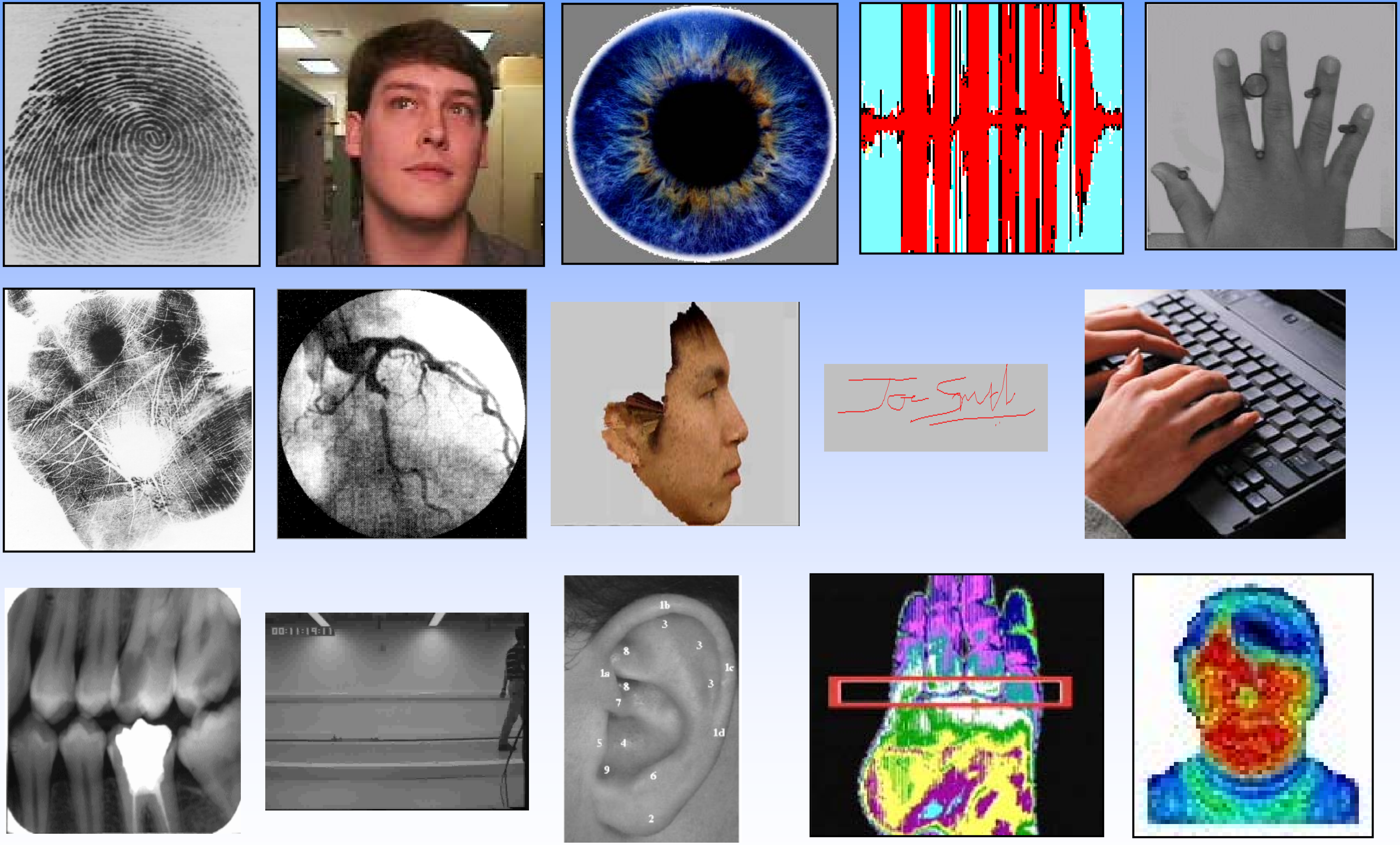
URL at your fingertip

Mobile phone



Secure multimedia

Biometric Characteristics



A scanner Delves Beneath Fingerprints

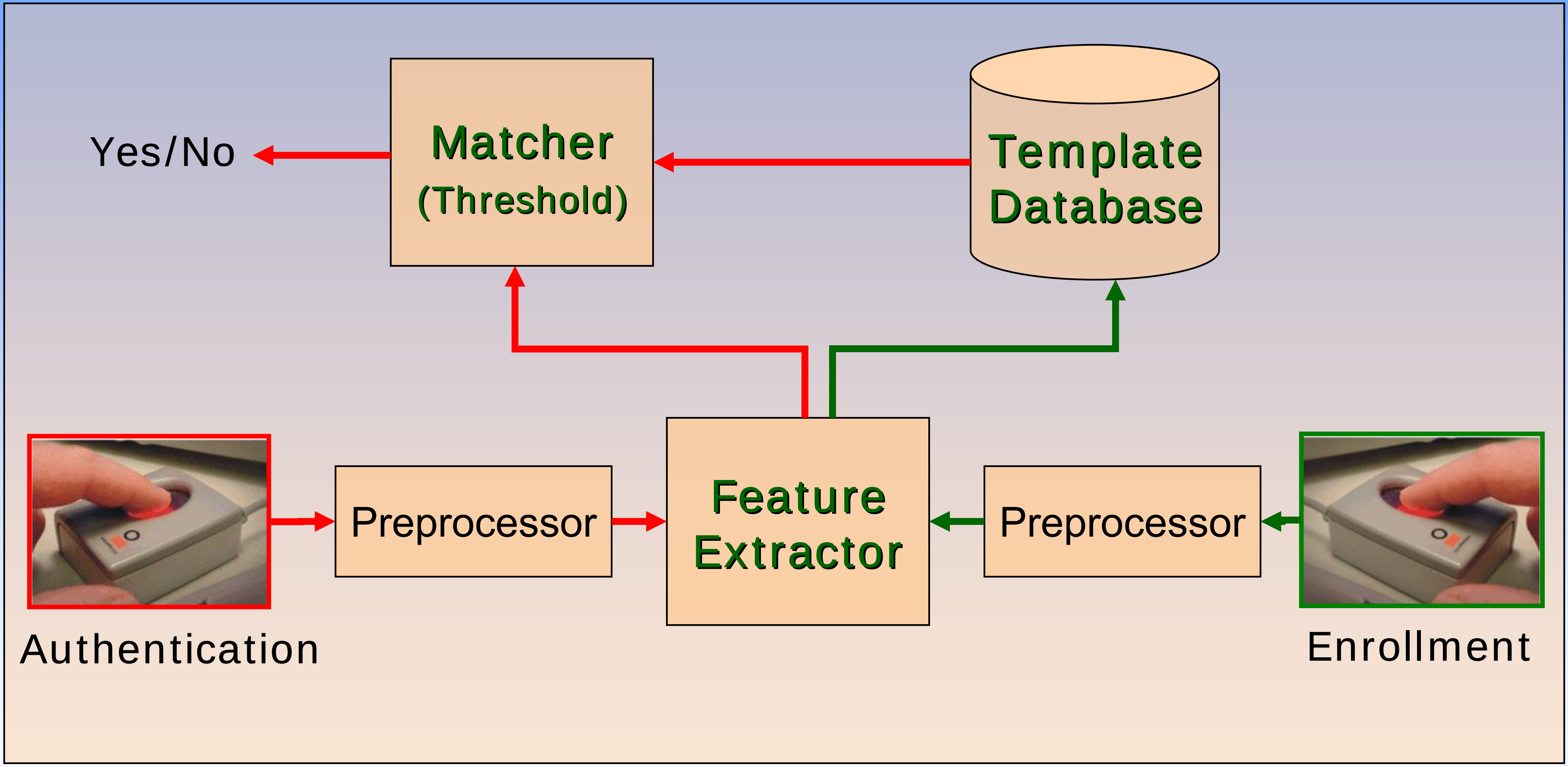
The patterns in your blood vessels are yours alone! Spectral signature by Lumidigm is obtained by illuminating the skin by polarized light in five different wavelengths

Which Biometric is the Best?

- **Universality** (all users possess this biometric)
- **Uniqueness** (varies across users)
- **Permanence** (does not change over time)
- **Collectability** (can be measured quantitatively)
- **Performance** (low error rates and processing time)
- **Acceptability** (is it acceptable to the users?)
- **Circumvention** (can it be easily spoofed?)

No biometric modality is optimal

Biometrics: A Pattern Recognition System

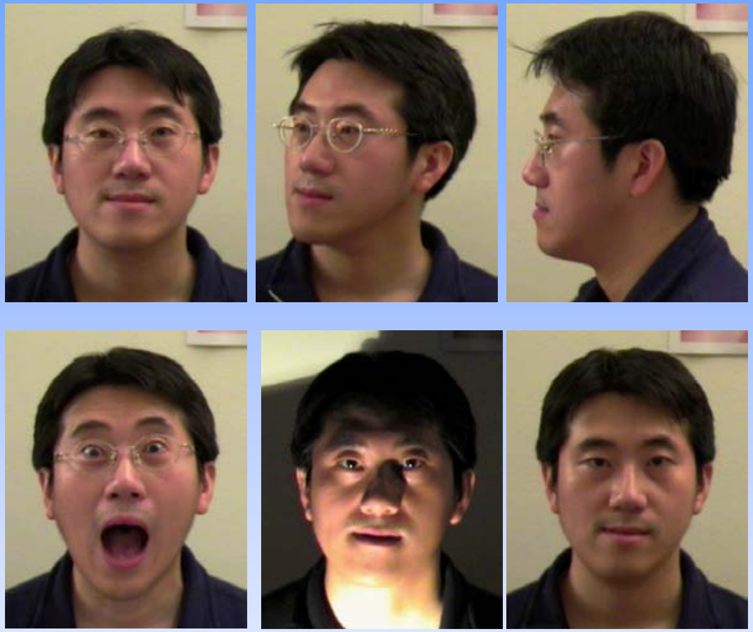


- False accept rate (FAR): Proportion of imposters accepted
- False reject rate (FRR): Proportion of genuine users rejected
- Failure to enroll rate
- Failure to acquire rate

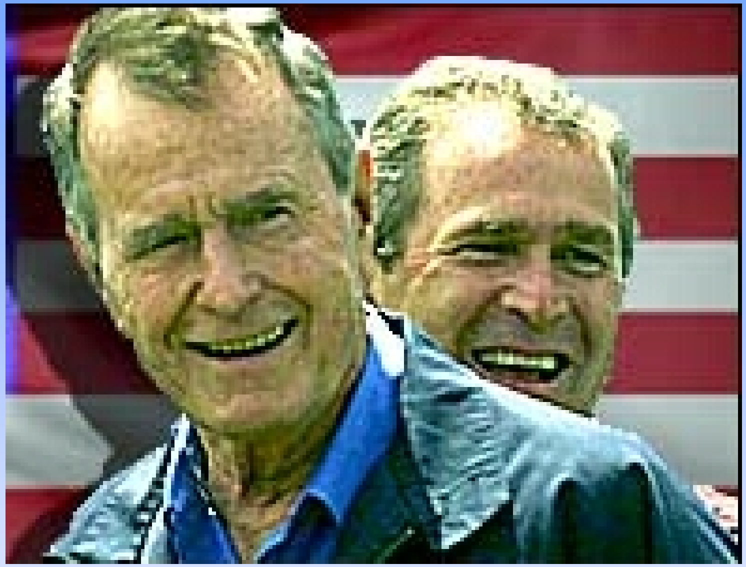
Why is Biometrics so Difficult?

- Intra-class variability and inter-class similarity
- Segmentation
- Noisy input & population coverage
- Individuality of biometric characteristics
- Scalability
- Template aging and update

Intra-class and Inter-class Variations



Variability observed in the face idue to change in pose, expression, lighting and eye glasses

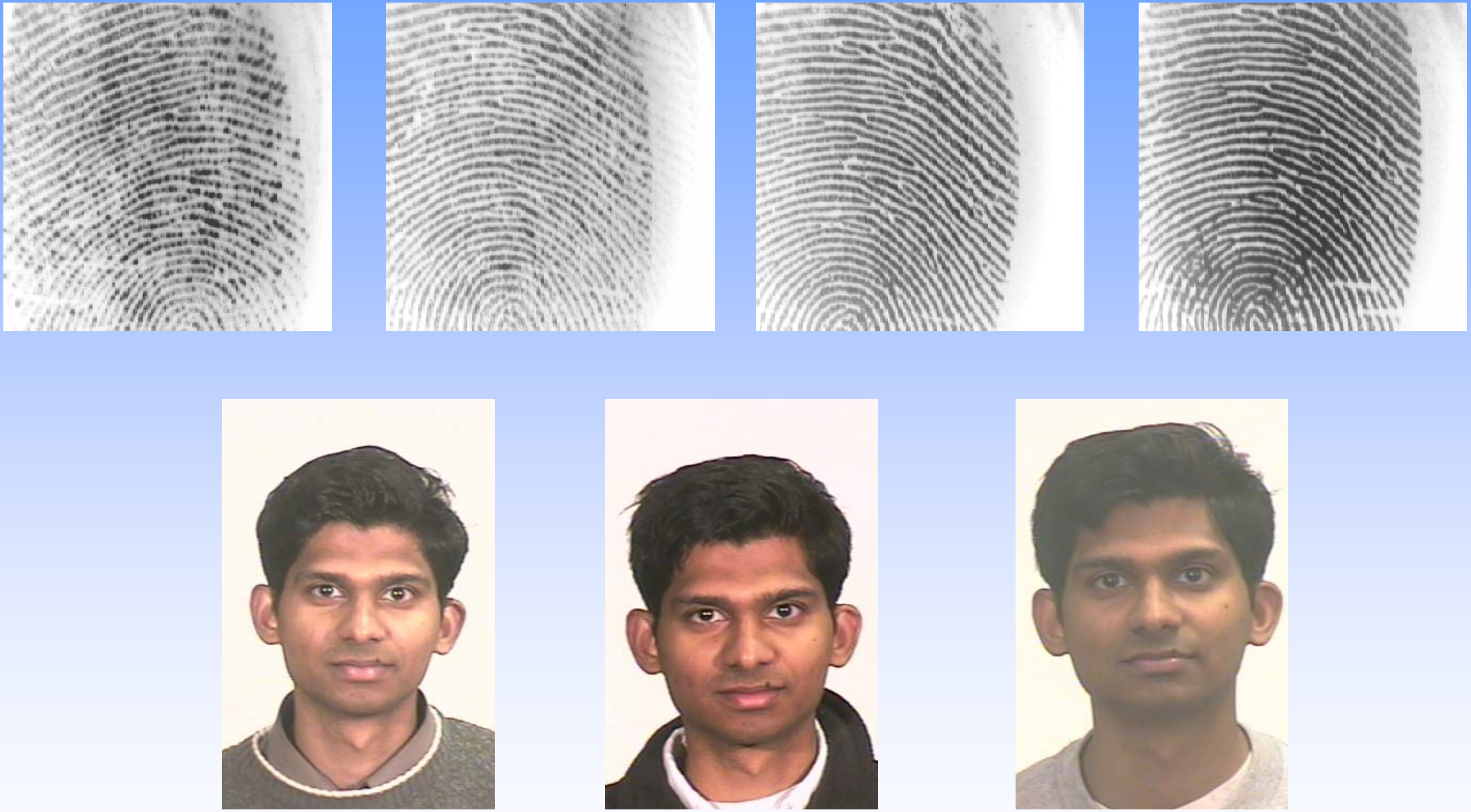


news.bbc.co.uk/hi/english/in_depth/americas
/2000/us_elections

Father and son

R.-L. Hsu, “Face Detection and Modeling for Recognition”, Ph.D. Thesis, 2002

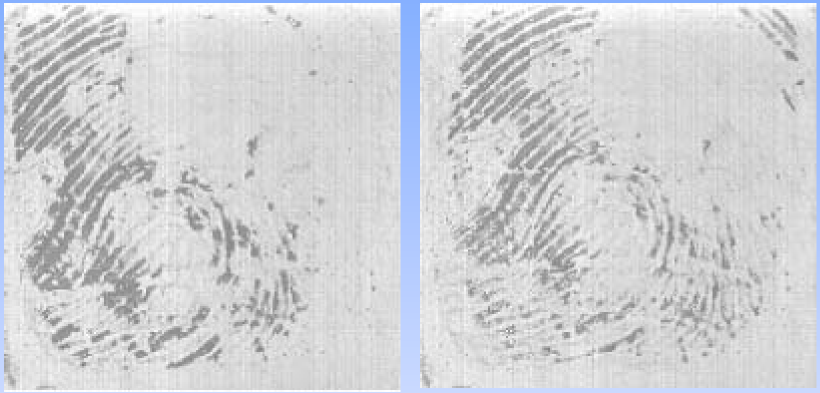
Temporal Variations



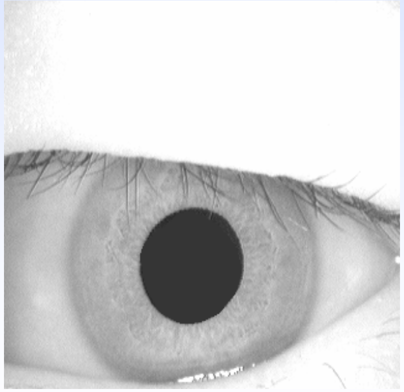
Template aging

Non-Universality

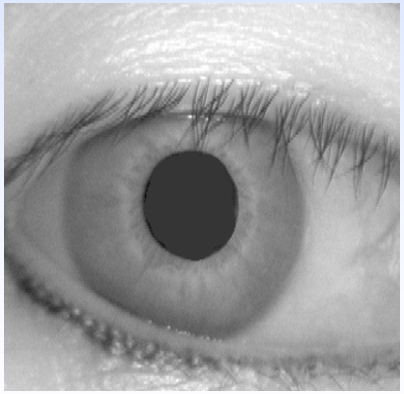
- ~ 3% of the population has poor quality fingerprint images



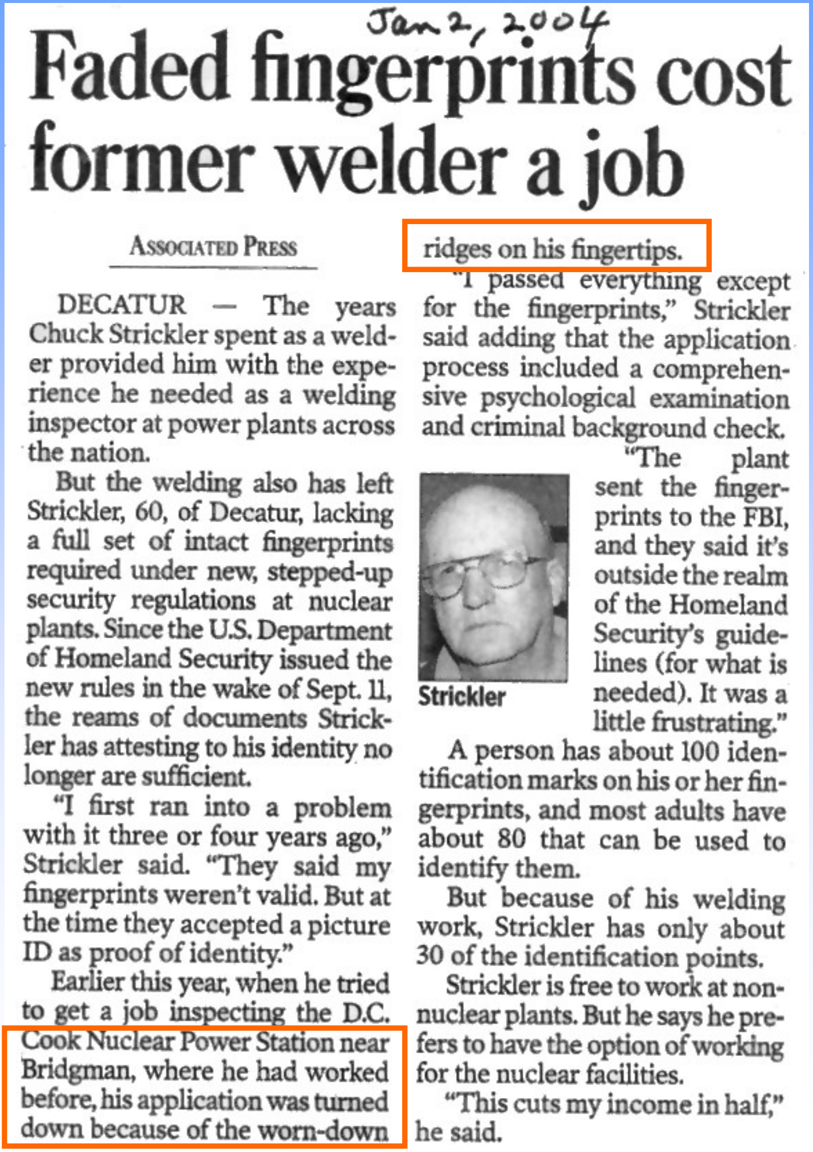
- Failure to enroll for iris is ~7%



Drooping eyelids



Large pupil



Jan 2, 2004

Faded fingerprints cost former welder a job

Associated Press

DECATUR — The years Chuck Strickler spent as a welder provided him with the experience he needed as a welding inspector at power plants across the nation.

But the welding also has left Strickler, 60, of Decatur, lacking a full set of intact fingerprints required under new, stepped-up security regulations at nuclear plants. Since the U.S. Department of Homeland Security issued the new rules in the wake of Sept. 11, the reams of documents Strickler has attesting to his identity no longer are sufficient.

"I first ran into a problem with it three or four years ago," Strickler said. "They said my fingerprints weren't valid. But at the time they accepted a picture ID as proof of identity."

Earlier this year, when he tried to get a job inspecting the D.C. Cook Nuclear Power Station near Bridgman, where he had worked before, his application was turned down because of the worn-down ridges on his fingertips.

"I passed everything except for the fingerprints," Strickler said adding that the application process included a comprehensive psychological examination and criminal background check.

"The plant sent the fingerprints to the FBI, and they said it's outside the realm of the Homeland Security's guidelines (for what is needed). It was a little frustrating."

Strickler

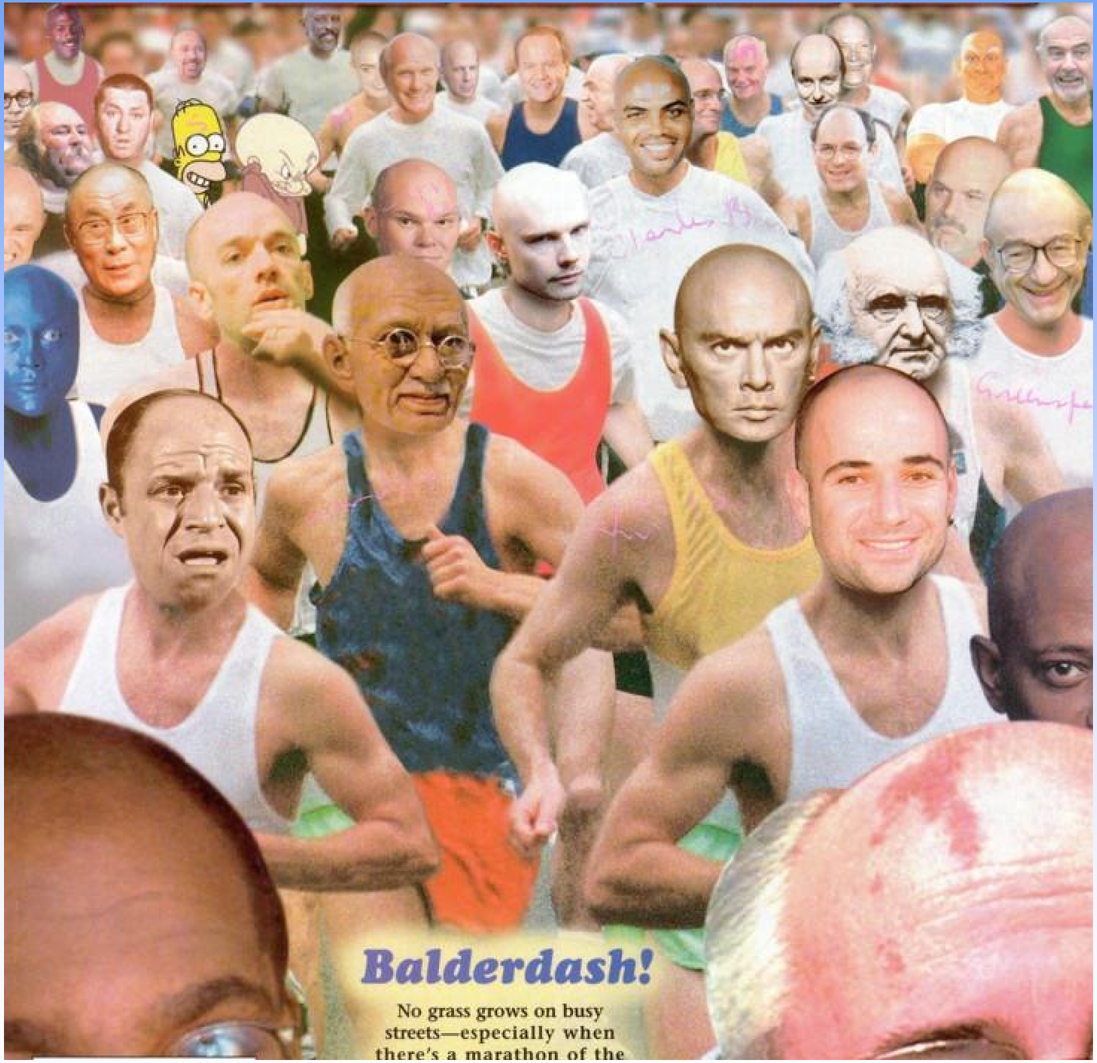
A person has about 100 identification marks on his or her fingerprints, and most adults have about 80 that can be used to identify them.

But because of his welding work, Strickler has only about 30 of the identification points.

Strickler is free to work at non-nuclear plants. But he says he prefers to have the option of working for the nuclear facilities.

"This cuts my income in half," he said.

Locating Faces in a Crowd

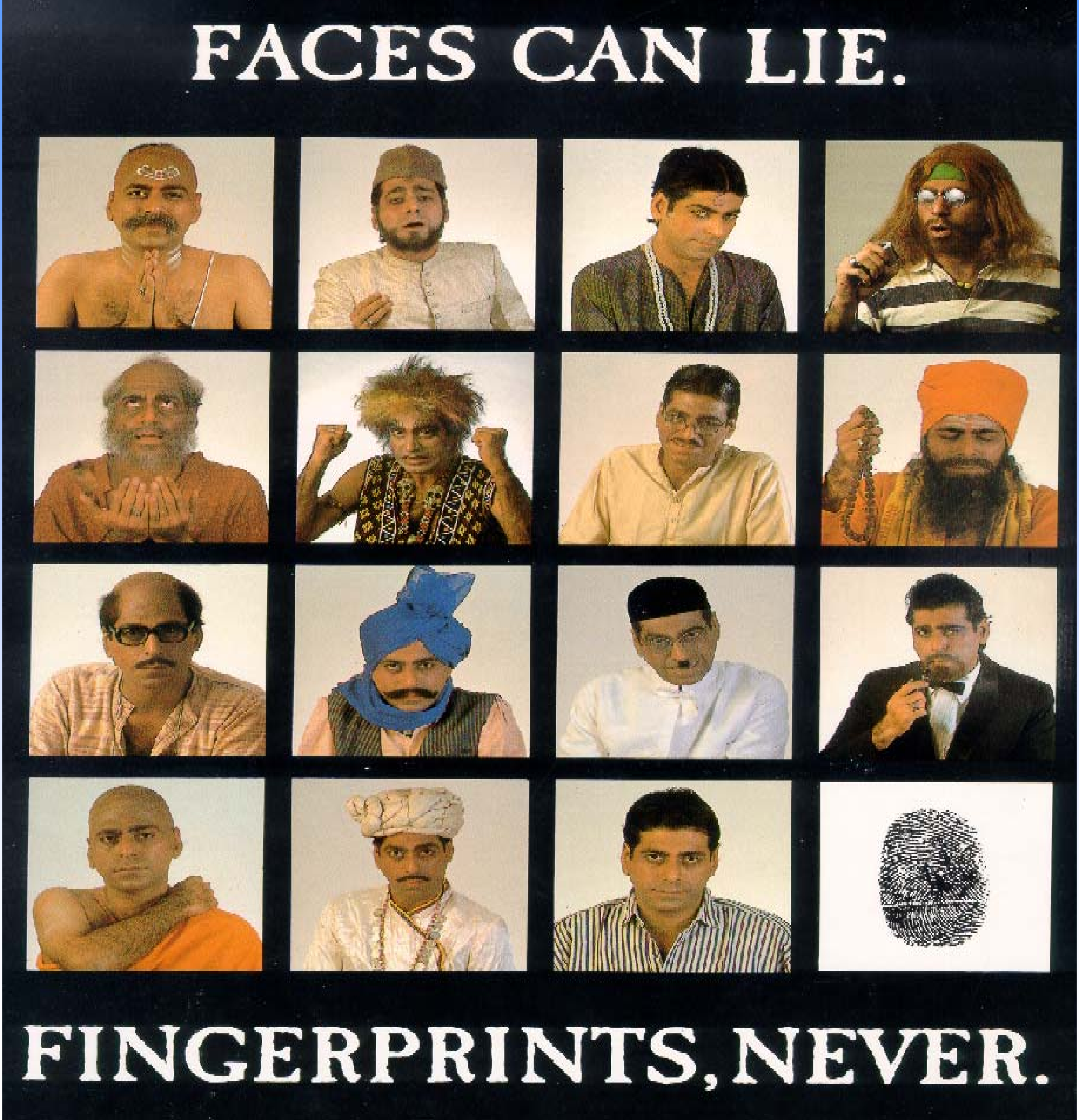


Games Magazine, September 2001

"State-of-the-art" Error Rates

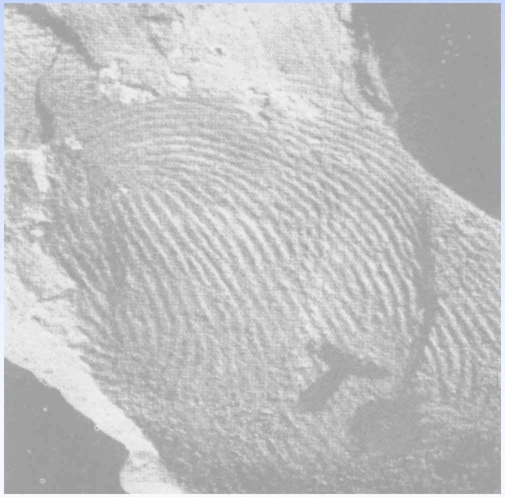
	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2004]	20 years (average age)	2%	2%
	FpVTE [2003]	US govt. ops. Data	0.1%	1%
Face	FRVT [2002]	Varied lighting, outdoor/indoor	10%	1%
Voice	NIST [2000]	Text Independent	10-20%	2-5%

At NY airports, an average of ~ 200,000 passengers pass through daily. There would be 4000 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


FACES CAN LIE.
FINGERPRINTS, NEVER.

Fingerprints

- Graphical flow like ridges present in human fingers; formation depends on the initial conditions of the embryonic development
- Different fingers have different ridge characteristics;
- Minute details are permanent
- Fingerprint evidence is acceptable in a court of law

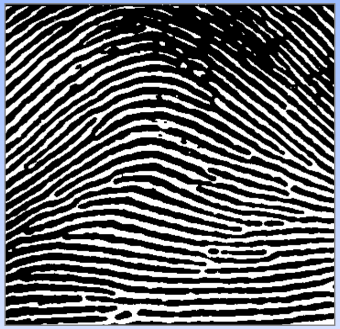


Fingerprint on Palestinian lamp (400 A.D.)

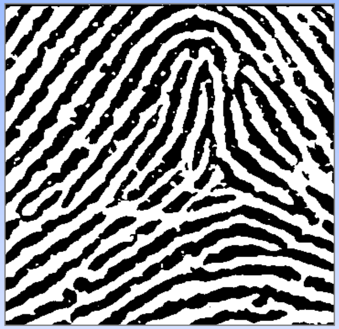
Identical Twins

Fingerprint Classification

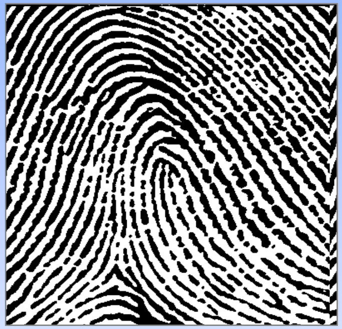
- Classify fingerprints for binning/indexing
- Goal: 99% classification accuracy with 20% reject rate
- Even experts cannot always do correct classification



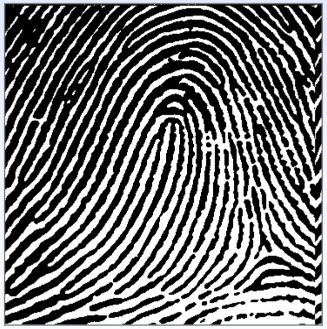
Arch (A)



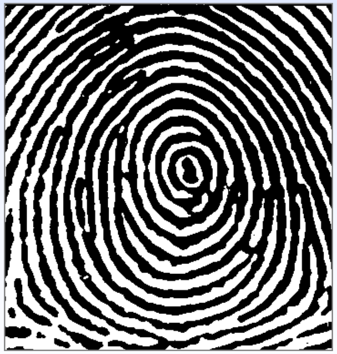
Tented Arch (T)



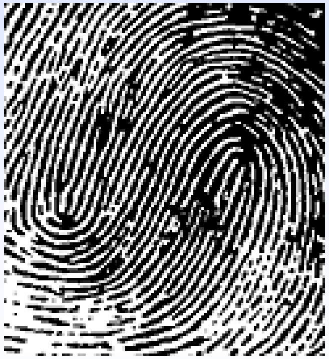
Right Loop (R)



Left Loop (L)



Whorl (W)

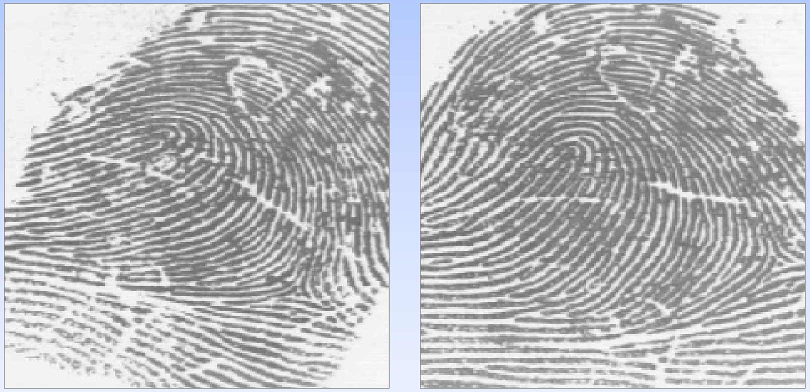


Double Loop (W)

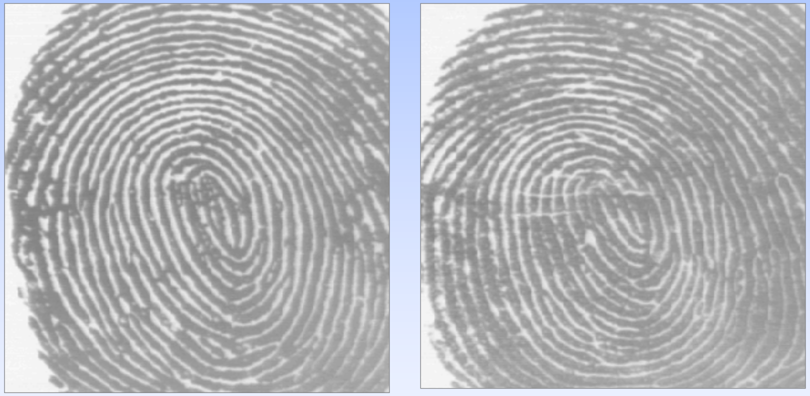
- Natural frequencies of W, L, R and A (A + T) are 27.9%, 33.8%, 31.7% and 6.6%

Fingerprint Matching

Find the similarity between two fingerprints



Fingerprints from the same finger

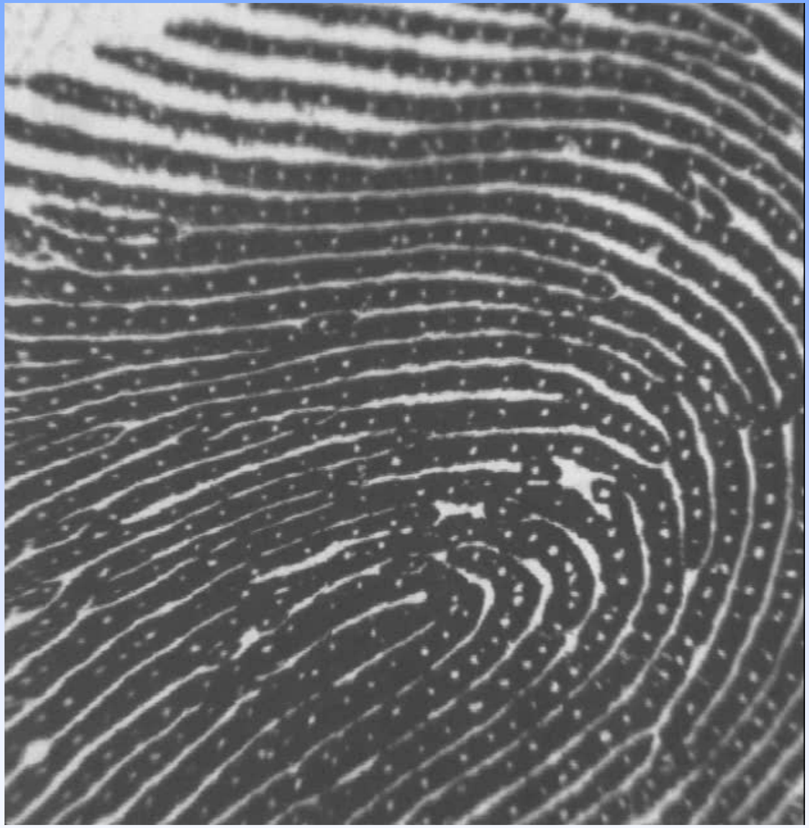


Fingerprints from two different fingers

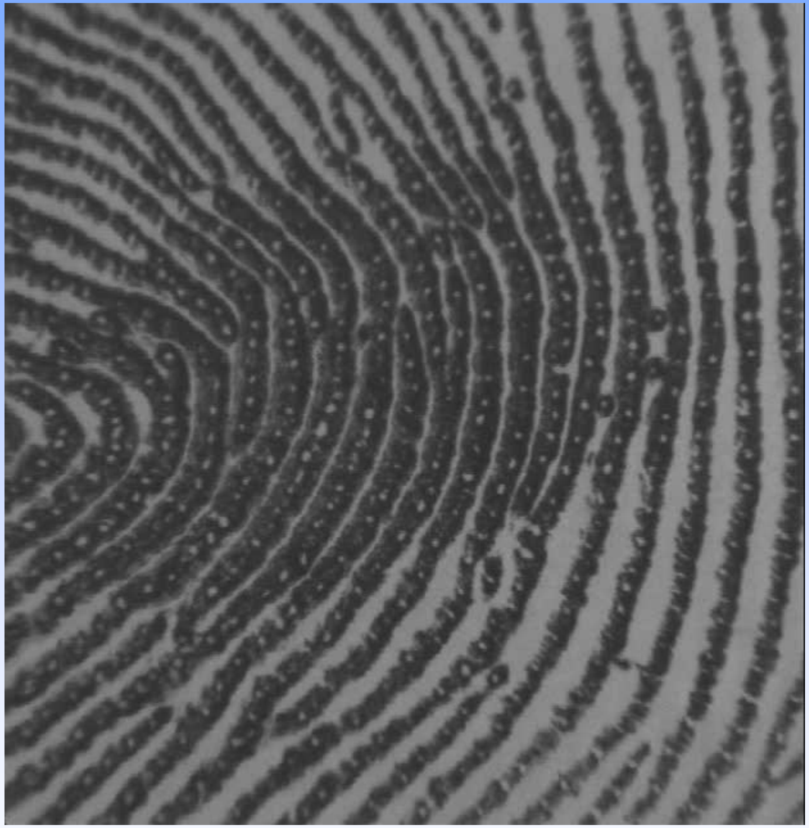
Challenges in Fingerprint Matching

- Fingerprint matching is difficult due to
  - large intra-class variations caused by sensor noise, partial overlap, and non-linear distortion
  - small inter-class variations (similarities in the global structure and ridge orientations)
- Despite extensive research, the best matcher in FVC 2004 had an EER of 2.07%
- Challenge is to handle poor quality fingerprints and fingerprints having little overlap

Non-rigid Deformation



Nonlinear Rotation



Nonlinear lateral movement

http://www.cim.mcgill.ca/~vleves/homepage/research/taxel/taxel.htm

Fingerprint Matching Techniques

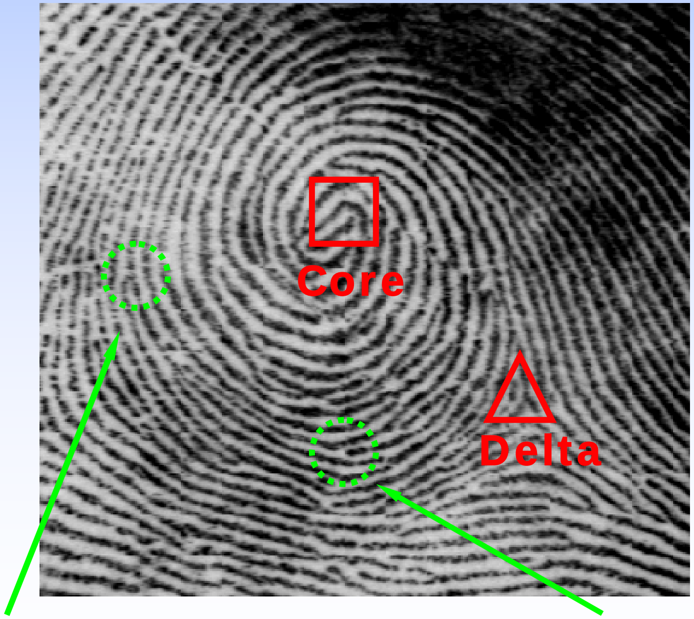
- Minutiae-based
  - Uses location, orientation, and minutia type
  - Point pattern matching problem
  - Hard decision is made on the correspondence
- Correlation-based
  - Spatial correlation of template and query
  - Sensitive to rigid and non-linear transformation
  - Computationally expensive
- Ridge Feature-based
  - Orientation and frequency of ridges, ridge shape, texture information, etc. are used
  - Suffers from low discriminative ability

Stages in Fingerprint Matching

- Alignment
  - Estimate rotation, translation, and distortion
  - Input fingerprint is aligned with the template
- Matching
  - Compute the similarity between the pre-aligned input and the template using the following metrics
    - Number of matching minutiae
    - Euclidean distance between ridge feature maps
    - Local correlation around minutiae
    - Orientation field match

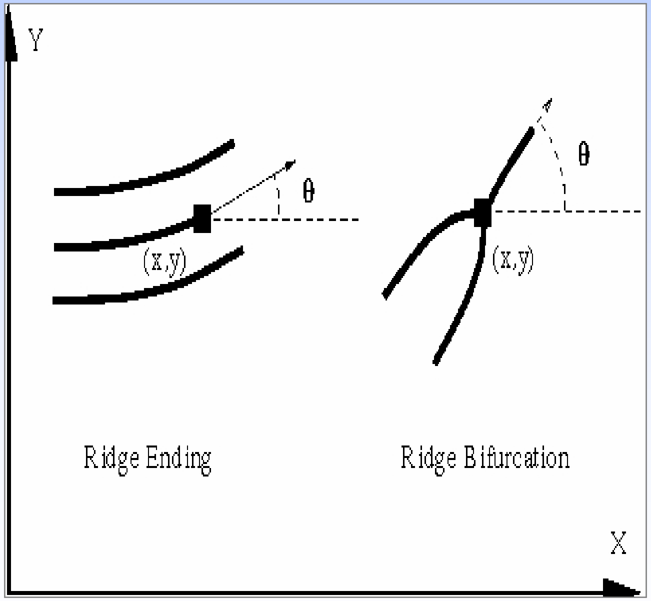
Minutiae-based Representation

- Local ridge characteristics (minutiae): ridge ending and ridge bifurcation
- Singular points (core and delta): discontinuity in ridge orientation



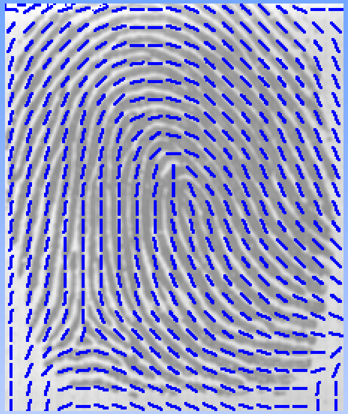
Ridge Bifurcation

Ridge Ending

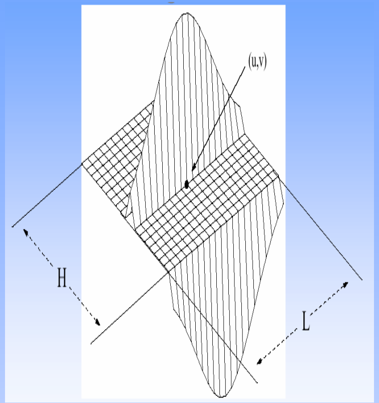


Minutiae Extraction

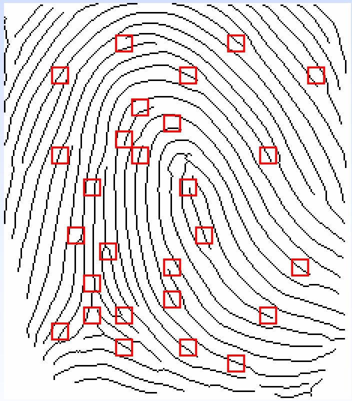
Input Image



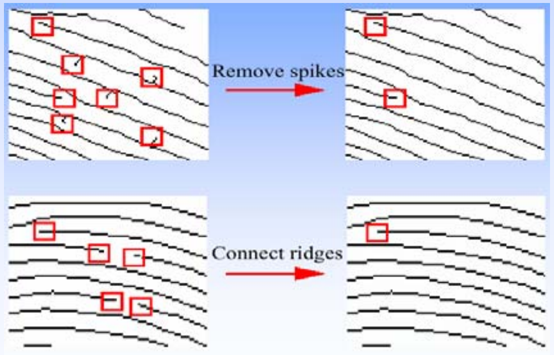
Orientation Estimation



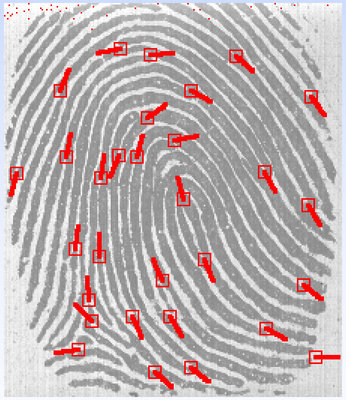
Ridge Filter



Ridge Thinning
Minutiae Detection



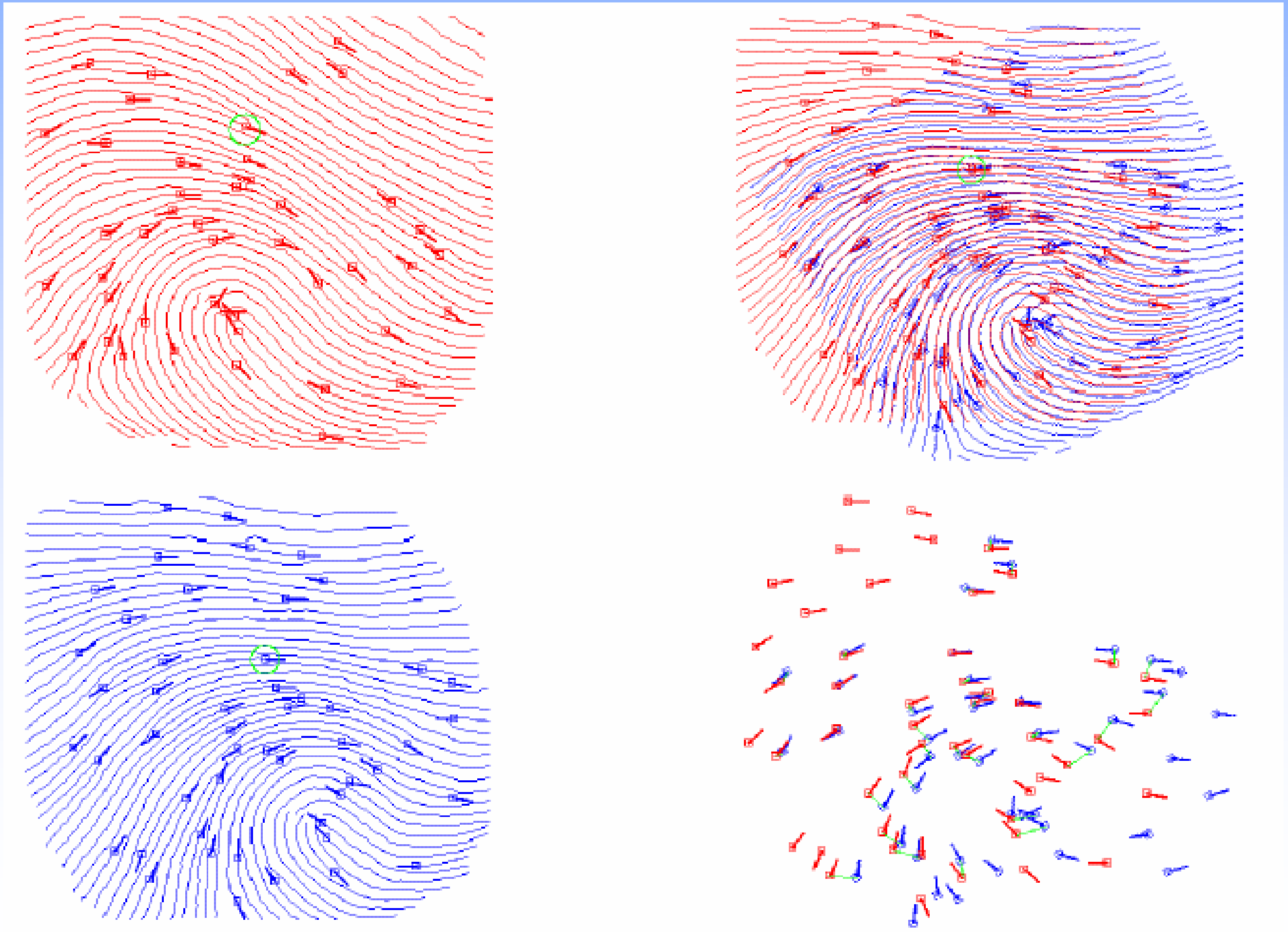
Post-processing



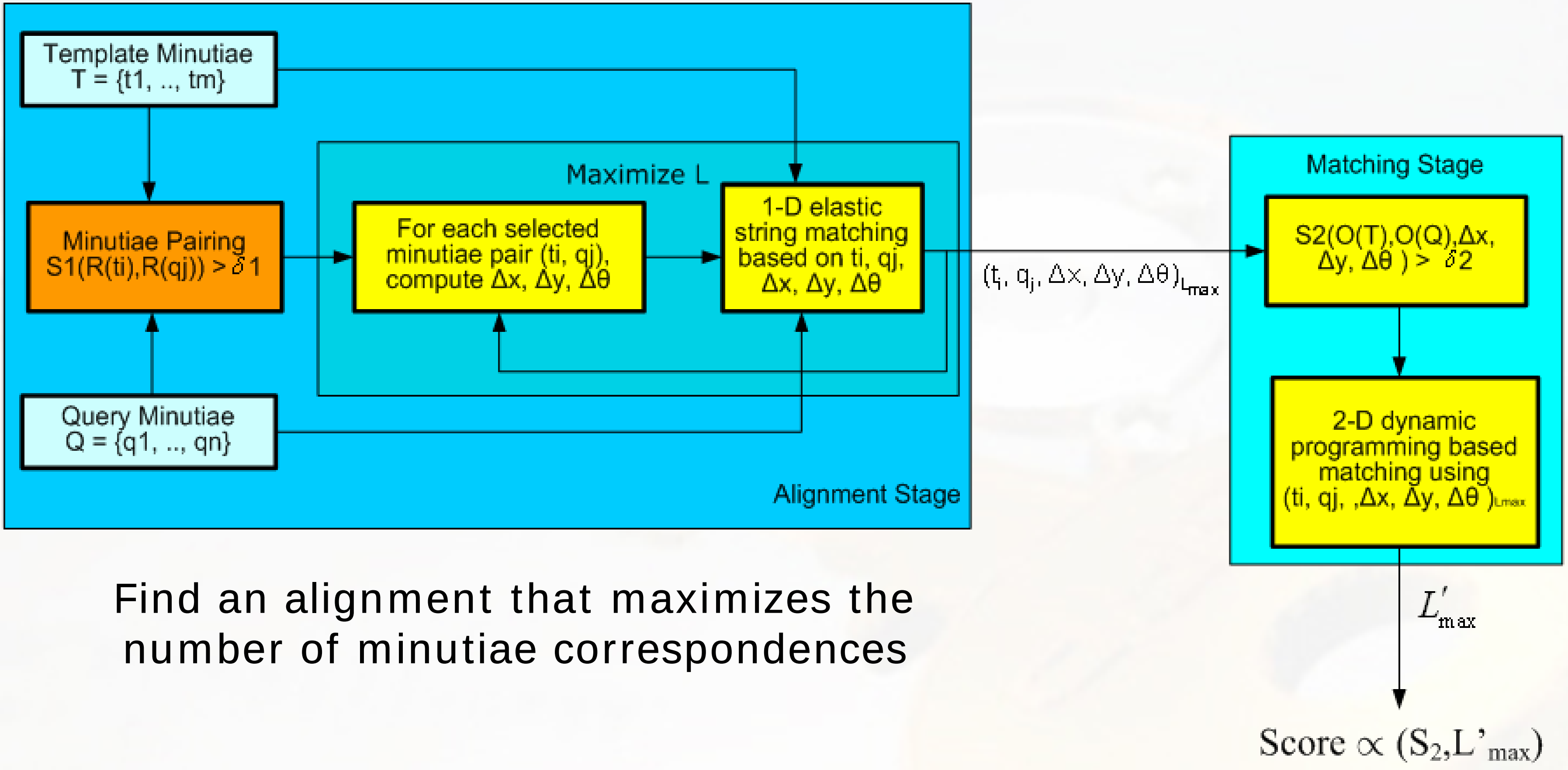
Extracted Minutiae

Minutiae-based Matchers

- Point matching problem
- Given m minutiae in template and n minutiae in input query, find the number of corresponding minutiae



2-D Dynamic Programming based Minutiae Matching


Template Minutiae
T = {t1, .., tm}
Minutiae Pairing
S1(R(ti),R(qj)) > δ1
Query Minutiae
Q = {q1, .., qn}
Maximize L
For each selected minutiae pair (ti, qj), compute Δx, Δy, Δθ
1-D elastic string matching based on ti, qj, Δx, Δy, Δθ
Alignment Stage
(ti, qj, Δx, Δy, Δθ)Lmax
Matching Stage
S2(O(T),O(Q),Δx, Δy, Δθ) > δ2
2-D dynamic programming based matching using (ti, qj, ,Δx, Δy, Δθ)Lmax
L'max
Score ∝ (S2,L'max)

Find an alignment that maximizes the number of minutiae correspondences

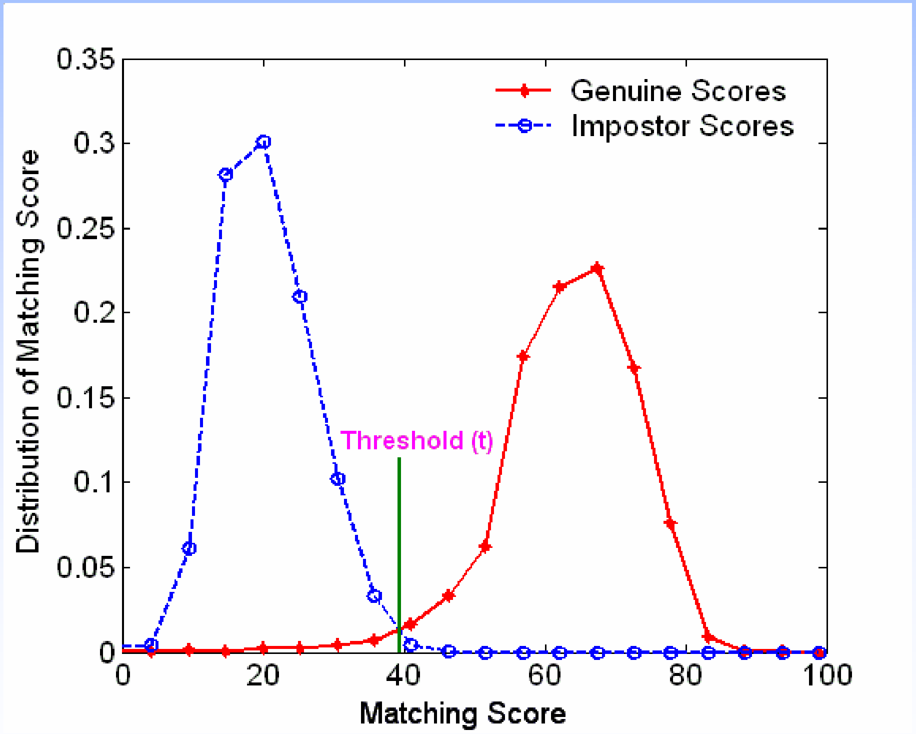
S_1 → Ridge similarity measure, S_2 → Orientation similarity measure,
R(t) → 1-D representation of ridge points of minutia t, O(T) → Orientation field

Matching time ~0.1 sec.

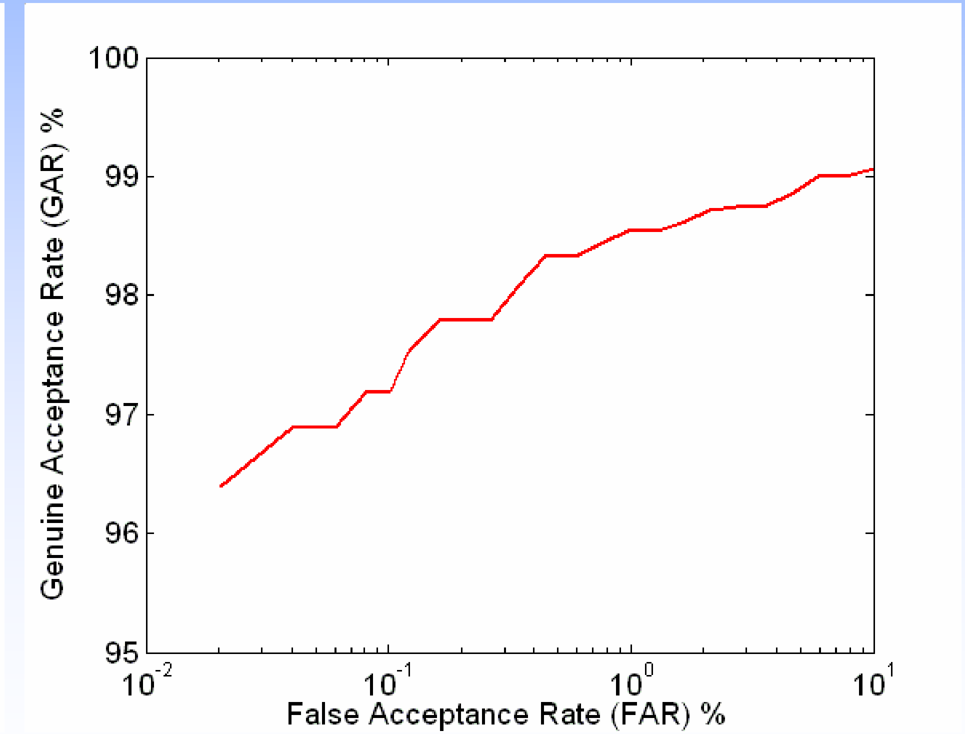
T = {t1, .., tm}

Matching Score Distributions

- Performance depends on the database. FVC2002 Database 1 (100 users, 8 impressions/user)
- For FAR = 0.1% (1 in 1000), GAR = 97.1%
- EER = 1.65%; at 0% False Accept, FRR = 4%



Matching Score Distribution

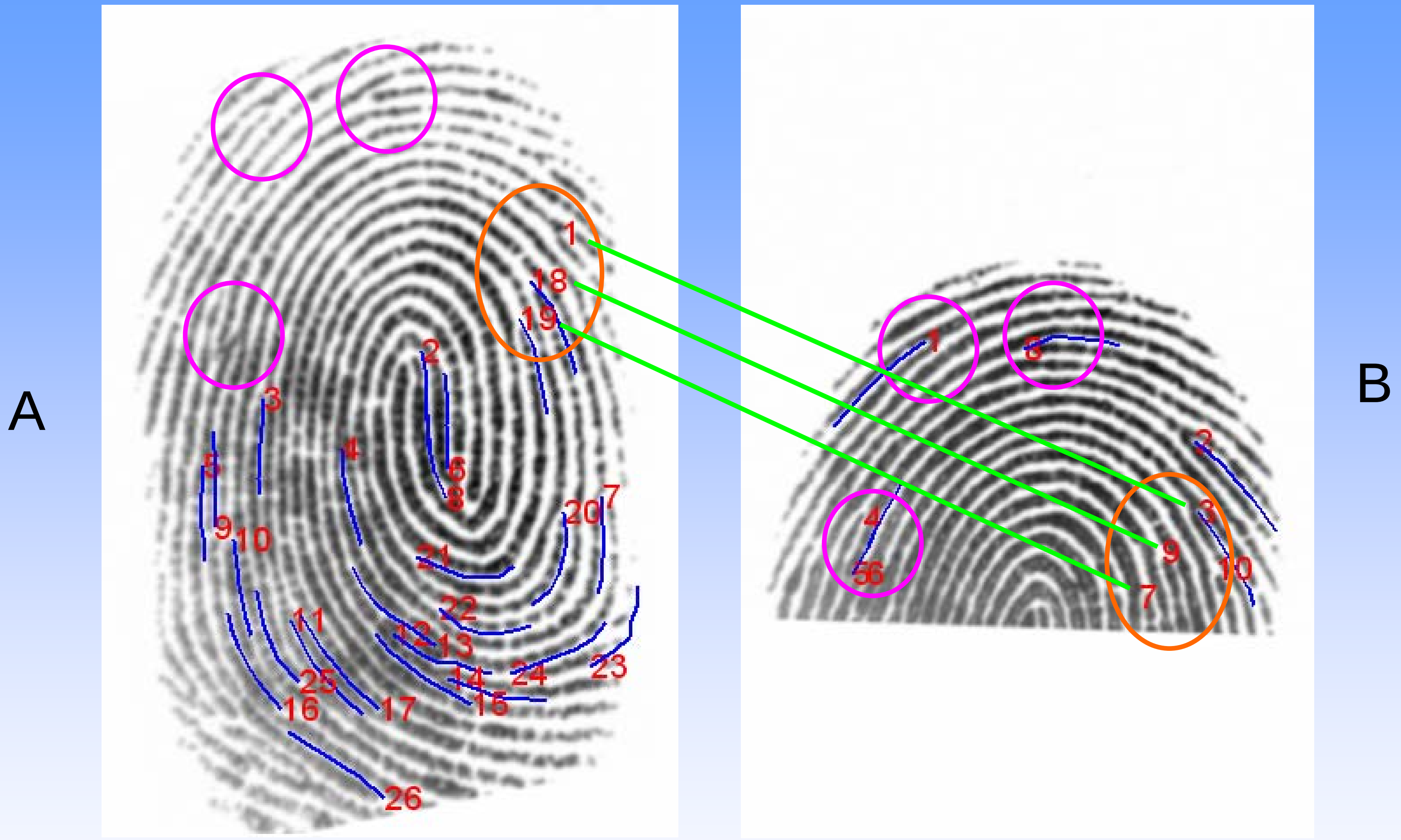


ROC Curve

Analysis of Errors

- Minutiae Extraction
  - Extraction stage does not extract all minutiae and their ridges
  - There may be no corresponding minutiae having ridge points for finding the correct alignment
- Alignment
  - Corresponding minutiae with ridge points exist
  - Alignment step fails due to small number of correspondences
- Matching
  - Estimated alignment is correct
  - But, the matching score is low because the number of correspondences is low compared to the number of minutiae
  - Reasons: deformation, spurious and missing minutiae

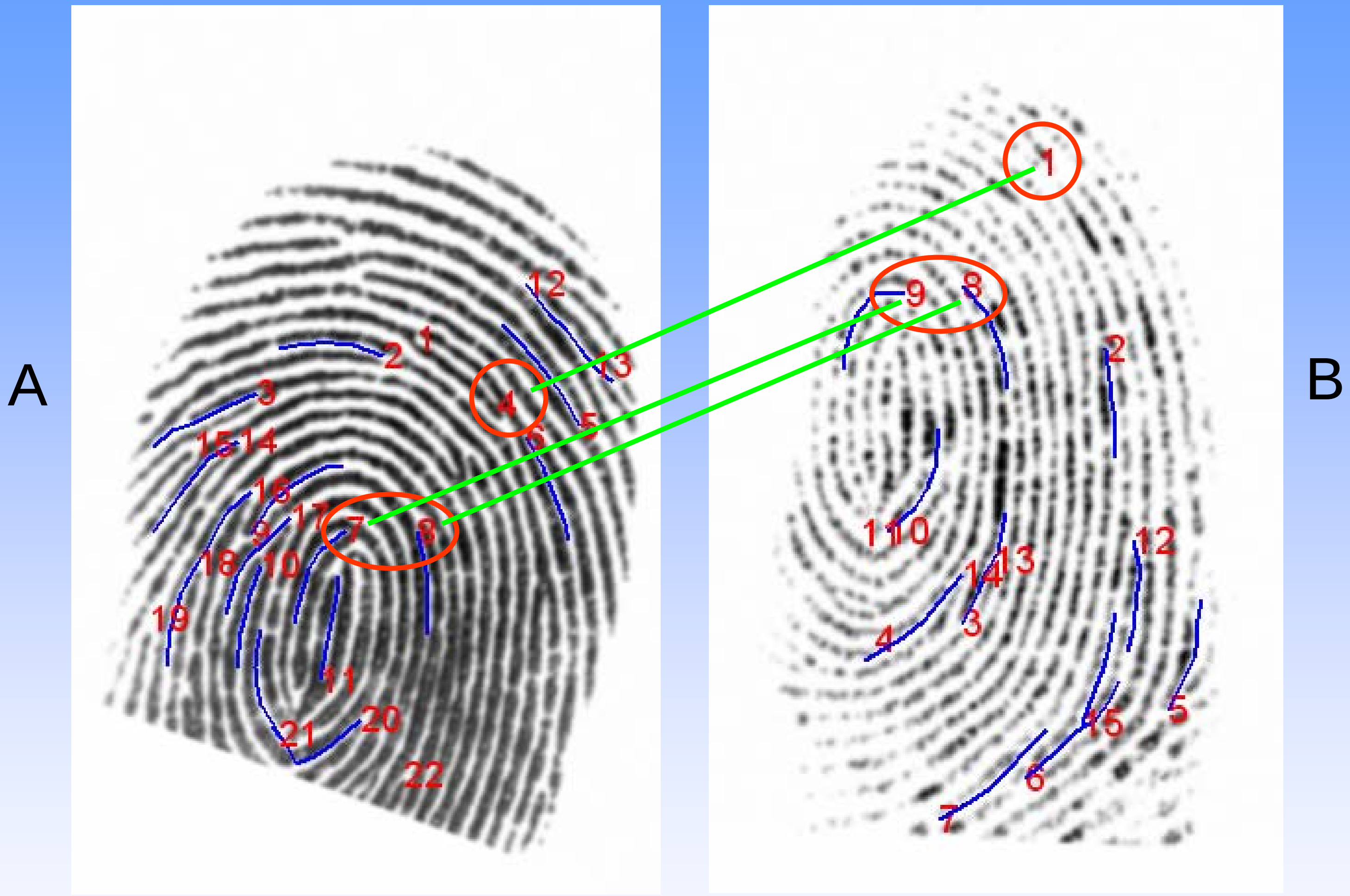
Minutiae Extraction Failure



True Minutiae Matches: A1→B3, A18→B9, A19→B7

A1, B9 and B7 were detected, but the associated ridges were not detected because they are close to the boundary

Alignment Failure

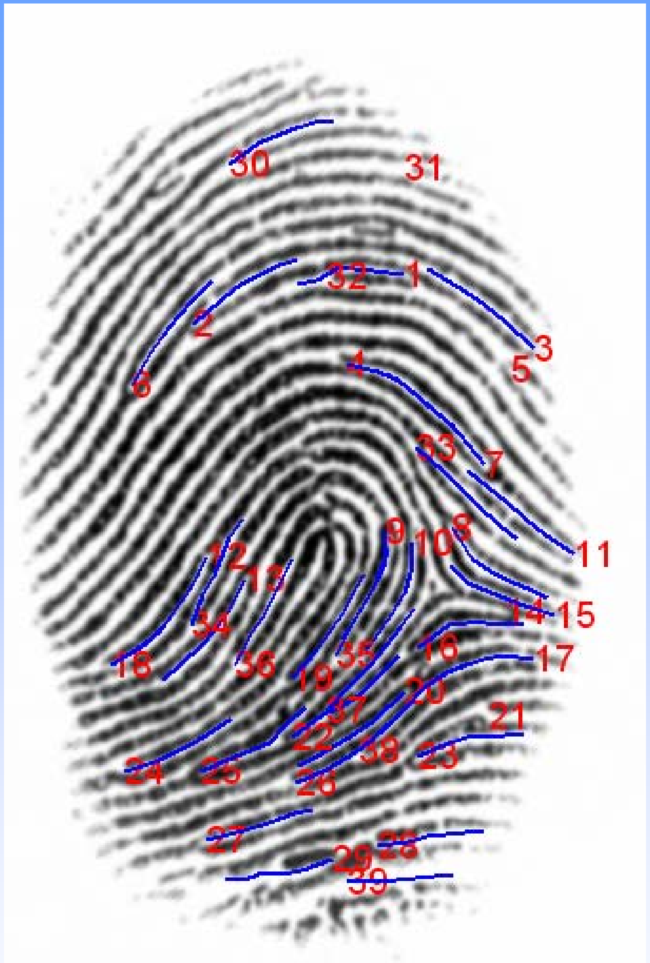


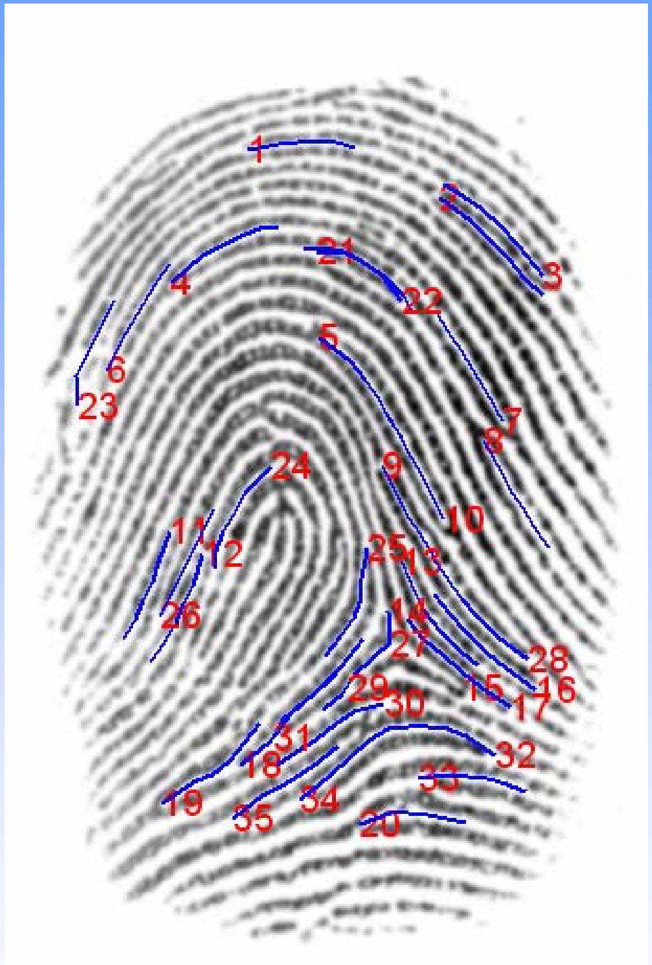
True Minutiae Matches: A7→B9, A8→B8, A4→B1

A7→B9 and A8→B8 pairs have ridge points; however, there exists a false alignment that results in more than three matches

Matching Failure

A





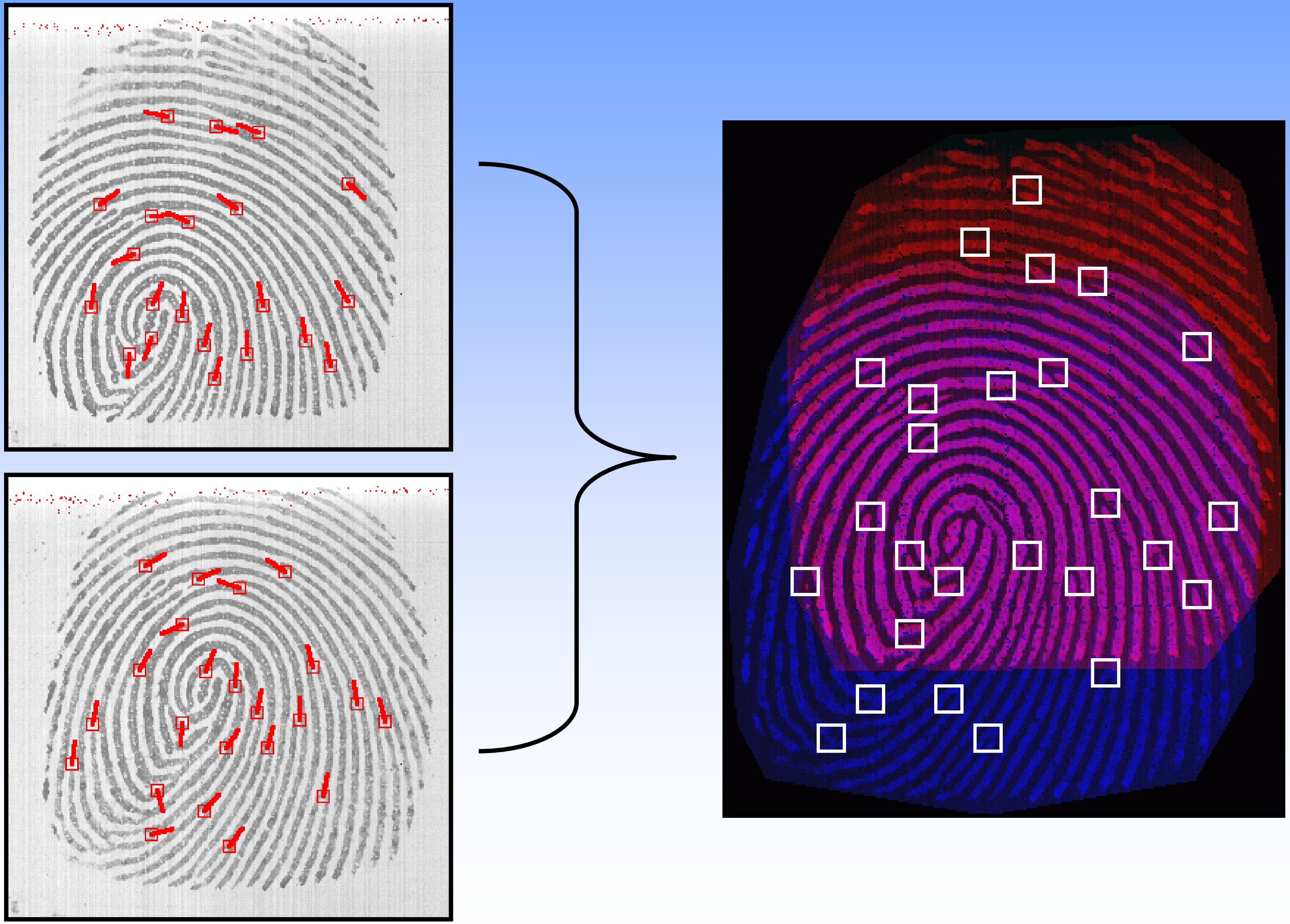
B

No. of matching minutiae identified by the matcher = 10

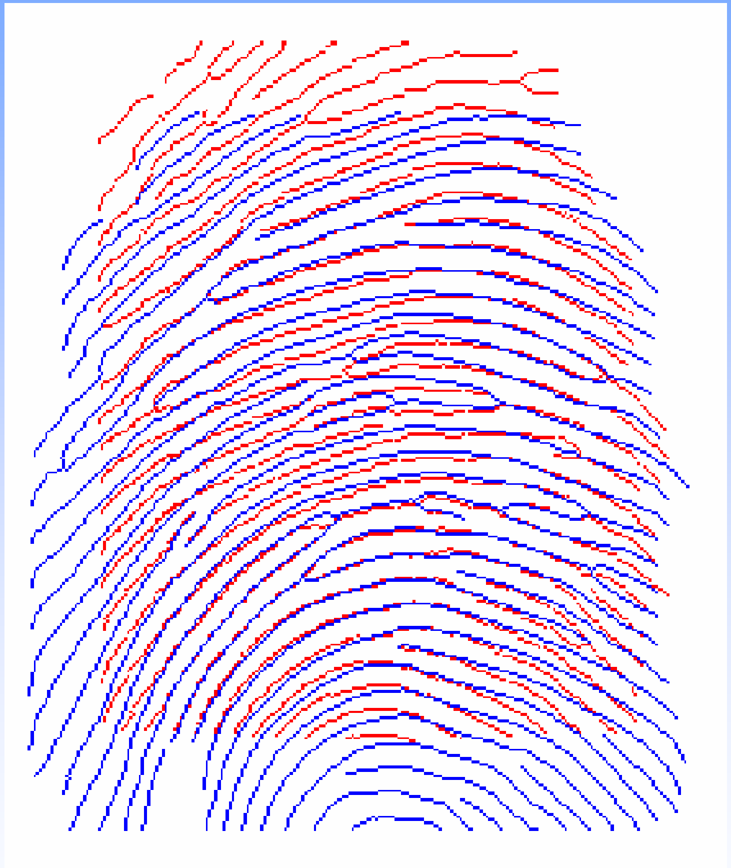
No. of minutiae in A = 38; No. of minutiae in B = 34

Spurious minutiae and large deformation leads to small score

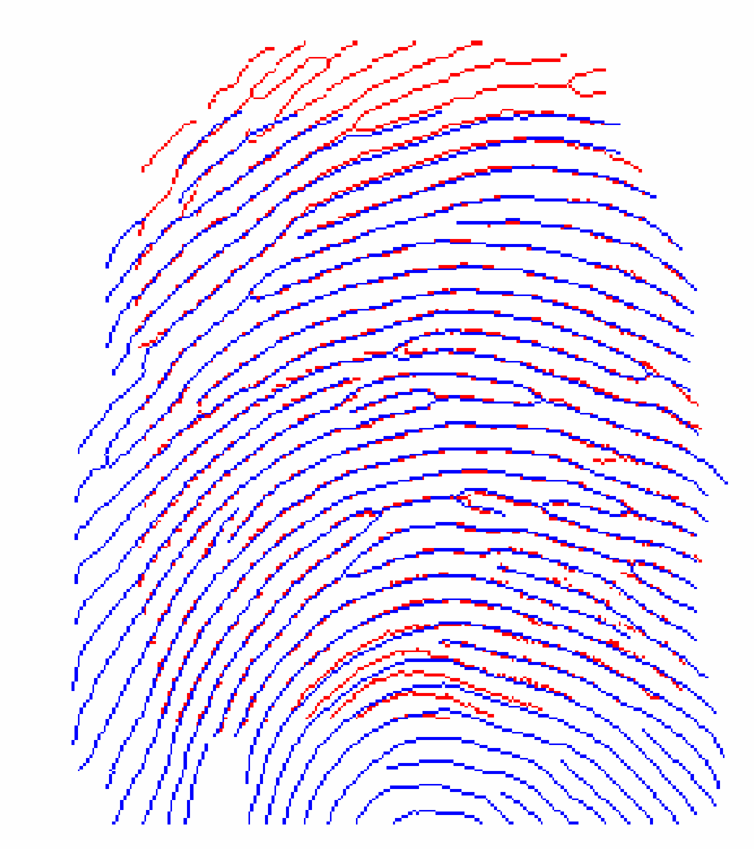
Template Mosaicking



Alignment using Thin Plate Spline

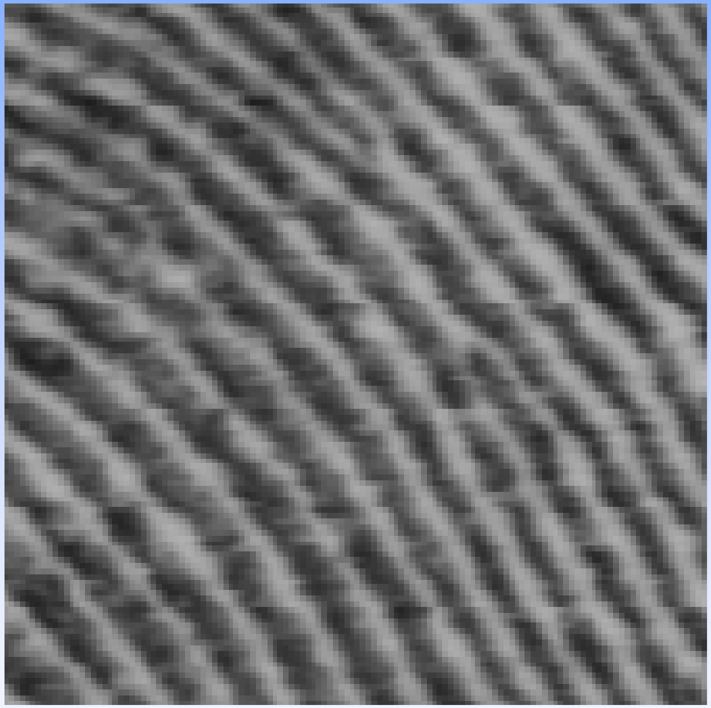


Alignment using minutiae correspondence

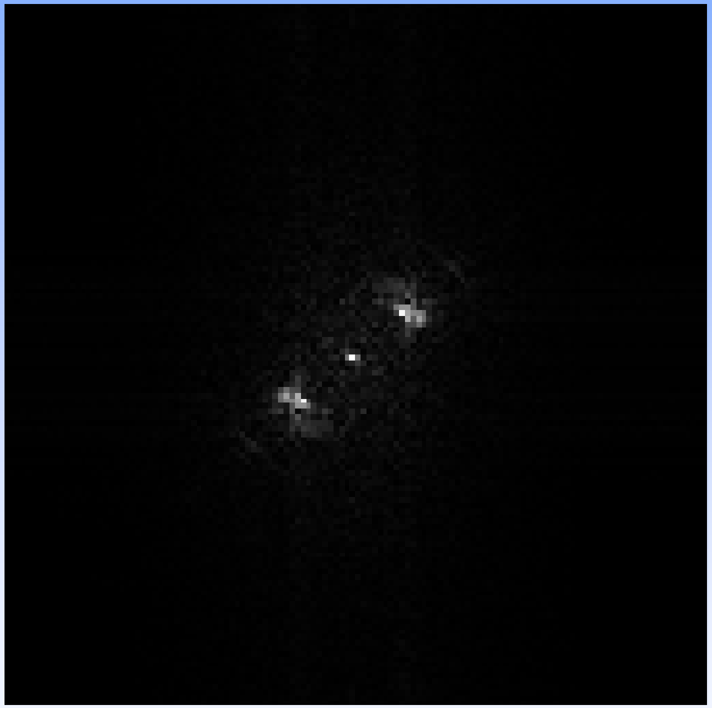


Alignment using ridge correspondence

Fingerprint as Oriented Texture



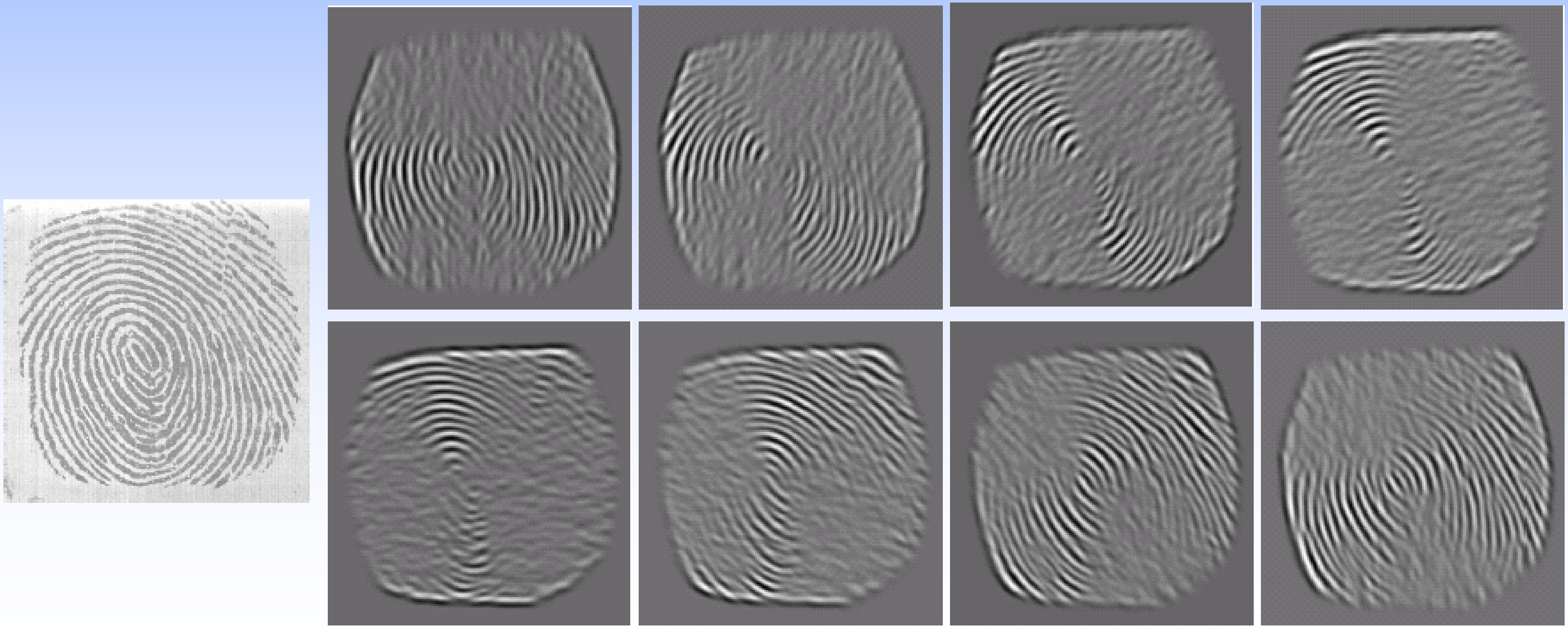
Ridges in local region



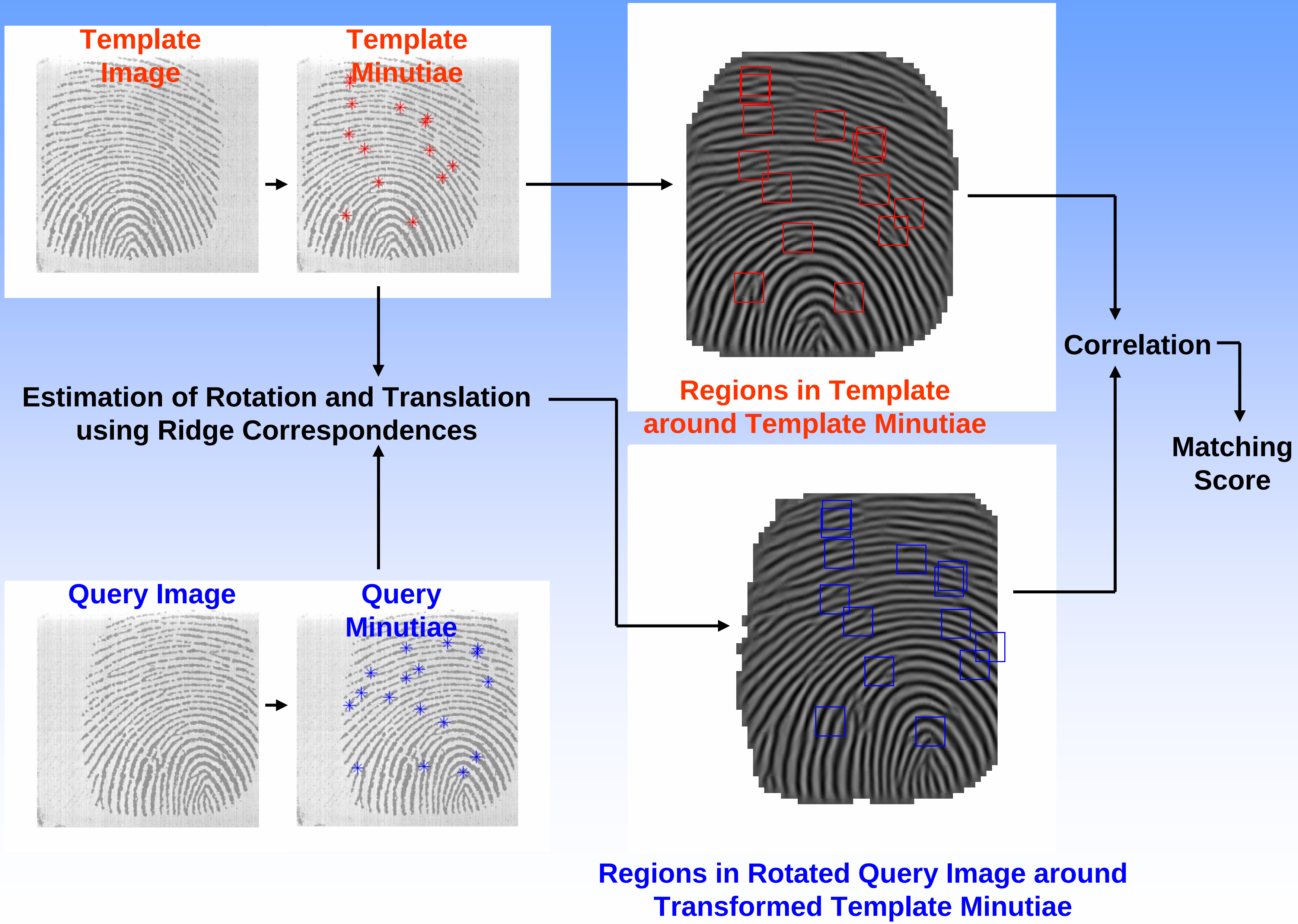
Fourier spectrum

Ridge Feature Maps

- An input fingerprint image is filtered using 8 Gabor filters all having the same frequency but different orientations (0°, 22.5°, 45°, 67.5°, 90°, 112.5°, 135°, 157.5°)



Local Correlation-based Matching



Template Image

Template Minutiae

Regions in Template around Template Minutiae

Estimation of Rotation and Translation using Ridge Correspondences

Correlation

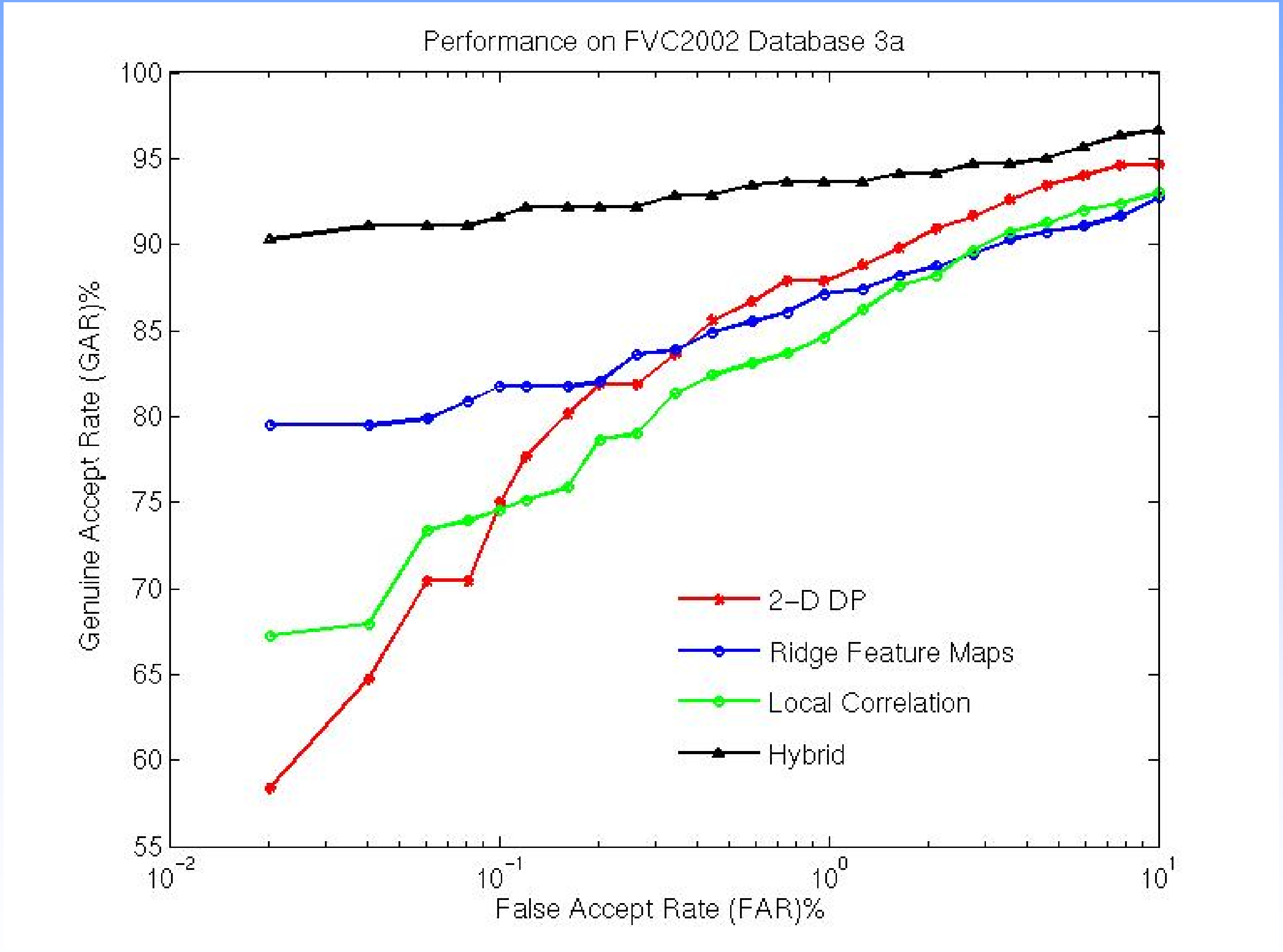
Matching Score

Query Image

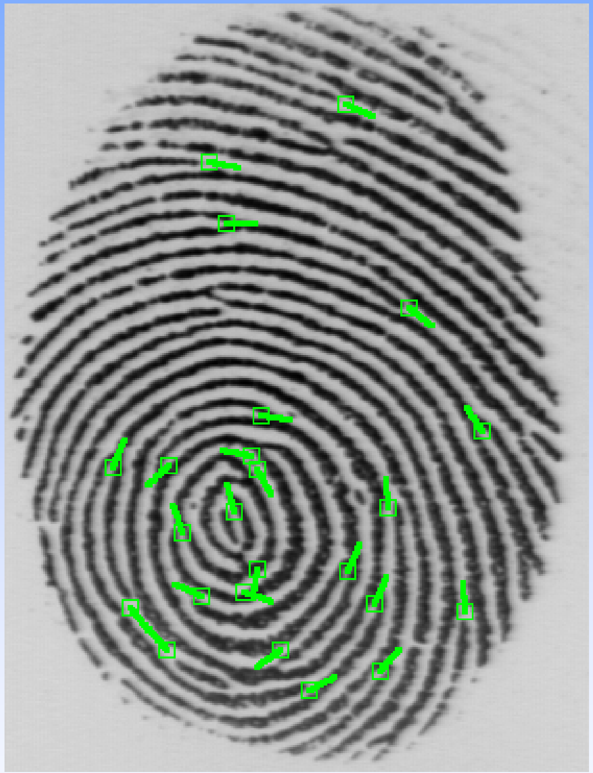
Query Minutiae

Regions in Rotated Query Image around Transformed Template Minutiae

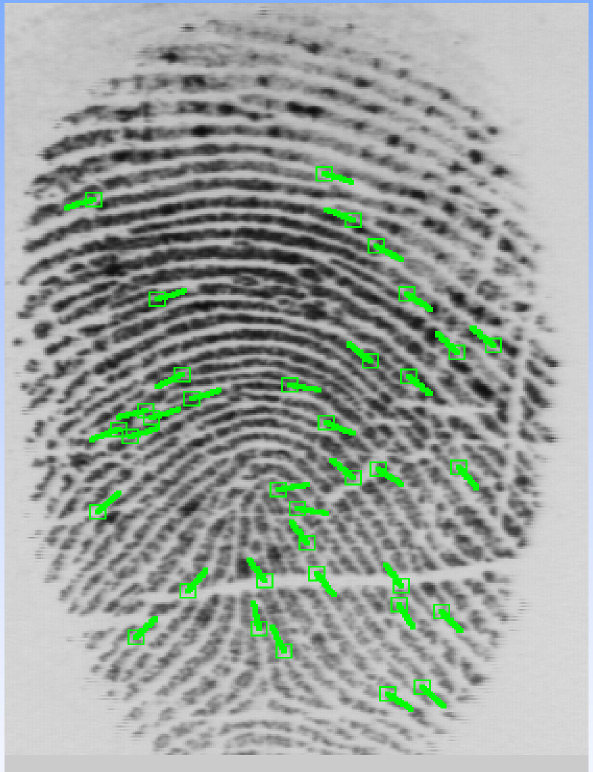
Performance of Hybrid Matcher (Minutiae, Texture & Local Correlation)



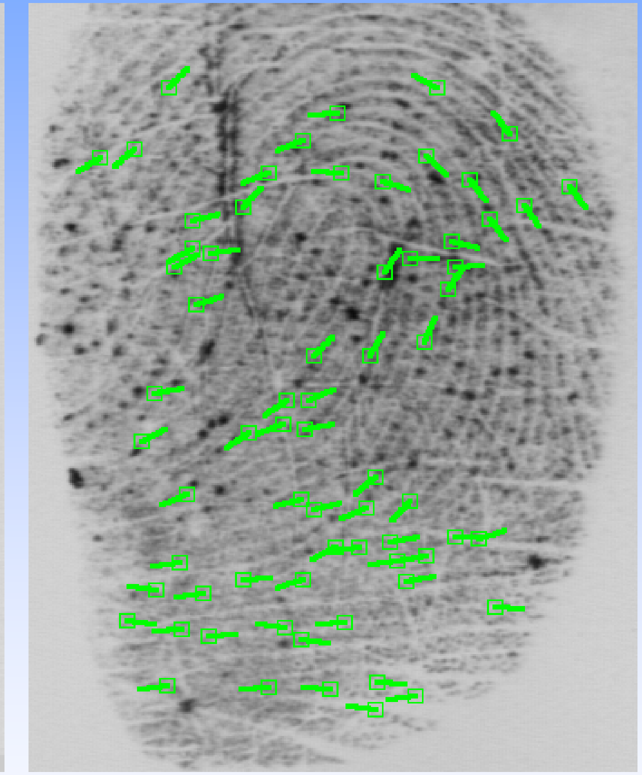
Noisy Images



Quality Index = 0.96
False Minutiae = 0



Quality Index = 0.53
False Minutiae = 7



Quality Index = 0.04
False Minutiae = 27

The Myth of Fingerprints

"They left a mark - on criminology and culture. But what if they're not what they seem?" - *Simon Cole, 2001*

"Only Once during the Existence of Our Solar System Will two Human Beings Be Born with Similar Finger Markings". - *Harper's headline, 1910*

"Two Like Fingerprints Would be Found Only Once Every 10^{48} Years" – *Scientific American, 1911*

Fingerprint identification is based on two premises

(i) Persistence: fingerprint characteristics are invariant

(ii) Uniqueness: fingerprint characteristics are unique

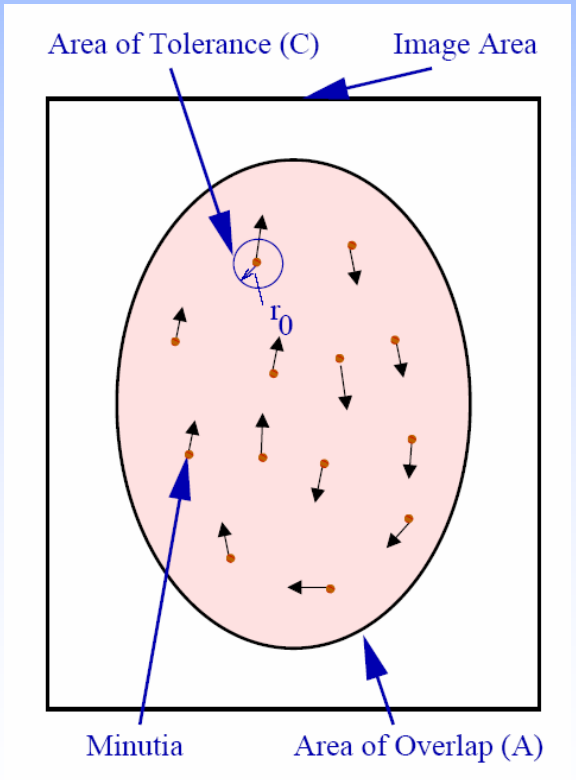
The uniqueness of fingerprints has been accepted over time because of lack of contradiction and relentless repetition. As a result, fingerprint based identification has been regarded as a perfect system of identification

Challenge to Fingerprint Individuality

- Factors determining admissibility of expert scientific testimony: (i) Hypothesis testing, (ii) Known or potential error rate, (iii) Peer reviewed and published, (iv) General acceptance (*Daubert vs. Merrell Dow Pharmaceuticals, 1993*)
- Fingerprint identification was challenged under *Daubert*: error rate is not known and the fundamental premise that "Fingerprints are distinctive or unique" has not been put to test (*USA v. Byron Mitchell, 1999*)

Probability of False Correspondence

- Given a fingerprint with *n* minutiae, what is the probability that it will share *q* minutiae with another fingerprint containing *m* minutiae. The corresponding minutiae should "match" in location and orientation.



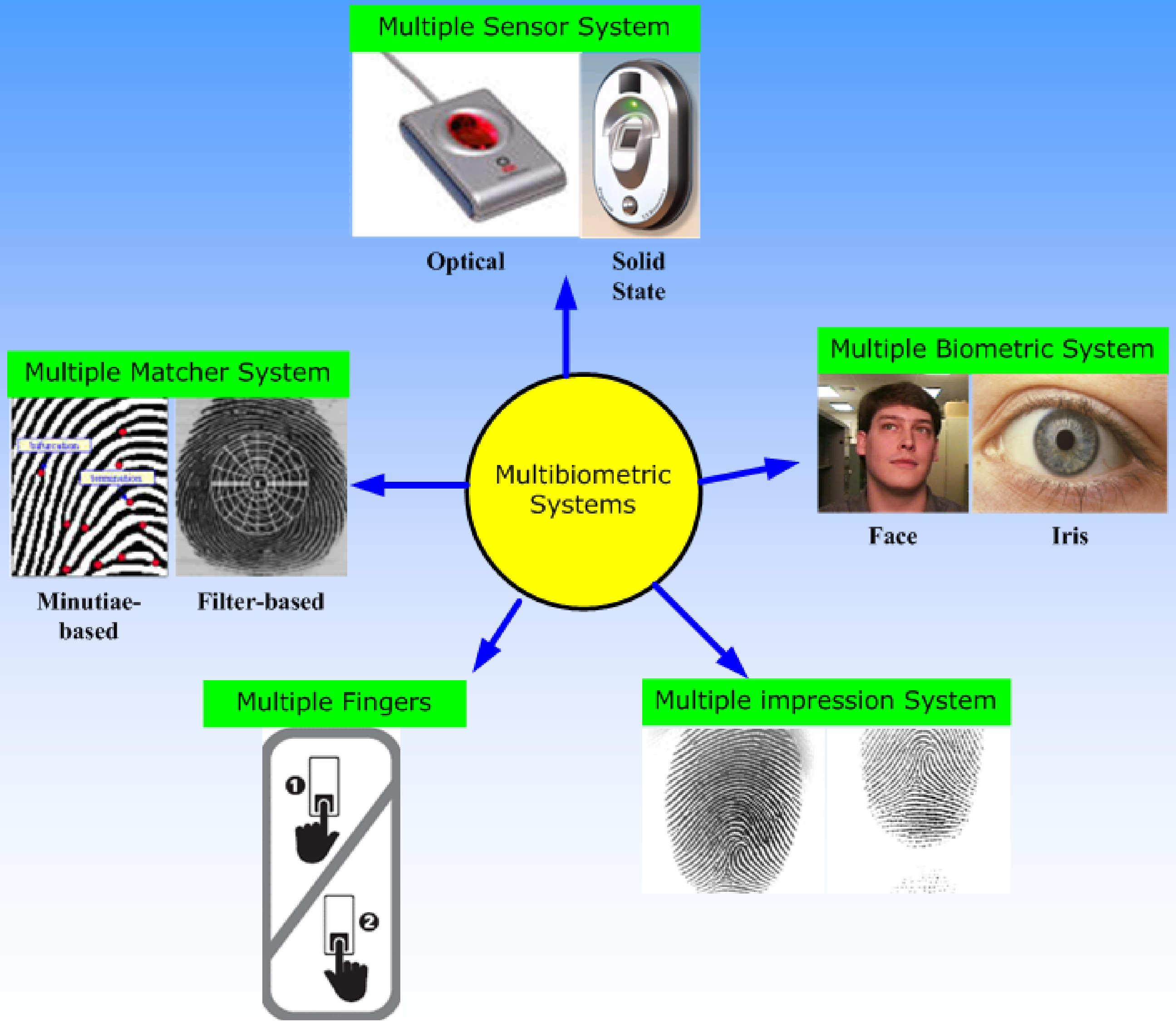
(a) M=52
m=n=q=26
P = 2.40 x 10^{-30}

(b) M=52
m=n=26, q=10
P = 5.49 x 10^{-4}

$M = A/C$

Pankanti, Prabhakar and Jain "On Individuality of Fingerprints" IEEE Trans. On PAMI Vol. 24, No. 8, pp. 1010-1025, 2002

Multibiometrics



Multibiometric Systems

Multiple Sensor System

Optical

Solid State

Multiple Biometric System

Face

Iris

Multiple Matcher System

Minutiae-based

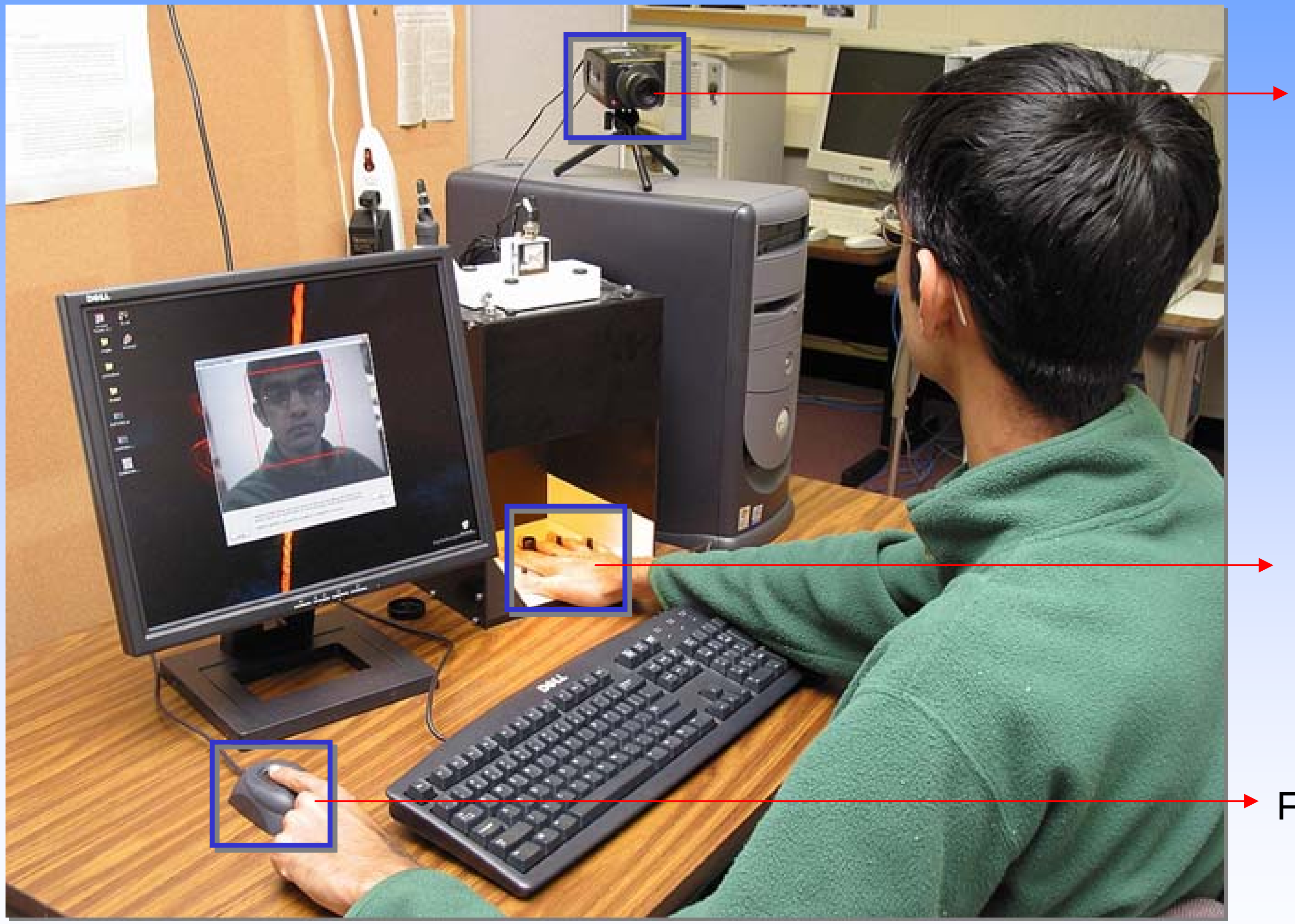
Filter-based

Multiple Fingers

Multiple impression System

http://www.dhs.gov/us-visit

Multibiometric systems



Face

Hand geometry

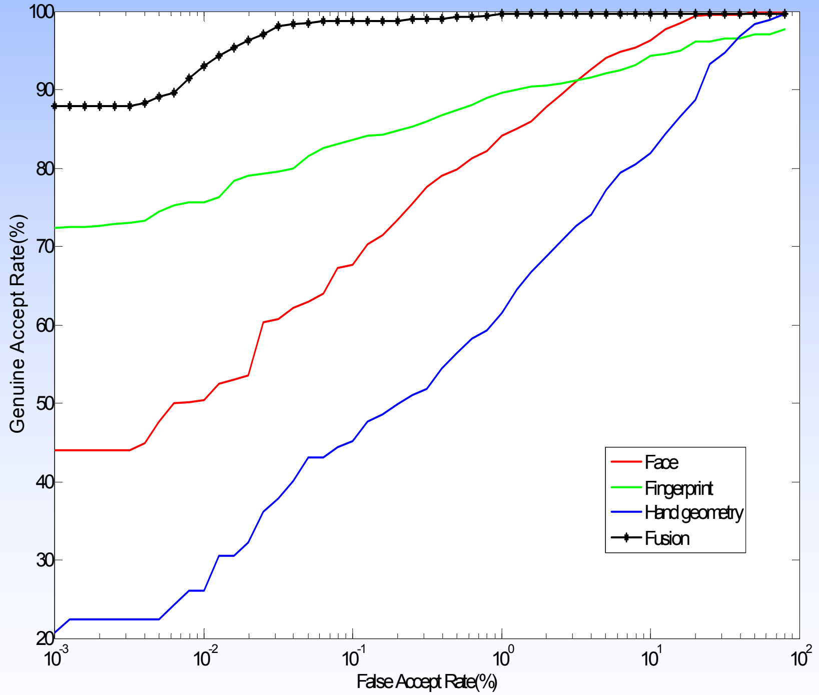
Fingerprint

Improves matching performance, increases population coverage and deters spoofing

Fusion Using Generalized Likelihoods

Obtain the genuine and impostor generalized likelihoods (GL_{GEN} and GL_{IMP}) for each of the K modalities. Given scores s_1, s_2, ... s_K, the fusion rule is based on the likelihood ratio:

$$C(s_1,s_2,\ldots,s_K) = \Pi \{GL_{GEN}(s_i)/GL_{IMP}(s_i)\}$$



Fusion of face, fingerprint and hand modalities for 100 users.

At FAR = 0.1%, GAR = 99.26%

Fusion of Fingerprint and Face

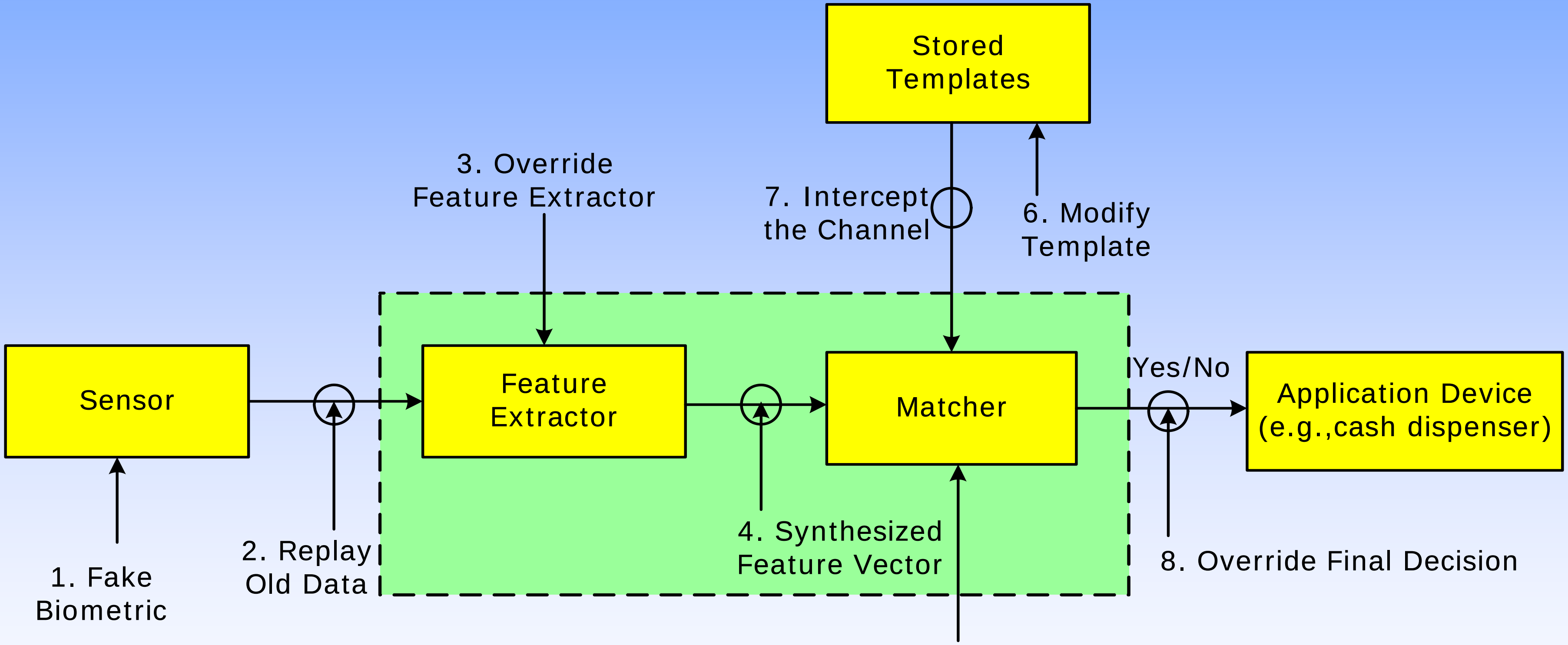
- Three commercial fingerprint matchers and one face matcher with EER values of 3.96%, 3.72%, 2.16% and 3.76%, respectively, were combined
- 972 individuals in the database
- The best EER values in individual columns (rows) are indicated with bold typeface (star (*))

Normalization Technique	*Fusion Technique*				
	Sum	Min	Max	MW	UW
Min-Max	0.99	5.43	0.86	**1.16**	***0.63**
Z-Score	*1.71	5.28	1.79	1.72	1.86
Tanh	1.73	**4.65**	1.82	*1.50	1.62
QLQ	**0.94**	5.43	***0.63**	**1.16**	***0.63**

MW – Matcher Weighting; UW – User Specific Weights

Security of Biometric System

Like any security system, biometric systems are not foolproof



Stored Templates

3. Override Feature Extractor

7. Intercept the Channel

6. Modify Template

Sensor

Feature Extractor

Matcher

Yes/No

Application Device (e.g.,cash dispenser)

1. Fake Biometric

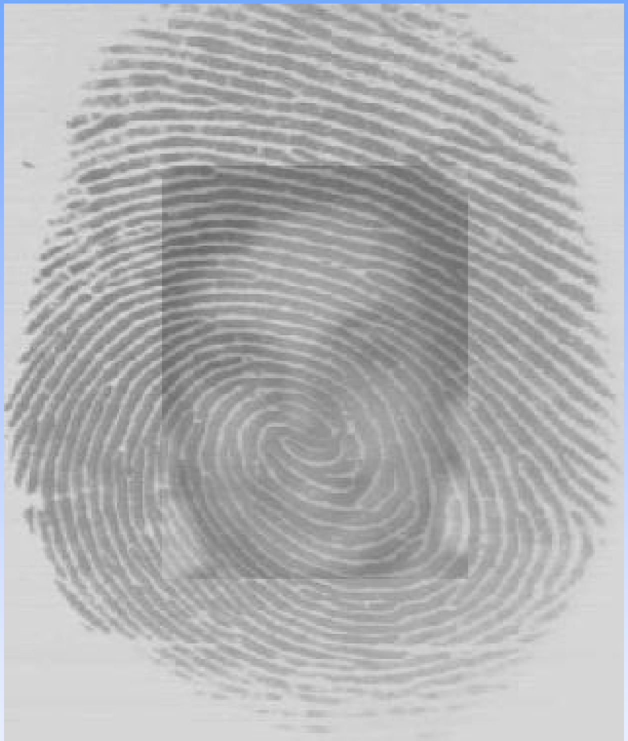
2. Replay Old Data

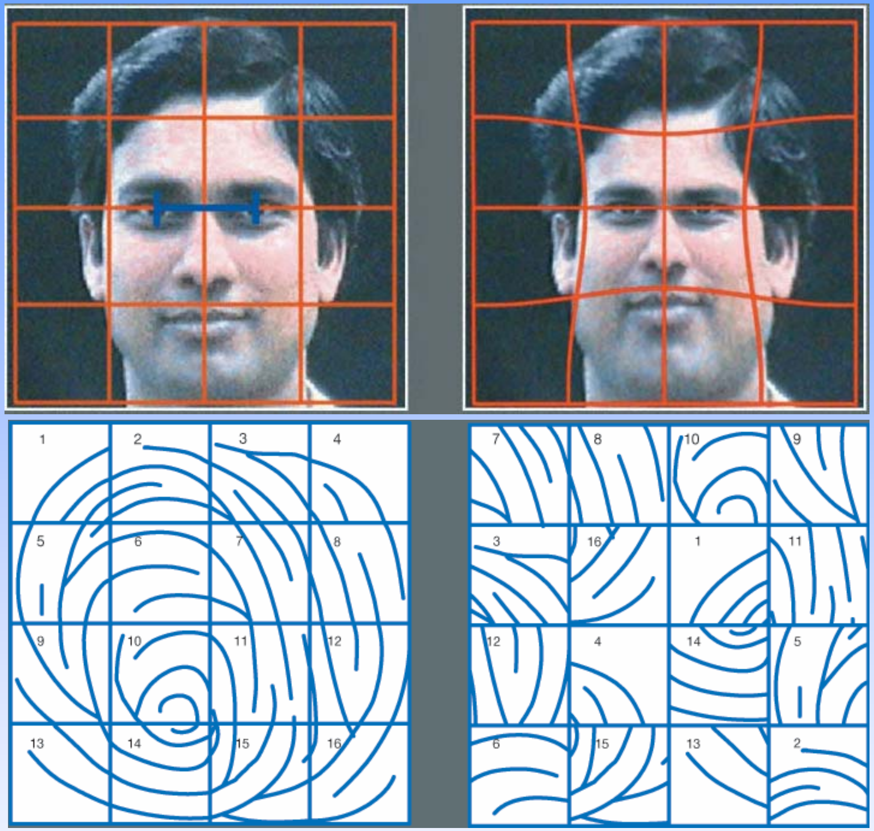
4. Synthesized Feature Vector

8. Override Final Decision

5. Override Matcher

Template Protection





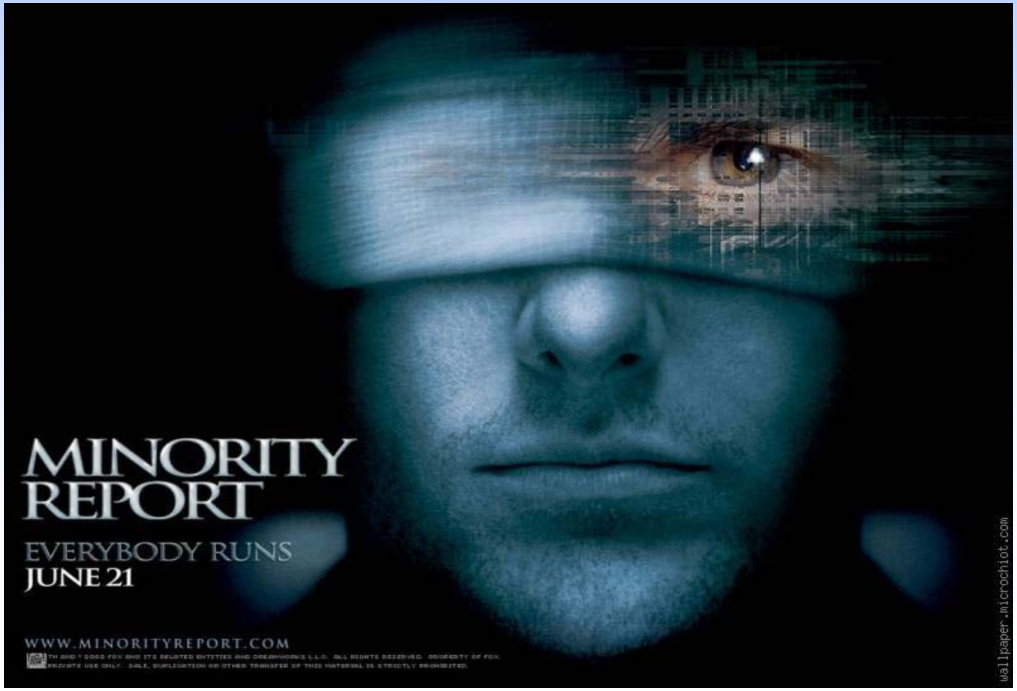
© *Ratha, Connell, Bolle (IBM)*

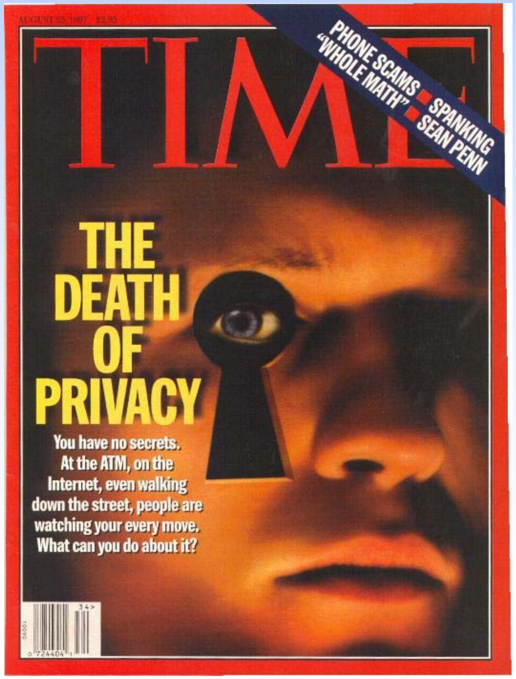
- Encrypting or watermarking templates in the database
- Storing only a transformed and unrecoverable version of a user’s template to protect the original template
- Cancelable biometric

Jain,Uludag, Hsu, "Hiding a Face in a Fingerprint Image", Proc. of ICPR, Aug., 2002
Ratha, Connell, Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM Systems Journal, vol. 40, no. 3, 2001, pp. 614-634.

Privacy Concerns

- Biometric can help in protecting individual privacy; because biometrics provides stronger identification than password, it can be used to guard personal & sensitive information (Health Information Privacy Protection Act)
- Will biometric data be used to track people (secretly) violating their right to privacy?
- Functionality creep: Will biometric data be used only for their intended purpose? Will various biometric databases be “linked”?




AUGUST 25, 1997 $2.95
TIME
PHONE SCAMS ■ SPANKING
“WHOLE MATH” ■ SEAN PENN
THE DEATH OF PRIVACY
You have no secrets. At the ATM, on the Internet, even walking down the street, people are watching your every move. What can you do about it?

Summary

- Reliable and automatic person identification is becoming a necessity; emerging applications include national ID card, border crossing, access control, Internet shopping, and computer data security
- There is no substitute to biometrics for effective person identification; it can enhance security, eliminate fraud and offer convenience to the users
- Biometrics is becoming a necessary component of ID management systems; need to make a business case
- Biometric sensors are cheap--fingerprint, face and voice sensors are embedded in laptops & mobile phones; system performance is not meeting the expectations
- Deployed systems should not infringe on civil liberties, so the citizens will not be concerned