Biometric Recognition: Overview and Recent Advances

Anil K. Jain

Dept. of Computer Science and Engineering

Michigan State University

http://biometrics.cse.msu.edu

Security Risks

Increased concerns/awareness at three levels

- National
  - Secure the borders
- Organizational/Enterprise
  - Identity and access management
- Personal
  - Preventing impersonation (ID theft)

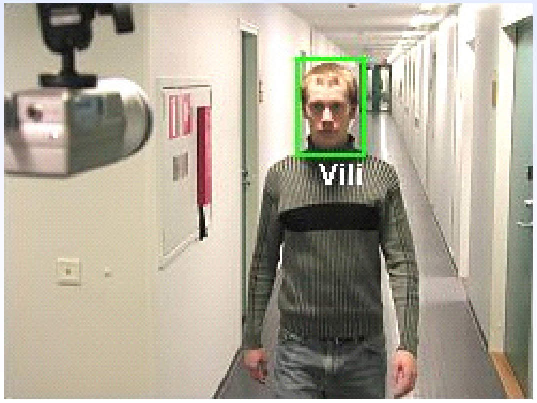
Securing National Borders

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

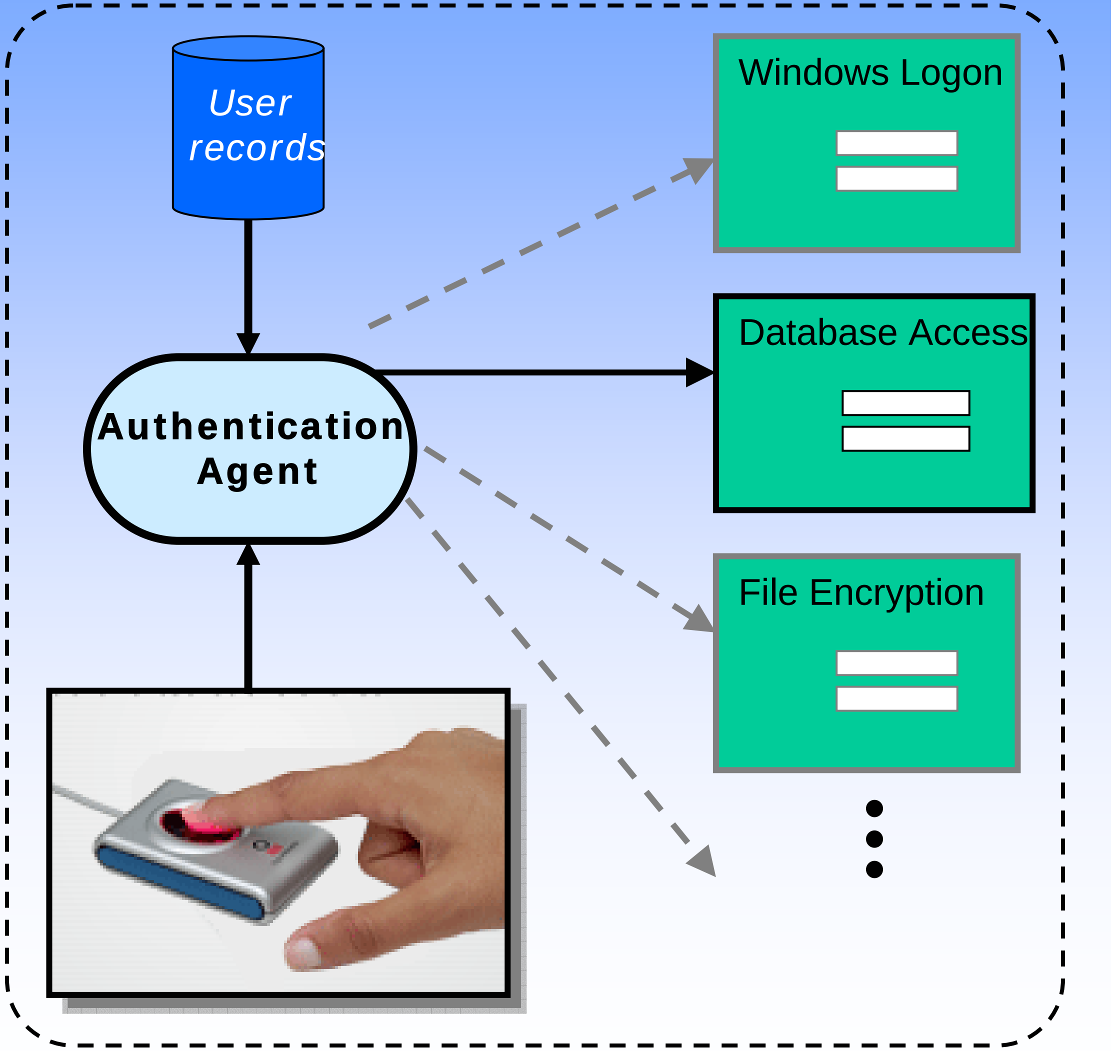
Enterprise Security

Physical Access

Surveillance



Logical Access



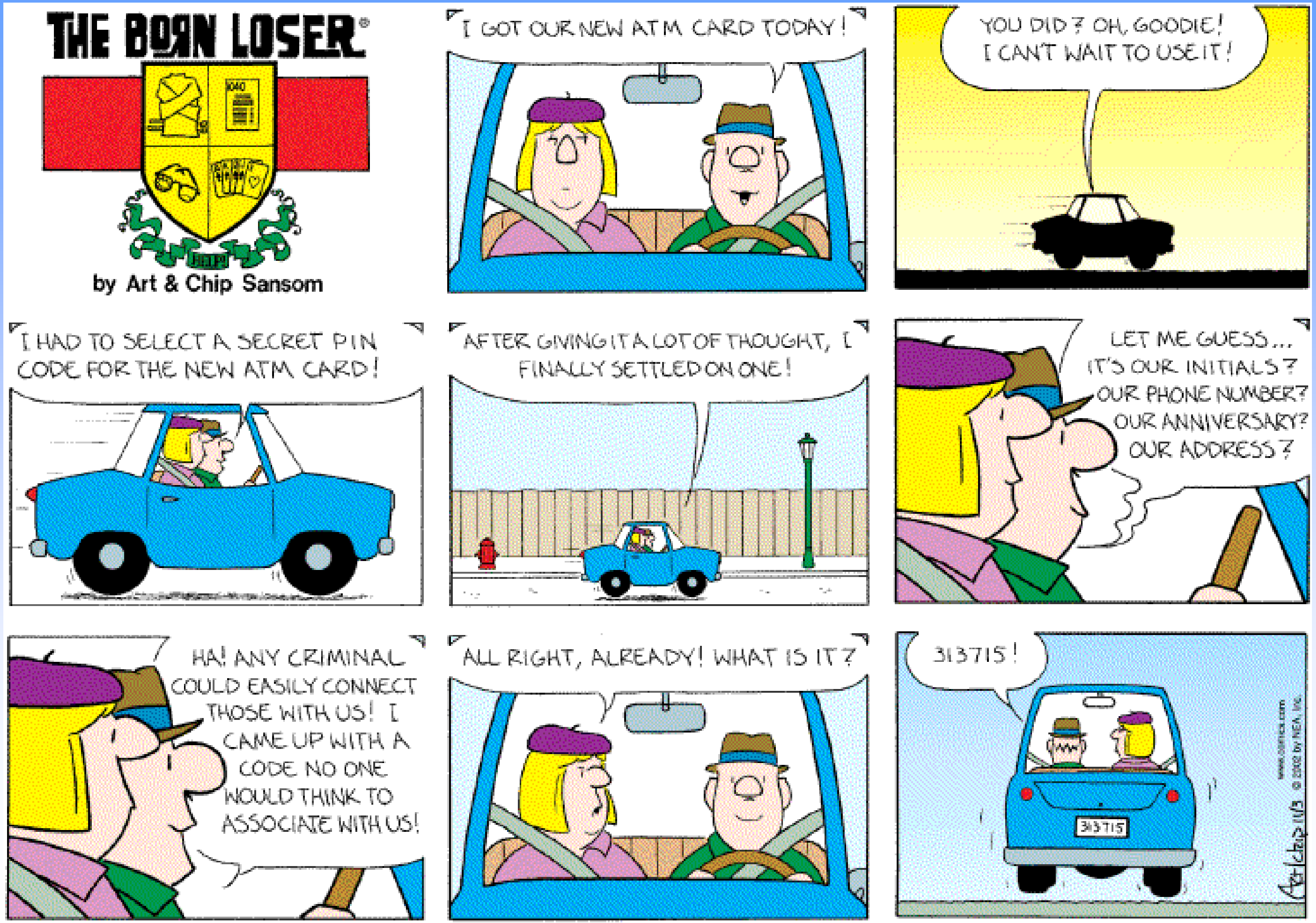
Personal Data Stolen

May 22, 2006 (Reuters) -- Personal data on 26.5 million U.S. veterans was stolen. The data included names, Social Security numbers and dates of birth for the military veterans and some spouses. *Computerworld*

300% annual growth rate in ID theft

IEEE Spectrum, July 2006

The Secret PIN!


THE BORN LOSER®
by Art & Chip Sansom
I GOT OUR NEW ATM CARD TODAY!
YOU DID? OH, GOODIE! I CAN'T WAIT TO USE IT!
I HAD TO SELECT A SECRET PIN CODE FOR THE NEW ATM CARD!
AFTER GIVING IT A LOT OF THOUGHT, I FINALLY SETTLED ON ONE!
LET ME GUESS... IT'S OUR INITIALS? OUR PHONE NUMBER? OUR ANNIVERSARY? OUR ADDRESS?
HA! ANY CRIMINAL COULD EASILY CONNECT THOSE WITH US! I CAME UP WITH A CODE NO ONE WOULD THINK TO ASSOCIATE WITH US!
ALL RIGHT, ALREADY! WHAT IS IT?
313715!
313715
www.comics.com © 2002 by NEA, Inc.
Art+Chip 11/3

Protecting Passwords

- 30% of customers write their PIN number on the back of ATM cards
- “A recent survey in London 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

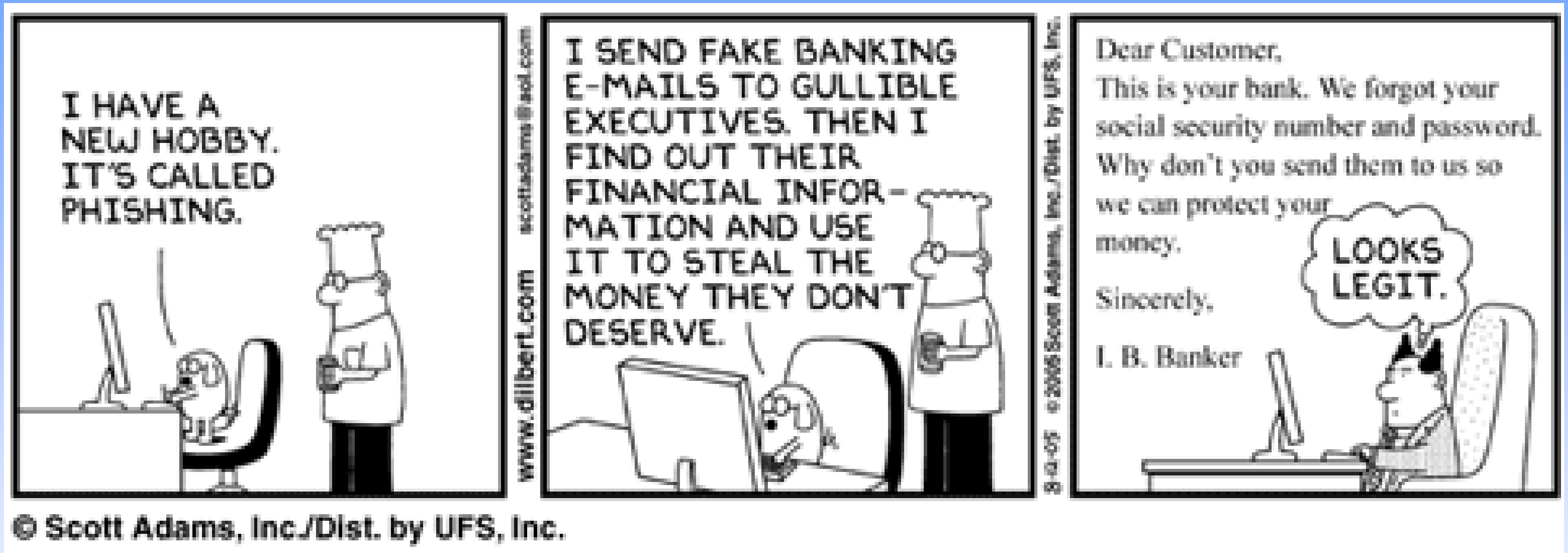
Too Many Passwords!

Copyright 1996 Randy Glasbergen. www.glasbergen.com

"Sorry about the odor. I have all my passwords tattooed between my toes."

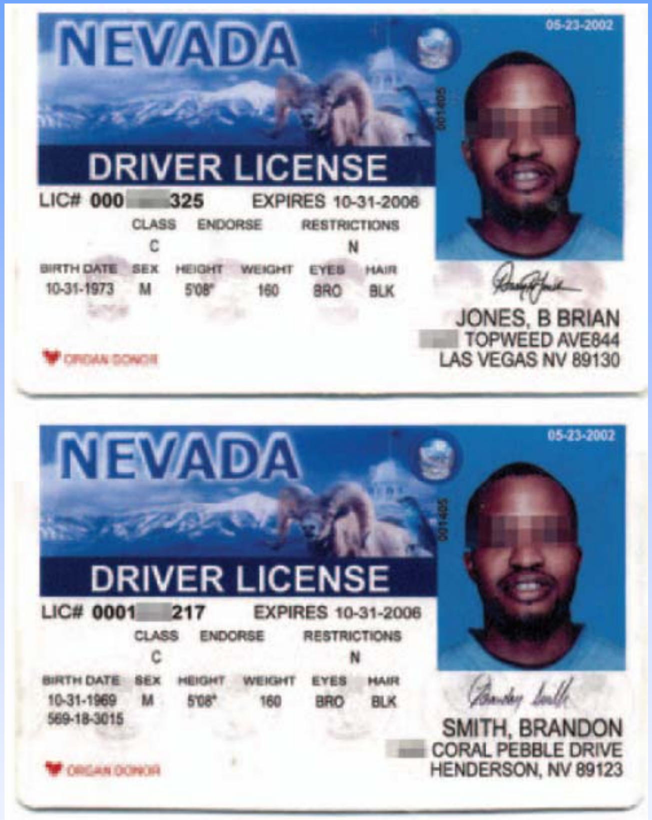
The most common pw is the word "password" *(2002 NTA Monitor Password Survey)*

Phising


I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
scottadams@aol.com
www.dilbert.com
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
© 2005 Scott Adams, Inc./Dist. by UFS, Inc.
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.

© Scott Adams, Inc./Dist. by UFS, Inc.

“Fungible” Credentials



NEVADA

DRIVER LICENSE

05-23-2002

LIC# 000[redacted]325 EXPIRES 10-31-2006

CLASS	ENDORSE	RESTRICTIONS
C		N

BIRTH DATE	SEX	HEIGHT	WEIGHT	EYES	HAIR
10-31-1973	M	5'08"	160	BRO	BLK

JONES, B BRIAN
[redacted] TOPWEED AVE844
LAS VEGAS NV 89130

ORGAN DONOR

NEVADA

DRIVER LICENSE

05-23-2002

LIC# 0001[redacted]217 EXPIRES 10-31-2006

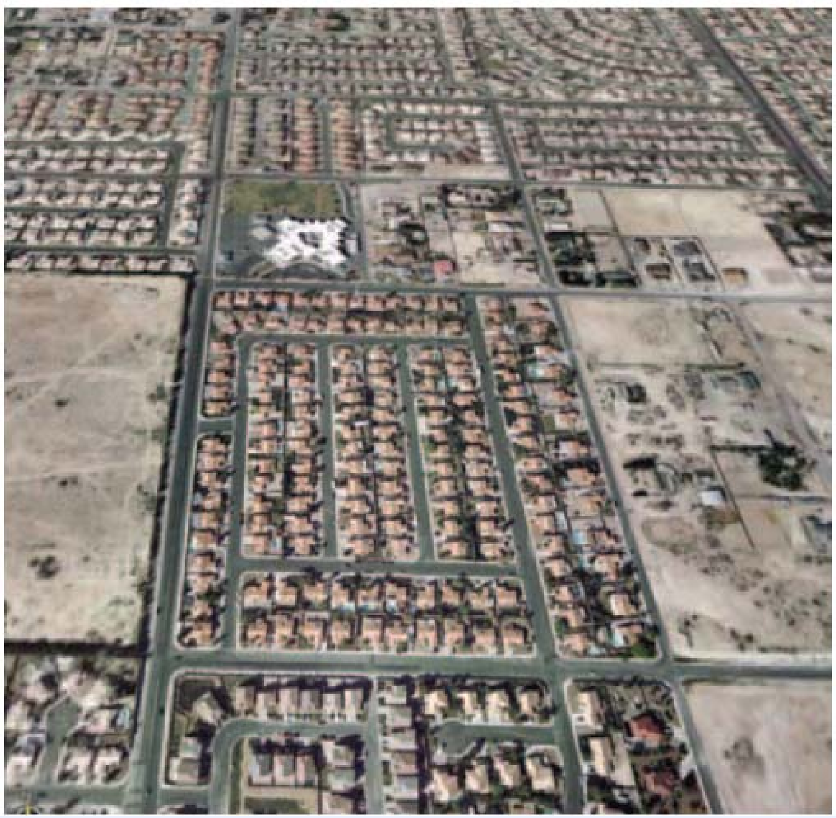
CLASS	ENDORSE	RESTRICTIONS
C		N

BIRTH DATE	SEX	HEIGHT	WEIGHT	EYES	HAIR
10-31-1969 569-18-3015	M	5'08"	160	BRO	BLK

SMITH, BRANDON
[redacted] CORAL PEBBLE DRIVE
HENDERSON, NV 89123

ORGAN DONOR

Two counterfeit driver’s licenses for the same person. Both identities are fictitious



A satellite image of the Topweed neighborhood. Note absence of apartment buildings

Source: Comm. of ACM, Dec. 2006

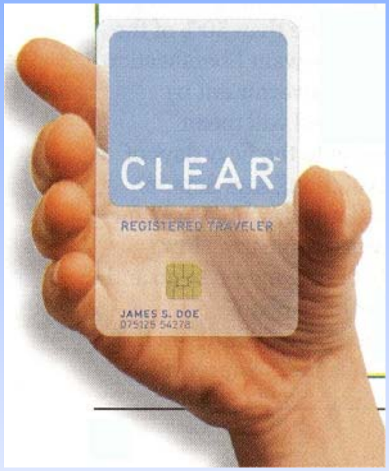
How Do I know Who You Are?

Surrogate representations of identity based on “what you know” (PINS, Passwords) or “what you have” (keys, cards) cannot be trusted

Biometric Recognition

Person recognition based on "who you are"

Stephen J. Boitano, AP



Recognition of a person by his body, then linking that body to an externally established "identity", is being adopted for identity management

Why Biometrics?

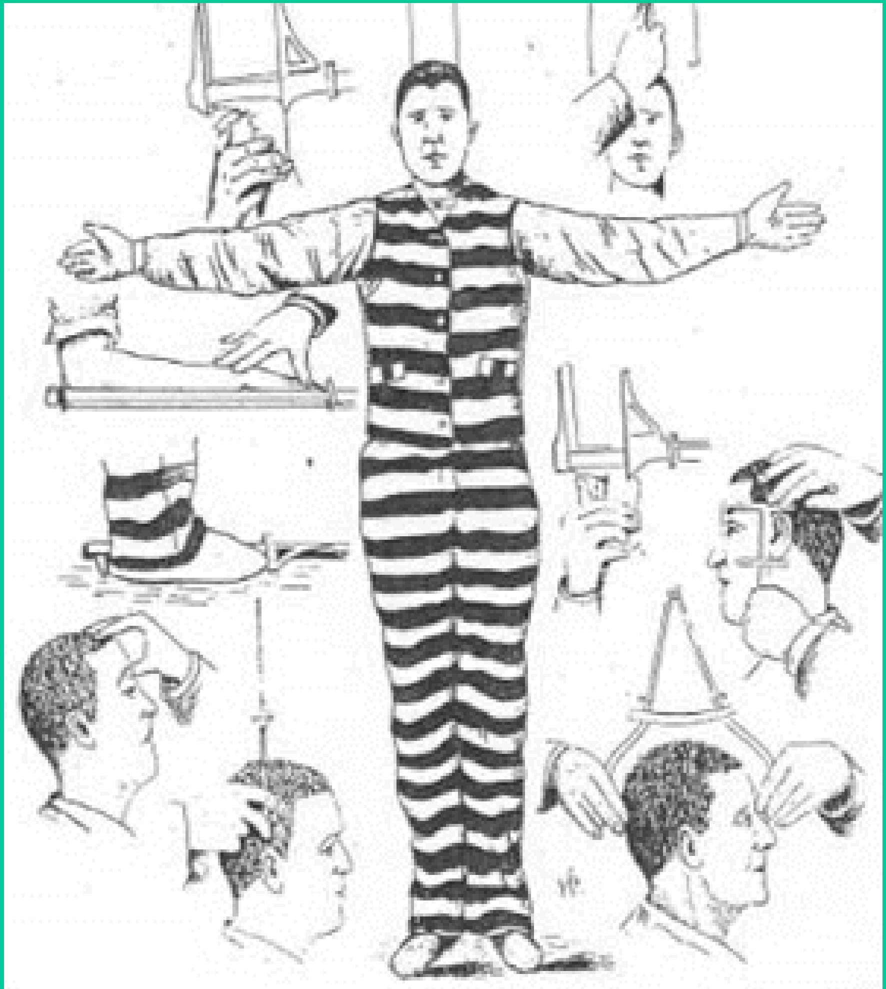
- Discourages fraud
- Enhances security
- Cannot be transferred, forgotten, lost or (easily) copied
- Eliminates repudiation claims
- Imparts convenience to users

Biometric Milestones

Galton

Fin
pe

300
B.C.



)01

A
of sale w
fingerprint

Bertillonage
invented

lc

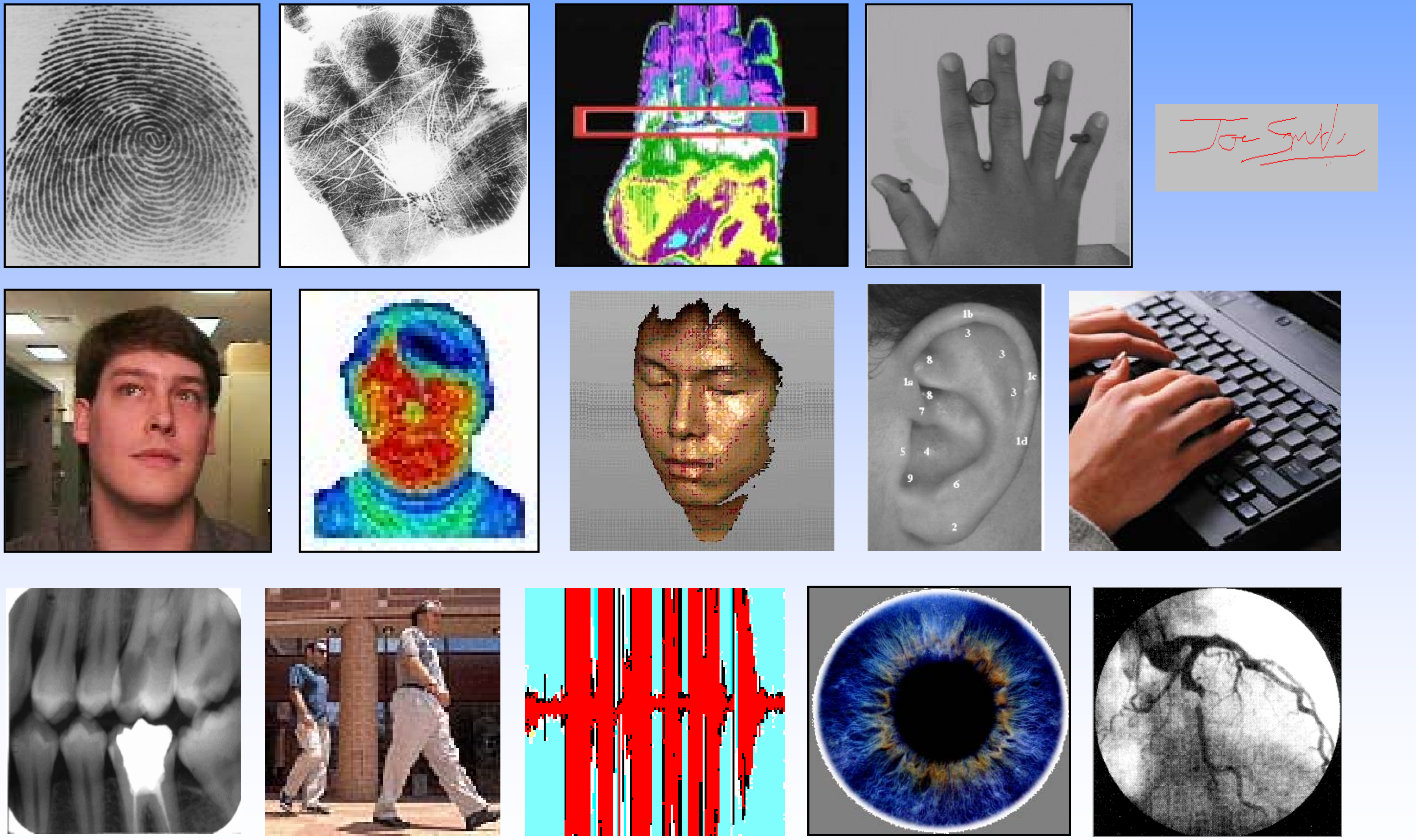
的

EEE (1971)

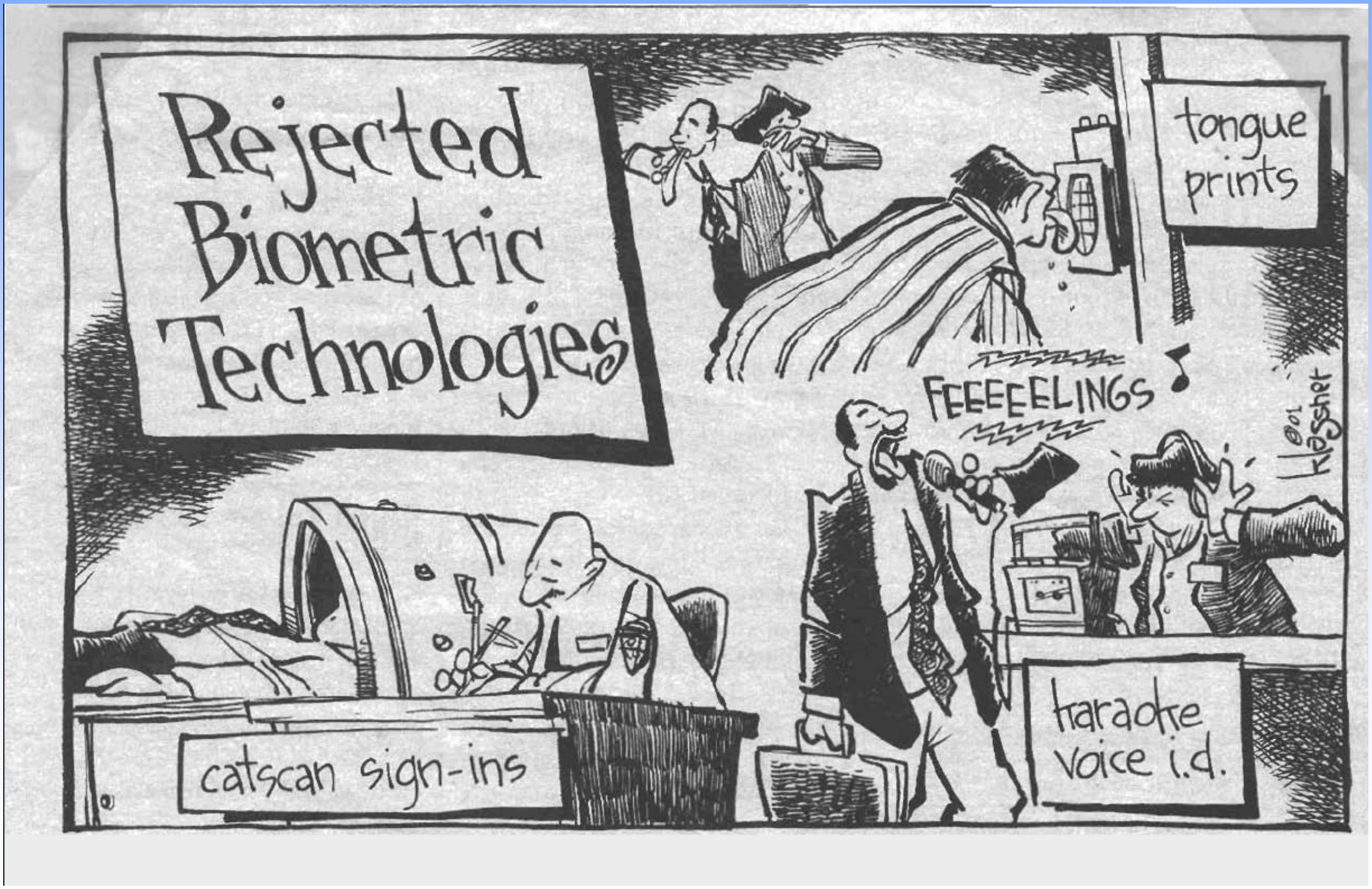
s

Courtesy: John D. Woodward, RAND Corporation

Biometric Traits



New Biometric Traits?



Which Biometric is the Best?

- **Universality** (everyone should have this trait)
- **Uniqueness** (everyone has a different value)
- **Permanence** (should be invariant with time)
- **Collectability** (can be measured quantitatively)
- **Performance** (achievable recognition accuracy, resources required, operating environment)
- **Acceptability** (are people willing to accept it?)
- **Circumvention** (how easily can it be spoofed?)

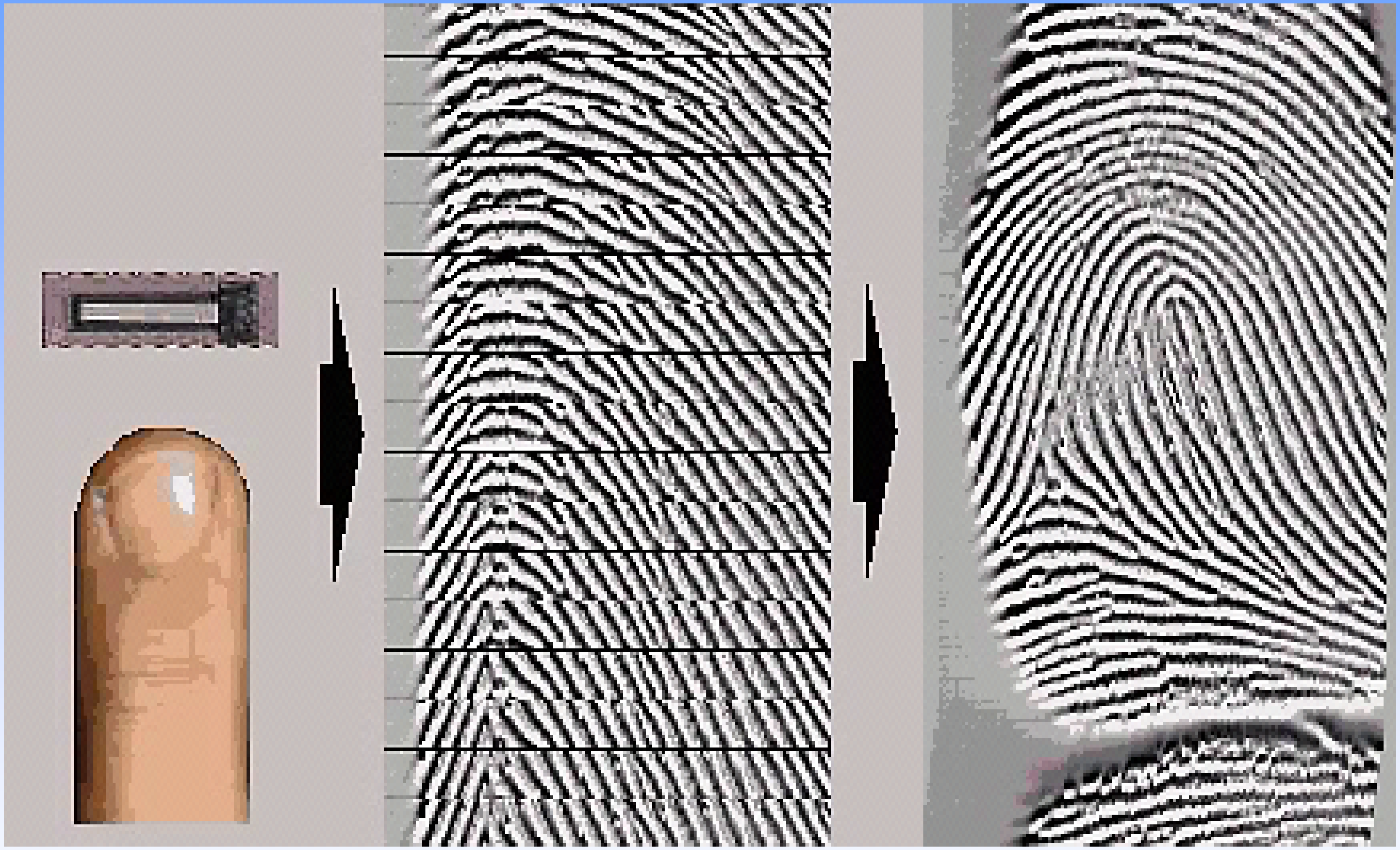
Choice of a biometric trait is domain dependent

Biometric Applications

Forensic	**Government**	**Business**
Corpse Identification	National ID Card E-passports	ATM Time/Attendance
Criminal Investigation	Driver’s License Voter Registration	Access Control Computer Login
Parenthood Determination	Welfare Disbursement	Cellular Phone
Missing Children	Border Crossing* US-VISIT program Guest Worker ID	E-commerce Internet Banking Smart Card

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

Live Scan Capture



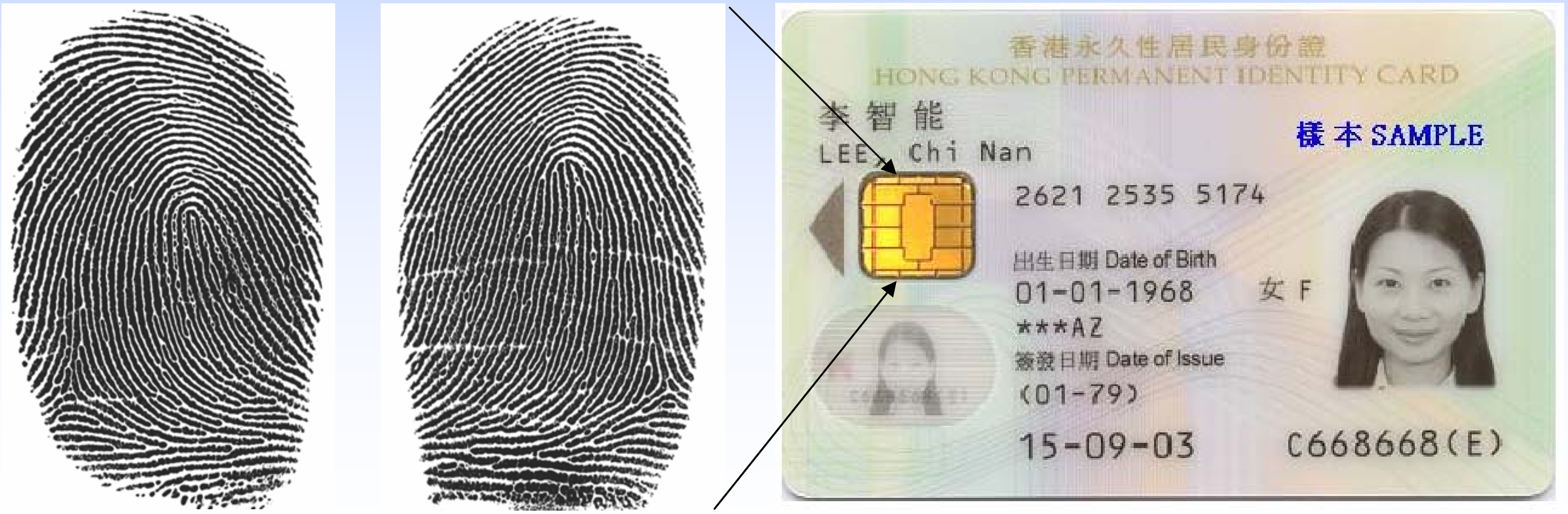
Sensors based on optical, ultrasound, thermal, solid-state, multispectral technologies

Hong Kong Smart Identity Card

HK Smart ID Card

Templates of two thumbprints stored in the chip

- Security: prevent misuse of lost cards
- Convenience: e-Certificate
- Service: delivery of electronic government services
- Travel: Automated Passenger Clearance System



Brazilian Elections: Voting Machines

- Voting machines in 2008 will have fingerprint ID
- TSE (Tribunal Superior Eleitoral) has already purchased 25,000 new voting machines
- System will cover ~125 million Brazilian electors

http://idgnow.uol.com.br/seguranca/2006/08/30/idgnoticia.2006-08-29.2323285944/IDGNoticiaPrint_view

Disney World, Orlando

Throughput: 100K/day, 365 days/ year

Iris Recognition at Schiphol Airport (Netherlands)

Automatic border passage system:

- Iris image of the user is encoded on the chip in a smart card
- When user enters the country, his iris image is matched with template on the smart card
- Passengers from European Economic Area (EEA) are eligible to use the system

“In a list of the greatest scientific achievements over the past 50 years compiled by a panel of leading British scientists to mark Queen Elizabeth II’s golden jubilee, the system at Schiphol was elected the innovation for the year 2002”

www.airport-technology.com/projects/schiphol

Hand Geometry – Time Attendance

Hilton Waterfront Beach Resort

- Eliminates “buddy punching” (one employee clocks in for another)
- Tracks time and attendance for more than 330 employees
- Eliminates the need to carry a badge; employees can’t lose or forget their hands, so it saves time and money

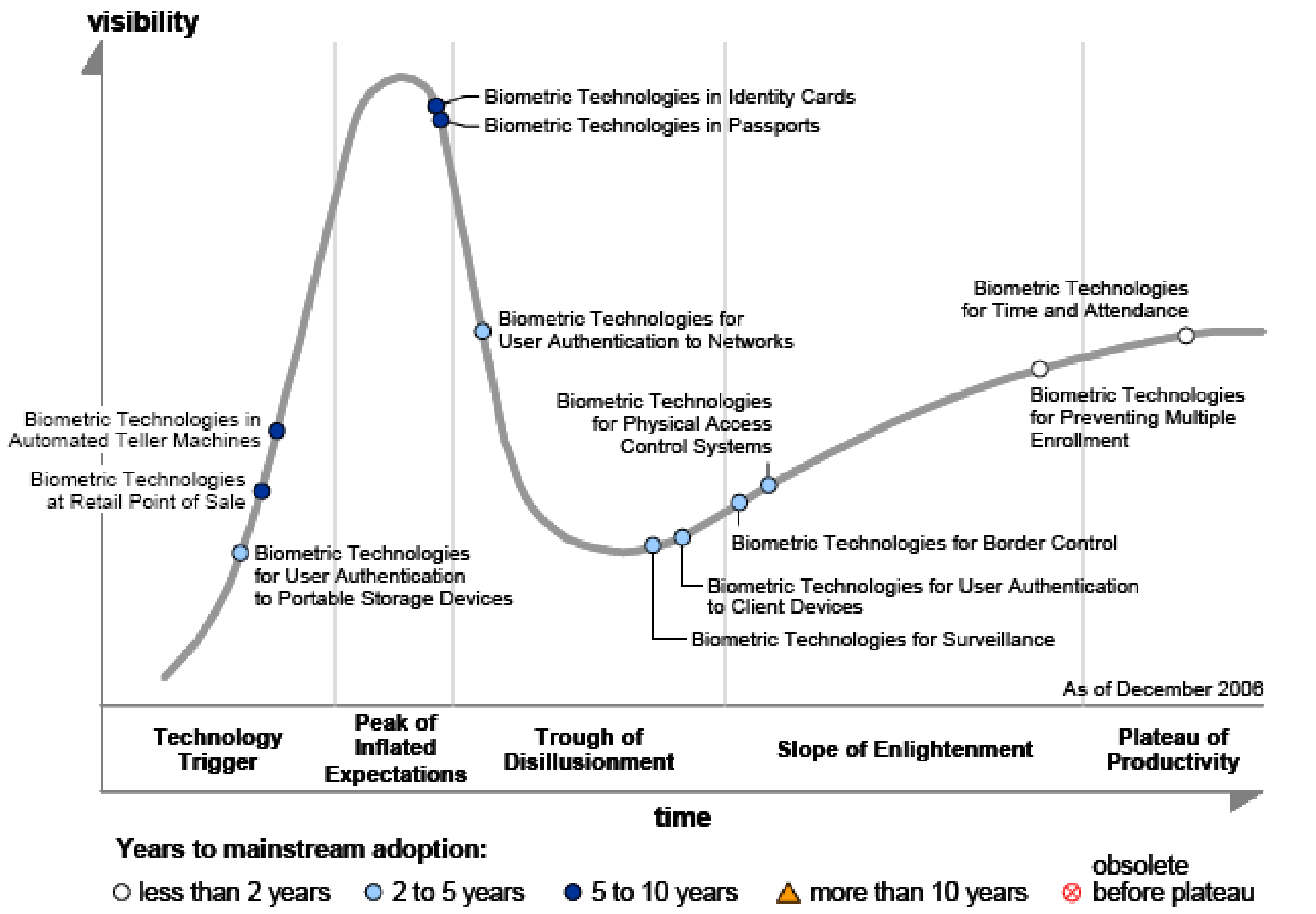
http://www.recognitionsystems.ingersollrand.com/news/pr.php?id=73

Iris on the Move

- Current commercial systems require:
  - close proximity of the sensor to the eye
  - significant cooperation from subjects
- Iris on the move
  - Subjects walk through a recognition portal at normal walking pace
  - Can identify up to 20 subjects per minute

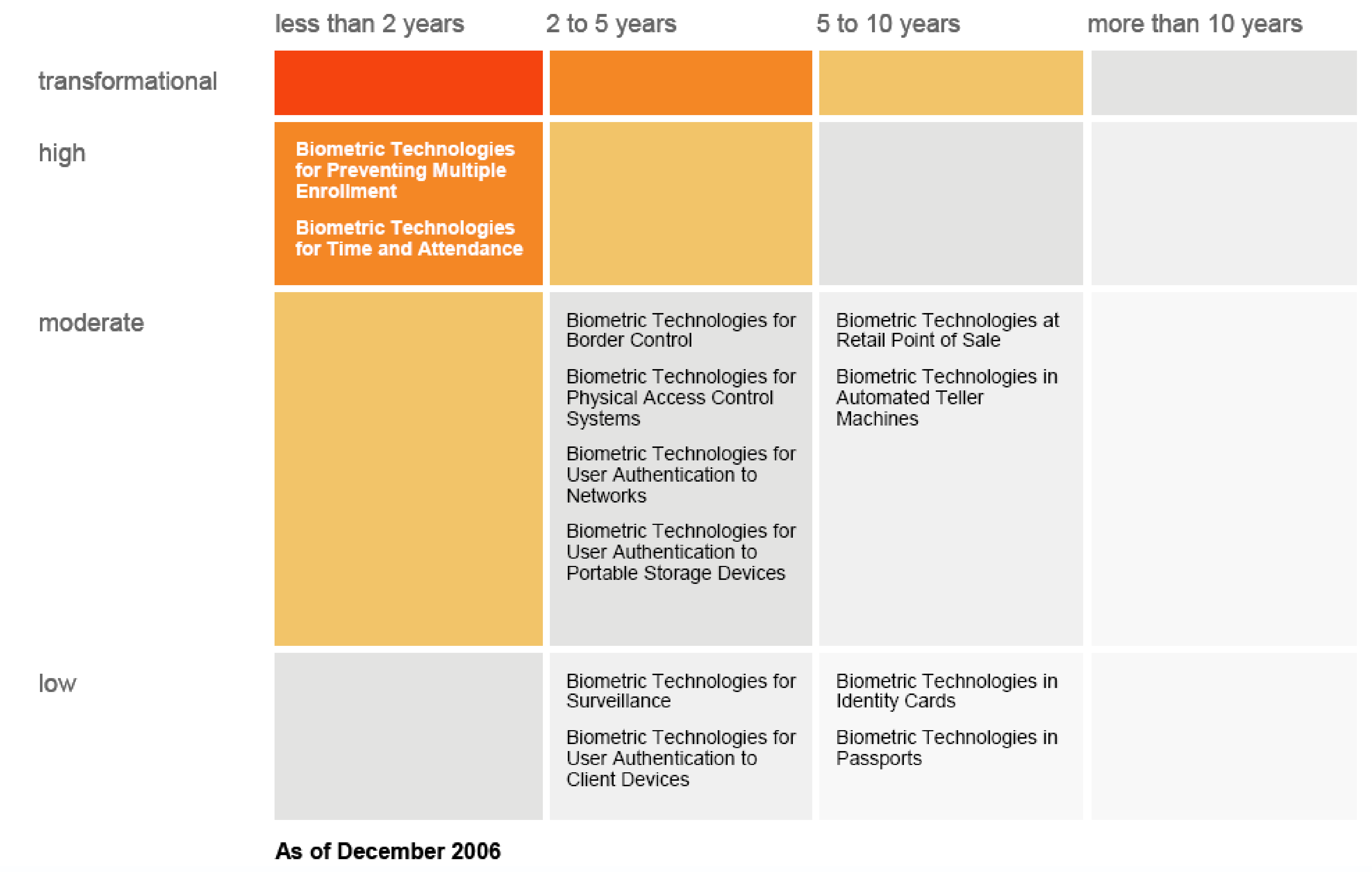
http://www.sarnoff.com/products_services/government_solutions/homeland_security/iris.asp

Hype Cycle for Biometric Technologies[1]



[1] Gartner Research Report, December 21, 2006, ID Number: G0014118

Hype Cycle for Biometric Technologies[1]



	less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational				
high	**Biometric Technologies for Preventing Multiple Enrollment** **Biometric Technologies for Time and Attendance**			
moderate		Biometric Technologies for Border Control Biometric Technologies for Physical Access Control Systems Biometric Technologies for User Authentication to Networks Biometric Technologies for User Authentication to Portable Storage Devices	Biometric Technologies at Retail Point of Sale Biometric Technologies in Automated Teller Machines	
low		Biometric Technologies for Surveillance Biometric Technologies for User Authentication to Client Devices	Biometric Technologies in Identity Cards Biometric Technologies in Passports	

As of December 2006

[1] Gartner Research Report, December 21, 2006, ID Number: G0014118

Telltale Fingertips[2]

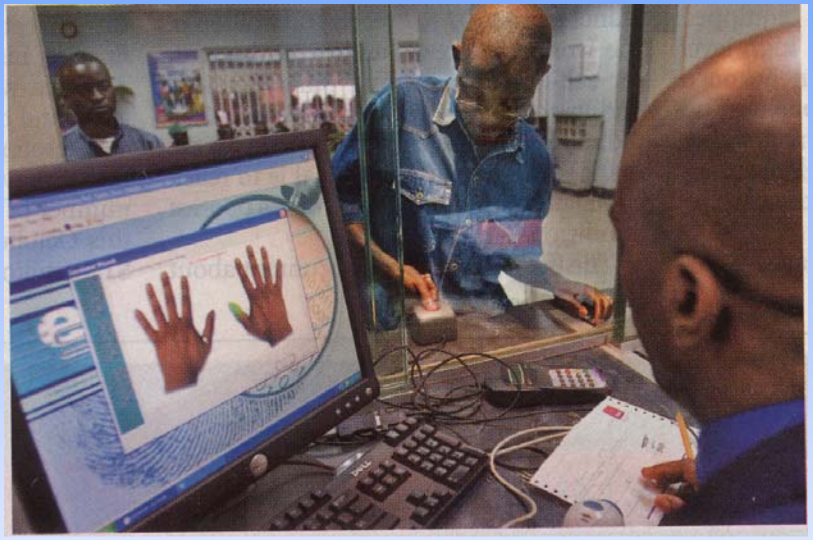
- With biometrics, how you type can allow websites to know who you are – or aren't
- Keystroke patterning was first employed by the military a century ago in its use of Morse code, which also allows senders to be identified by their typing rhythms

[2] Kathleen Kingsbury, "Telltale Fingertips", Time Bonus Section, page A10, January 2007

PAY BY TOUCH™

Customer pay by fingerprints; no need for cards/cash

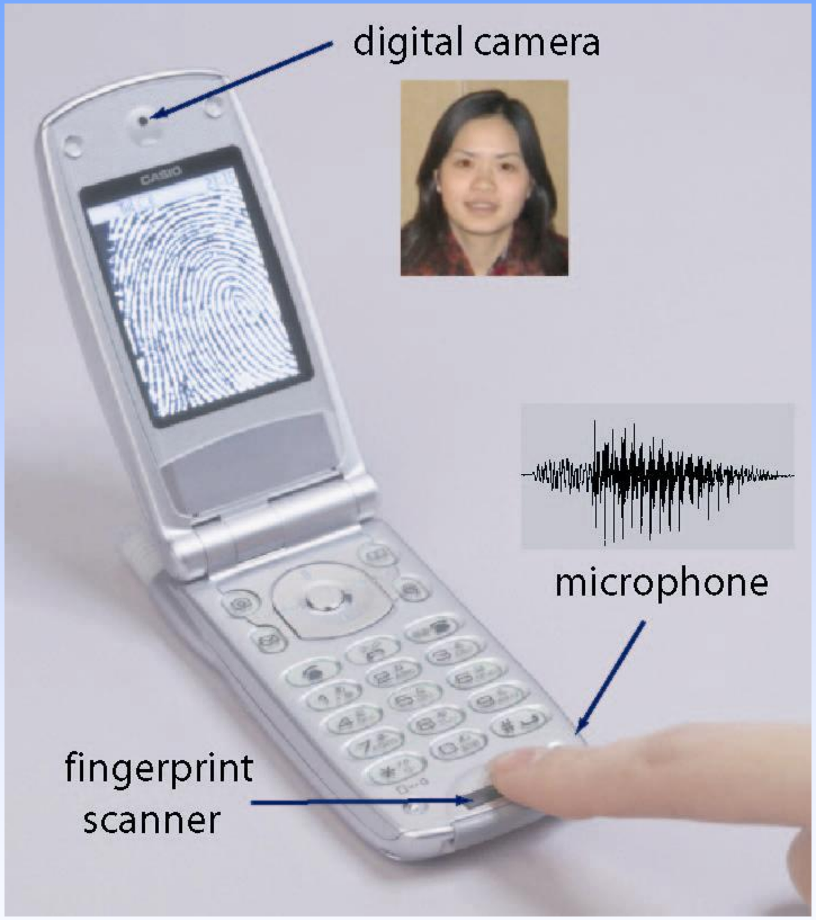
Biometric Applications



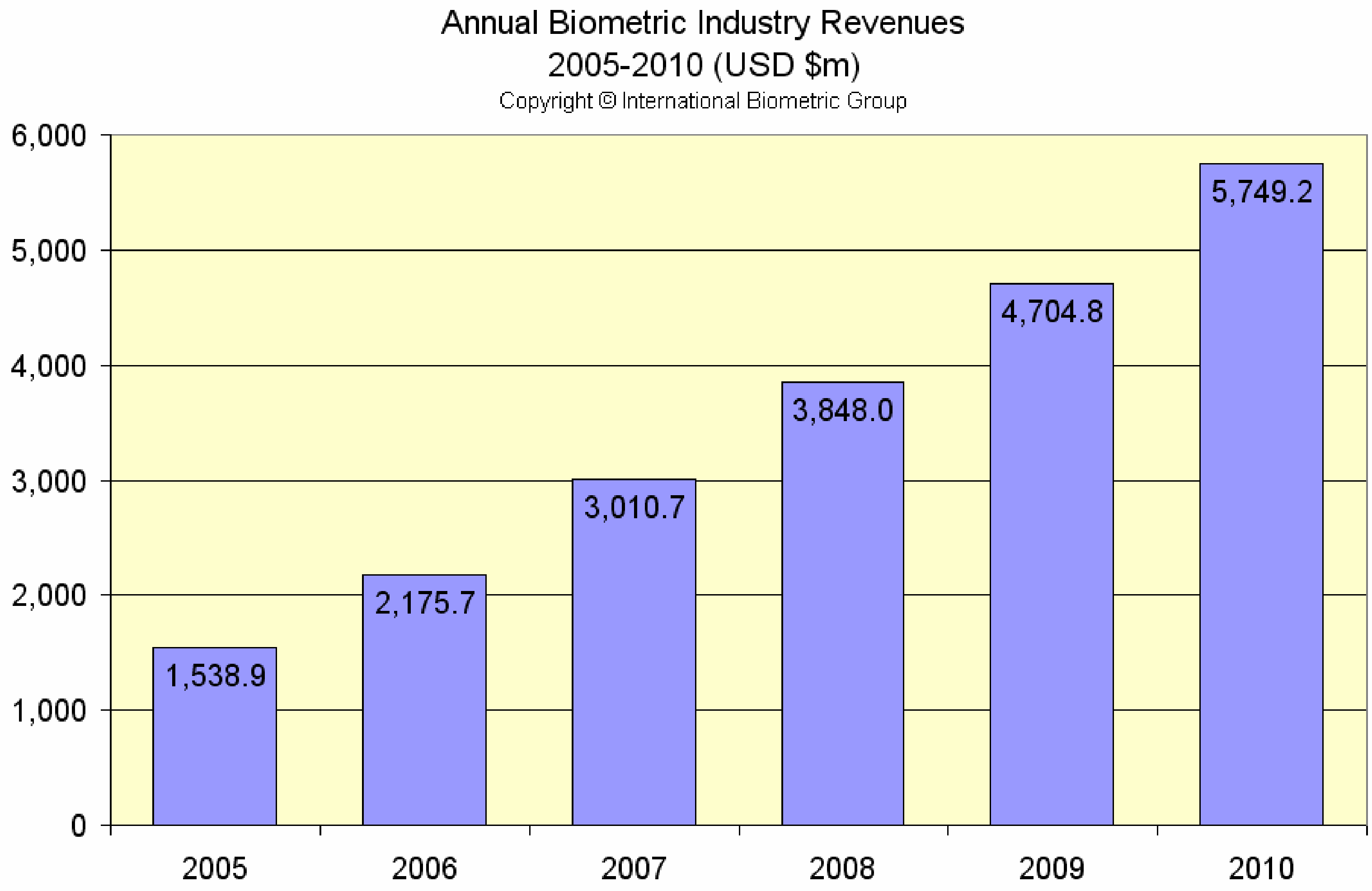
Bank in Malawi uses fingerprint smart cards for microloans

Securing Wireless Devices

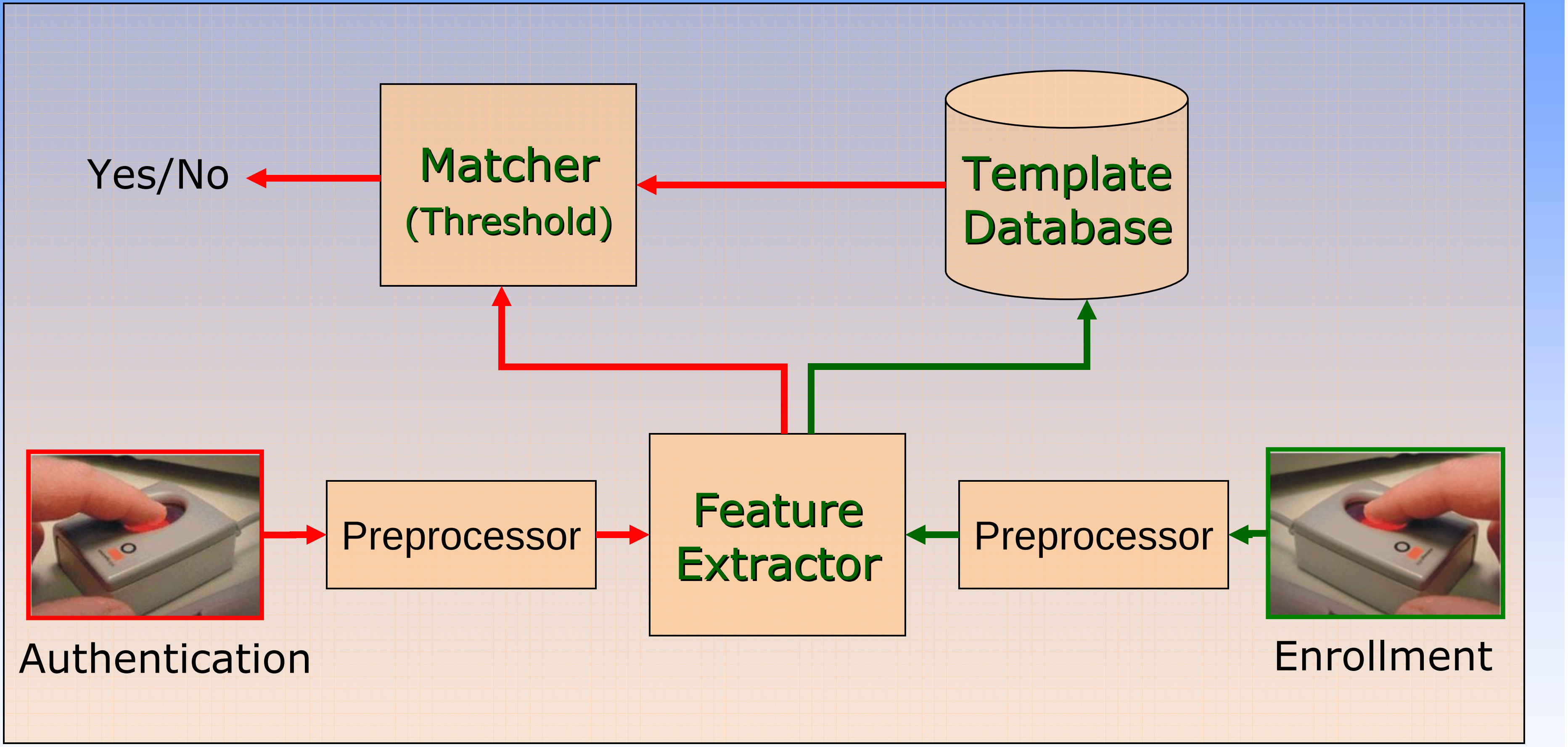
- AuthenTec has sold 10 million fingerprint sensors world-wide to provide secure authentication for mobile commerce and mobile banking



Biometric Market Growth



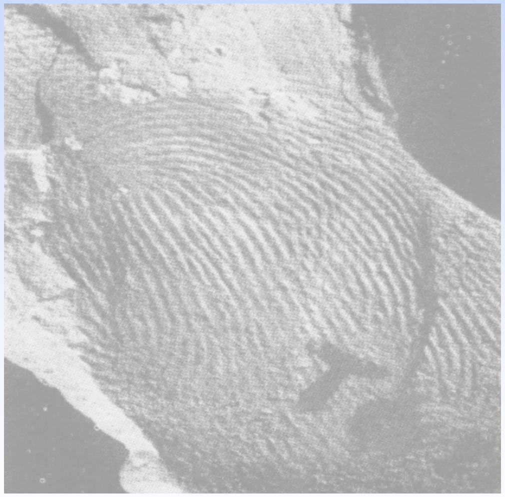
Biometric Recognition System



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

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

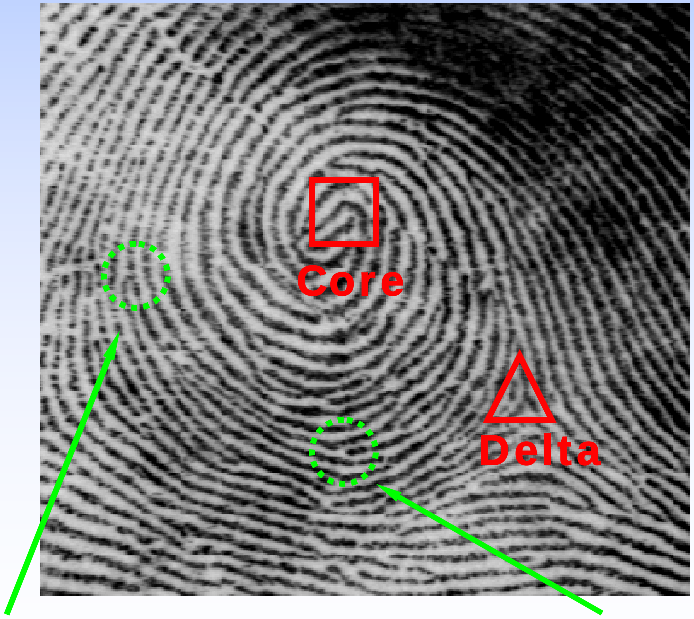


Fingerprint on Palestinian lamp (400 A.D.)

Identical Twins

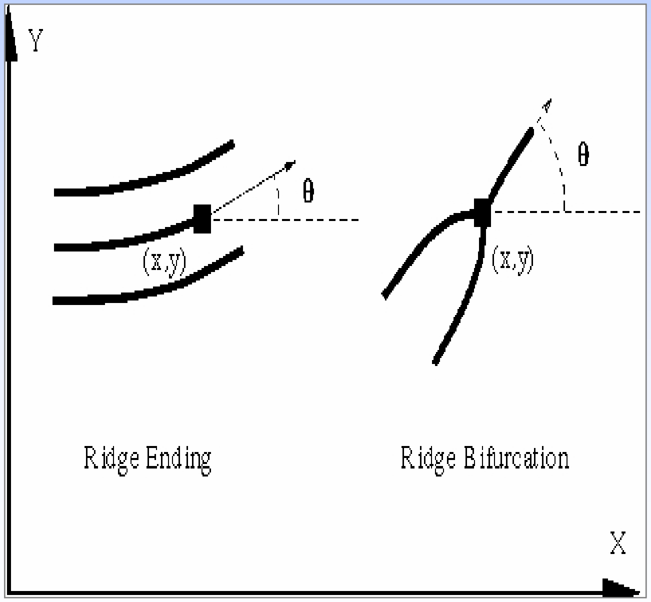
Representation

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



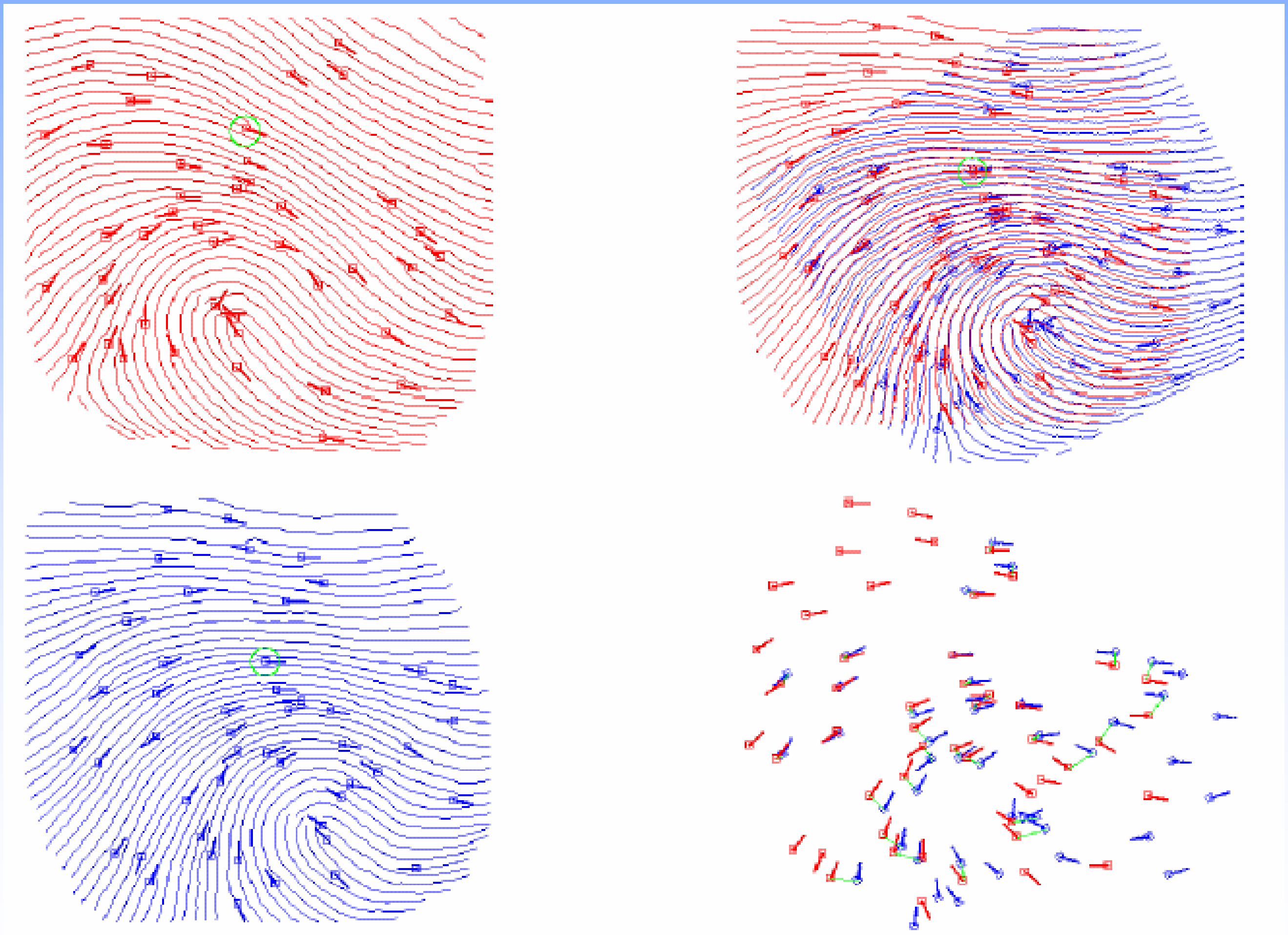
Ridge Bifurcation

Ridge Ending

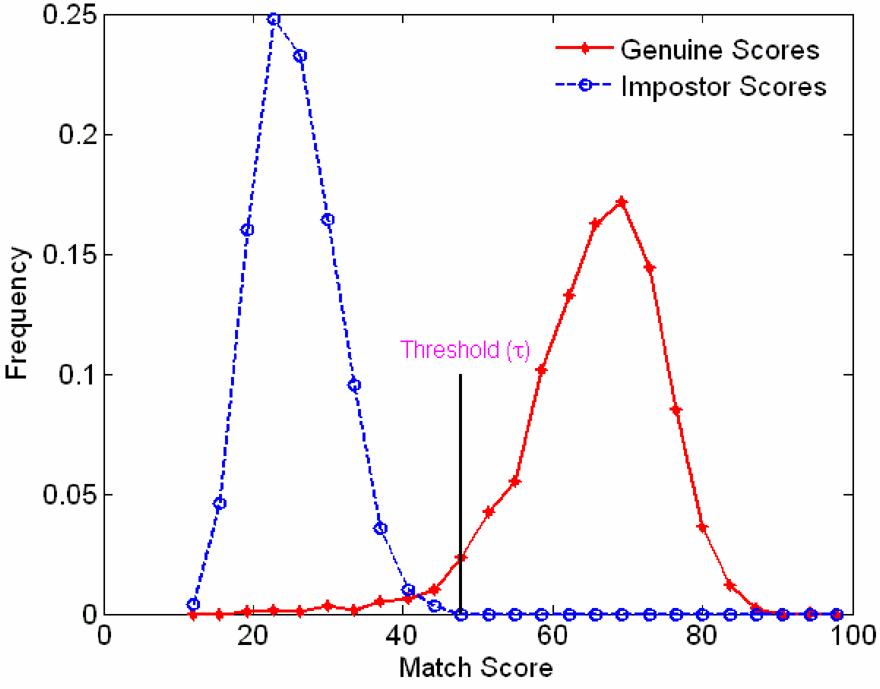


Minutiae-based Matchers

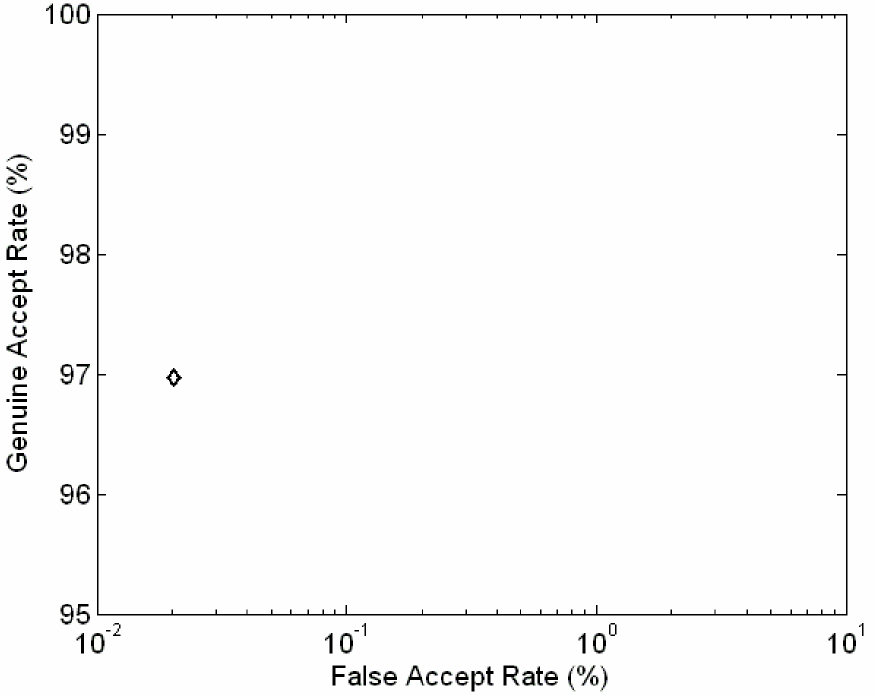
Find the number of corresponding minutiae in template and query



Match Scores



Match Score Distribution

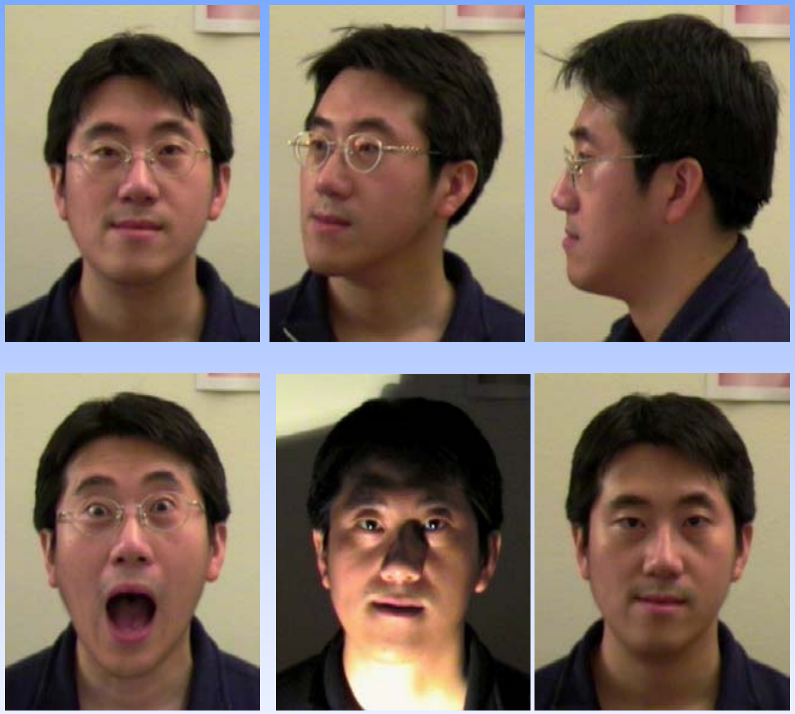


ROC Curve

Challenges

- Invariant representation
- Segmentation
- Noisy data/Non-universality
- Robust matching
- Large Database
- Securing biometric system
- Protect user privacy

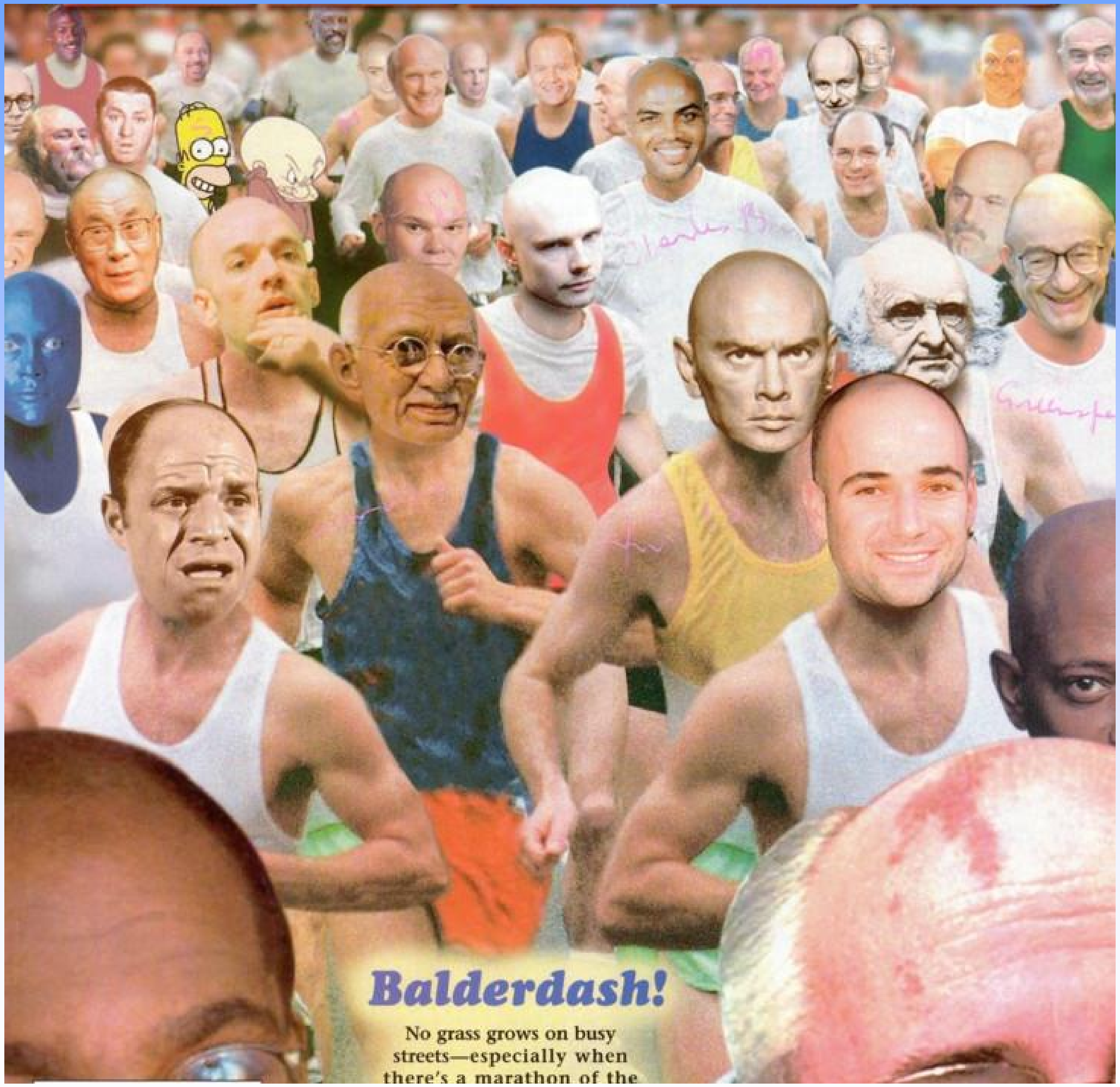
Representation



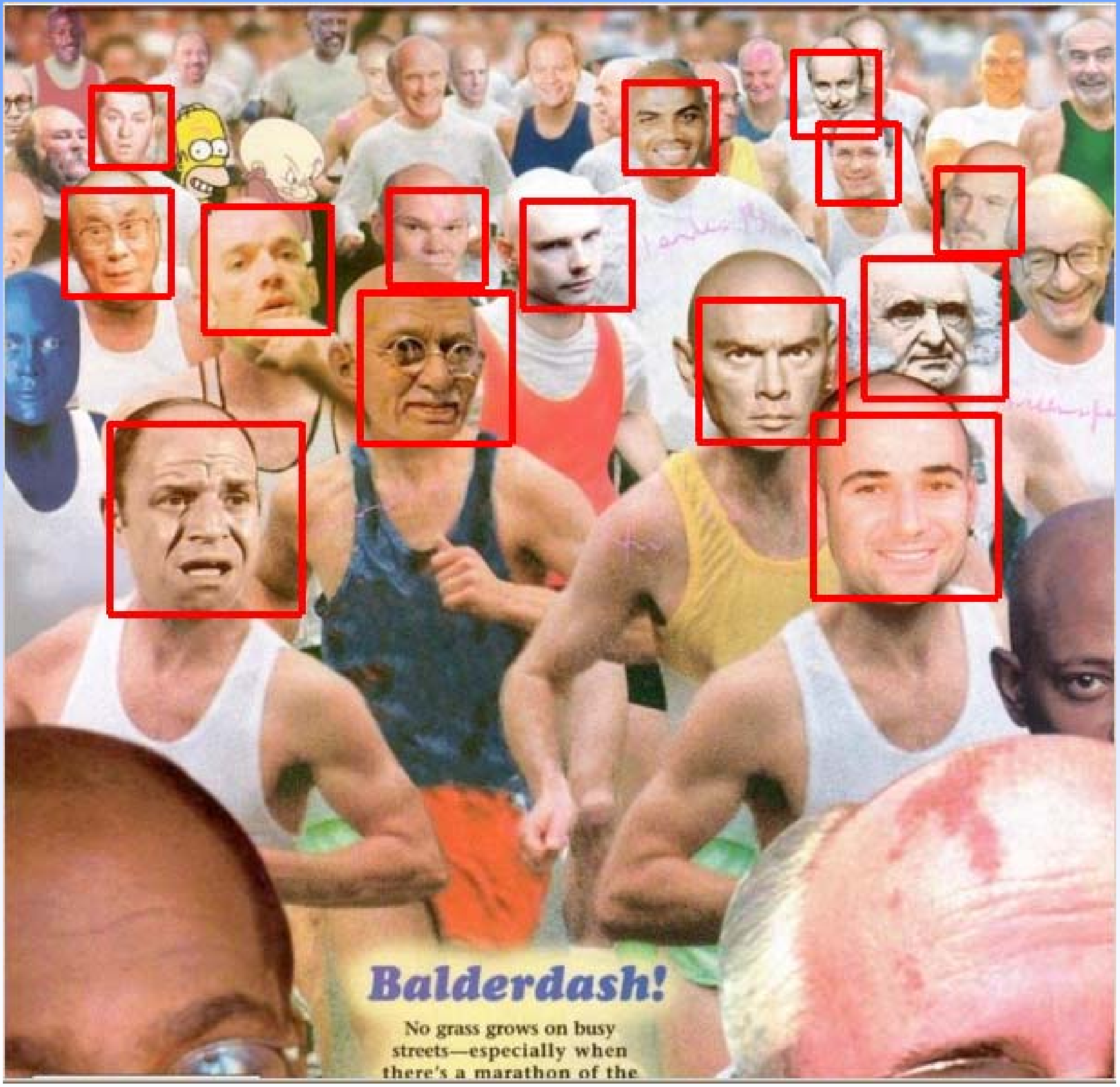
Variability in the facial image of a single person due to changes in pose, expression, lighting and glasses
(large intraclass variability)

Identical twins
(large interclass similarity)

Segmentation



Segmentation



Template Update

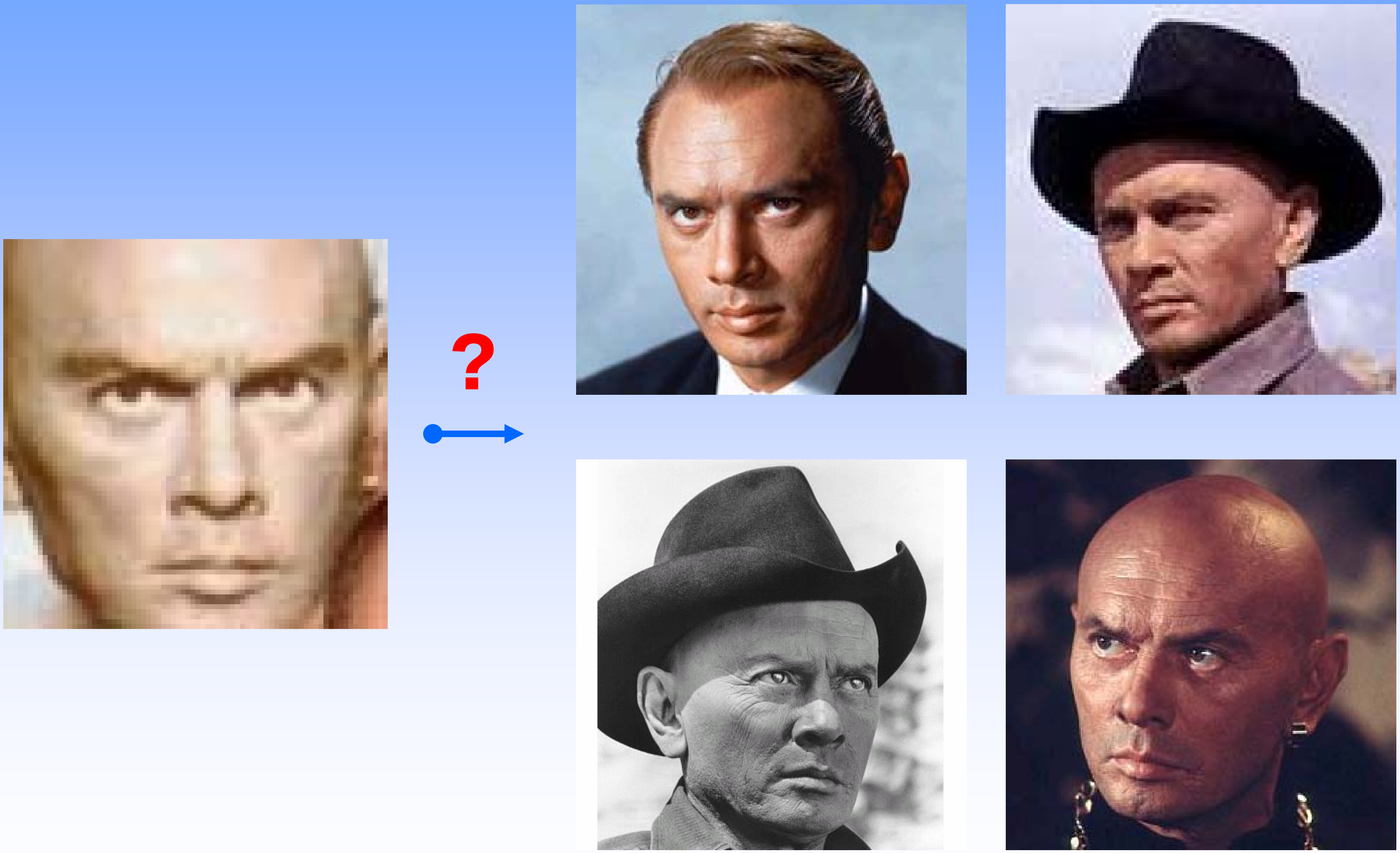
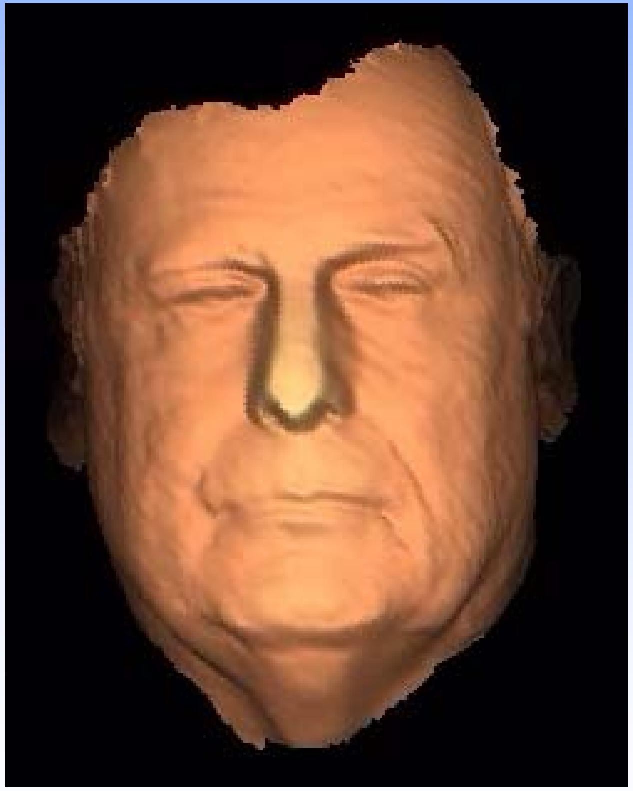
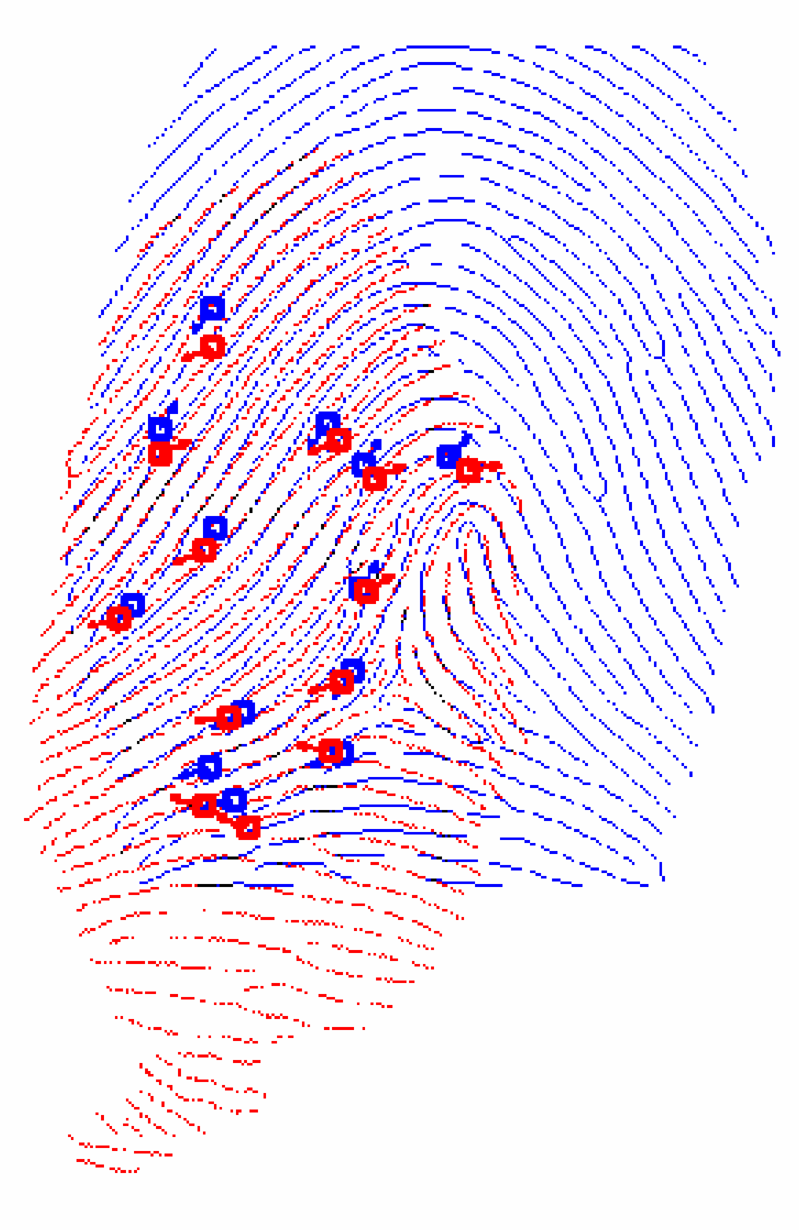


Image Deformation

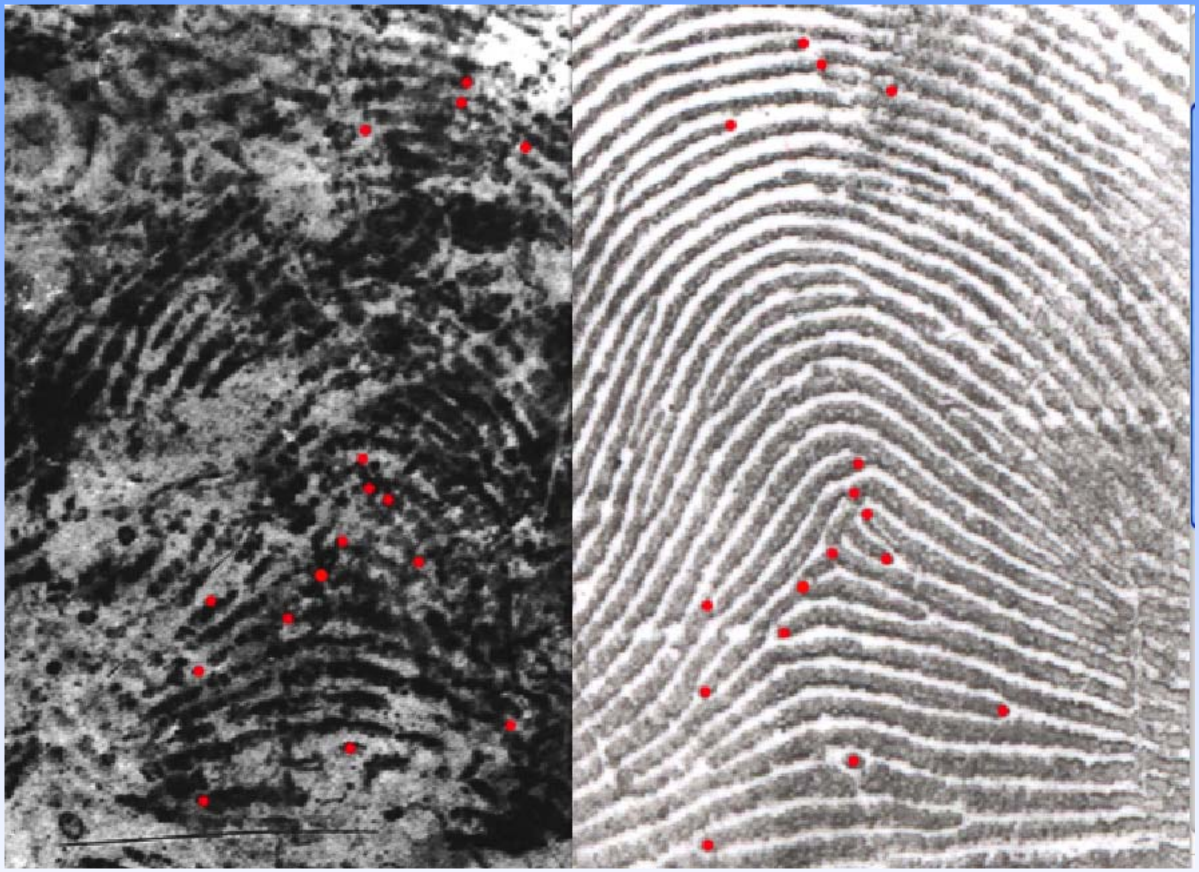
Large intra-class variation



Alignment



False Match

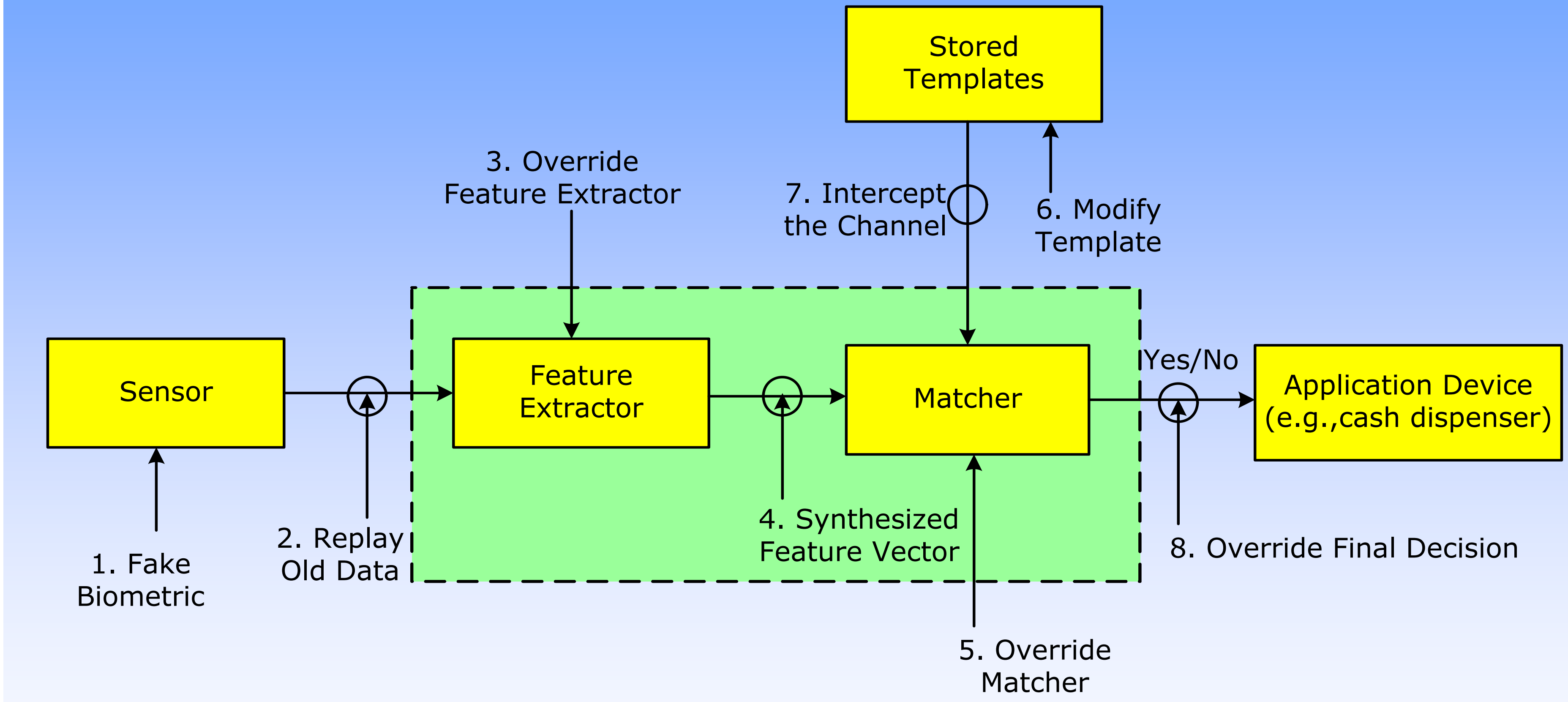


Mayfield's fingerprints were mistakenly matched with those found on a bag at the bombing site in Spain

“State-of-the-art” Error Rates

	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2004]	Exaggerated distortion	2%	2%
	FpVTE [2003]	US govt. operational data	0.1%	1%
Face	FRVT [2002]	Varied lighting, outdoor/indoor	10%	1%
	FRGC [2006]	Time lapse, varied lighting/expression, outdoor/indoor	10%	0.1%
Iris	ITIRT [2005]	Indoor environment, multiple visits	0.99%	0.94%
Voice	NIST [2004]	Text independent, multi-lingual	5-10%	2-5%

Biometric System Attacks

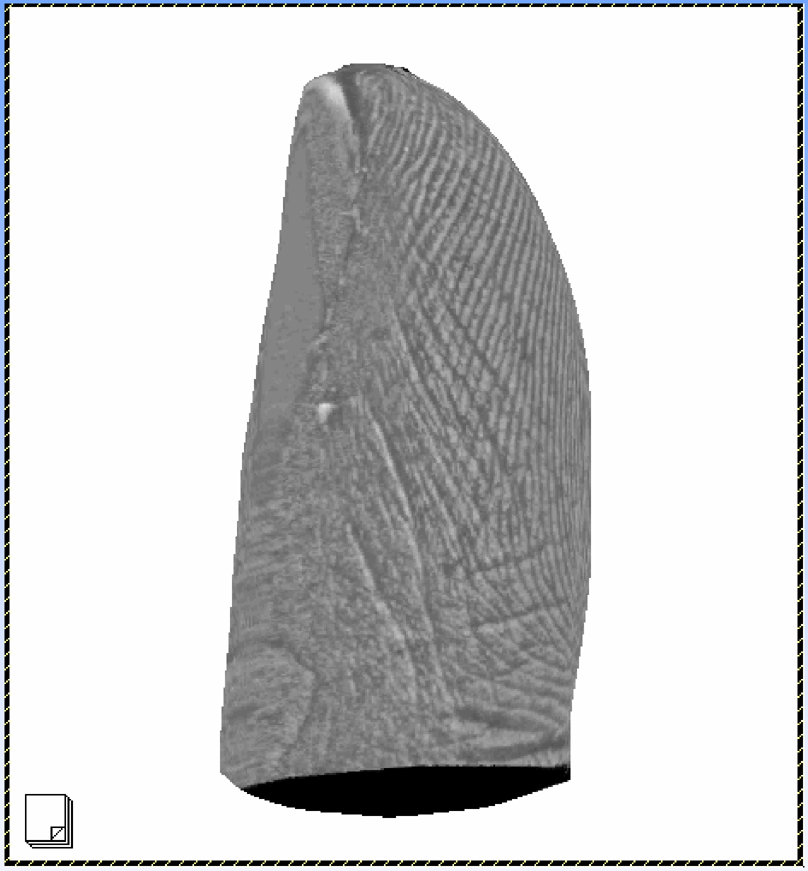


Fake Biometrics

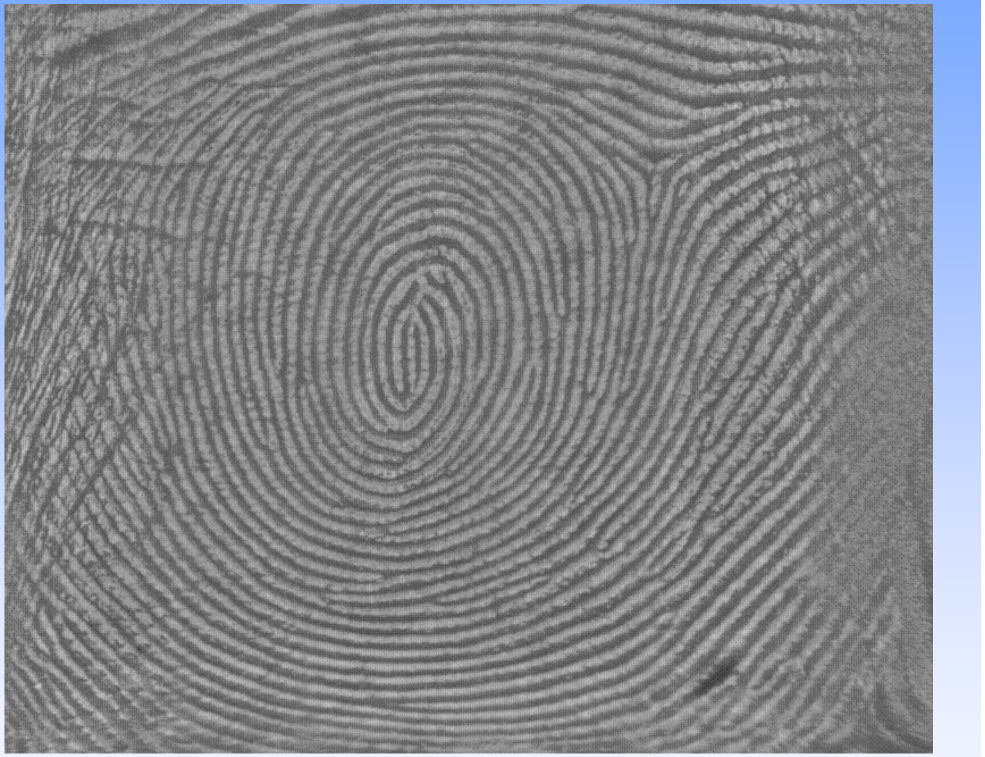
Research Directions

- Sensors
- Liveness detection
- Deformation Modeling
- Video Surveillance
- Image quality
- Individuality
- Multibiometrics
- Biometric cryptosystem

Touchless Fingerprint Sensor



Touchless 3D image

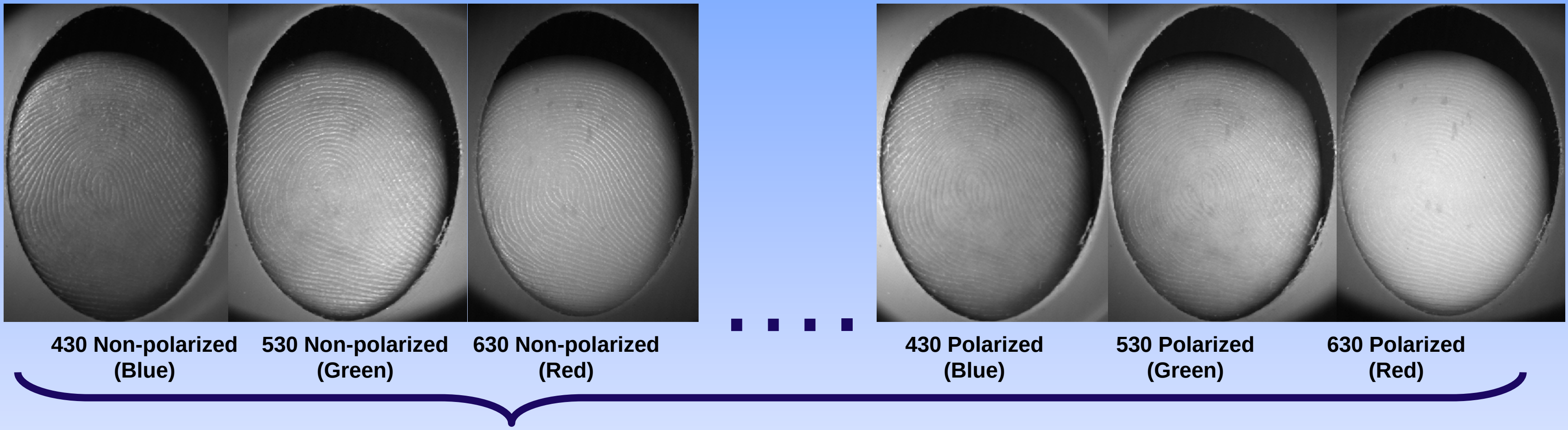


Touchless "rolled" image

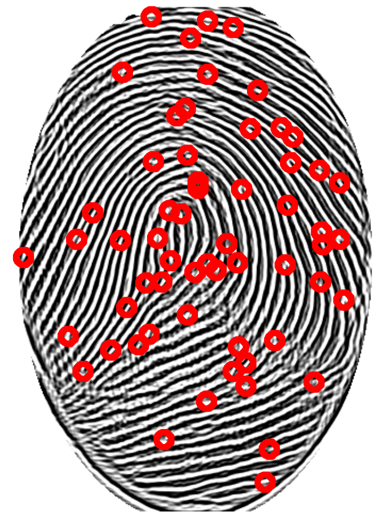
Courtesy: TBS North America, Inc.

Multispectral Fingerprint Imaging

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

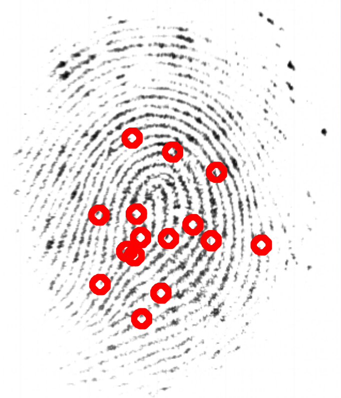


Jupiter 1.10 Combined Image - MSI



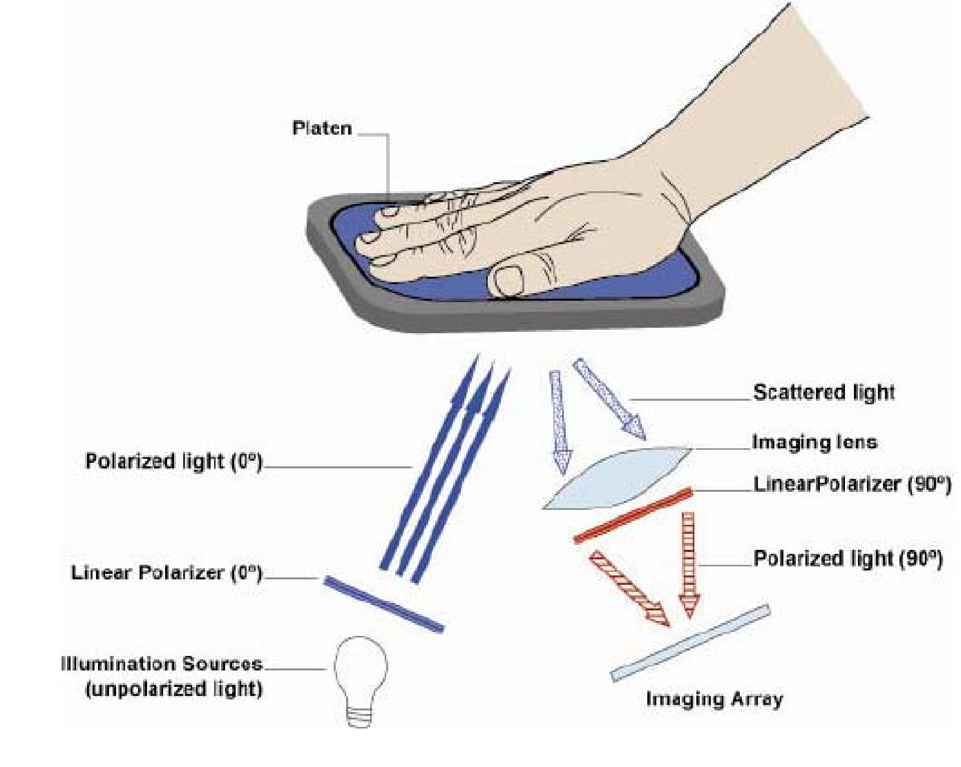
vs.

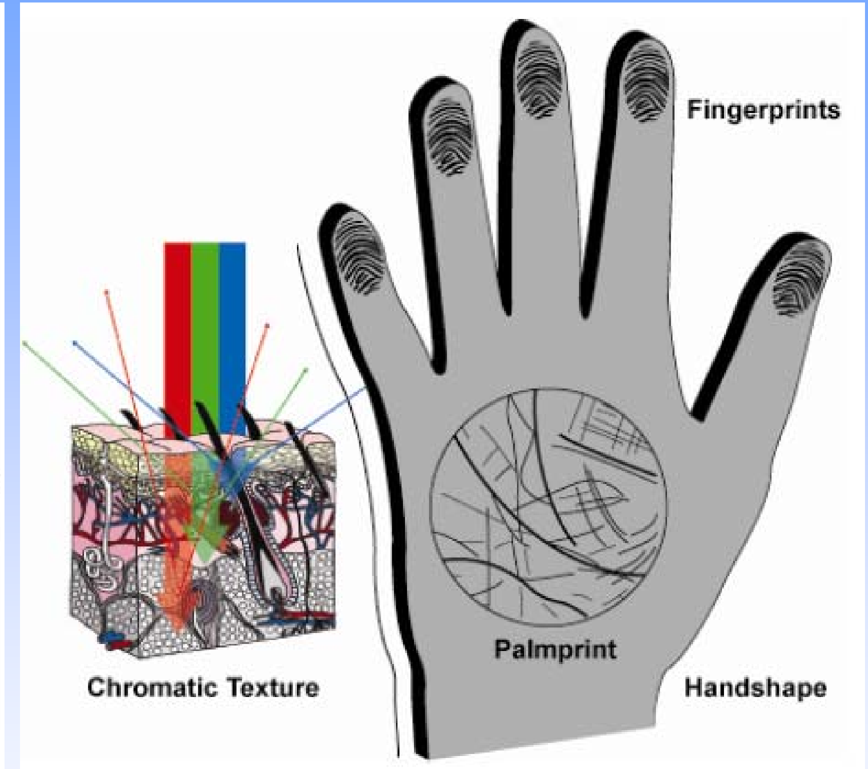
Cross Match Verifier Model 300 - TIR



Courtesy: Lumidigm

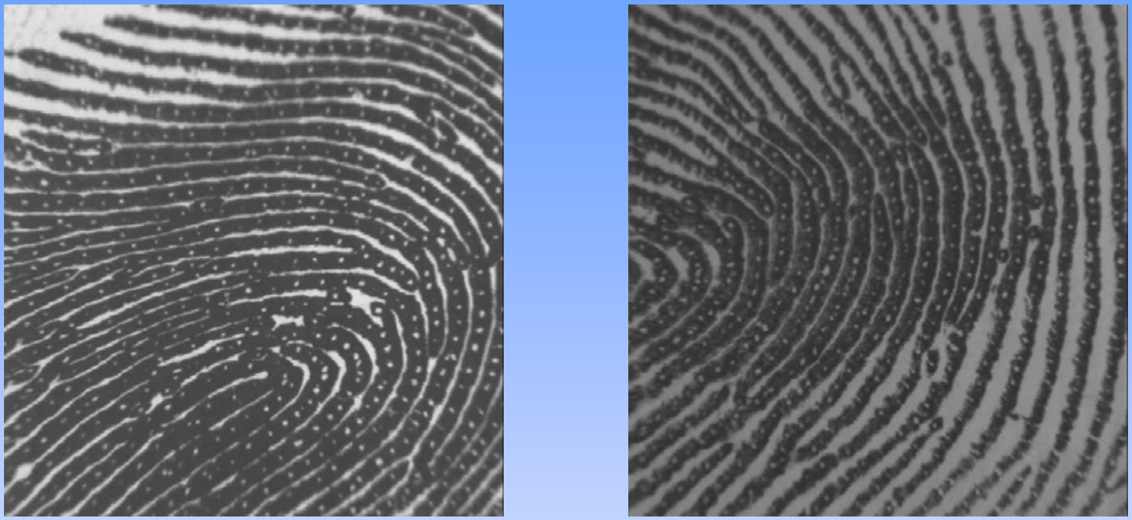
Multispectral Whole-Hand Imaging





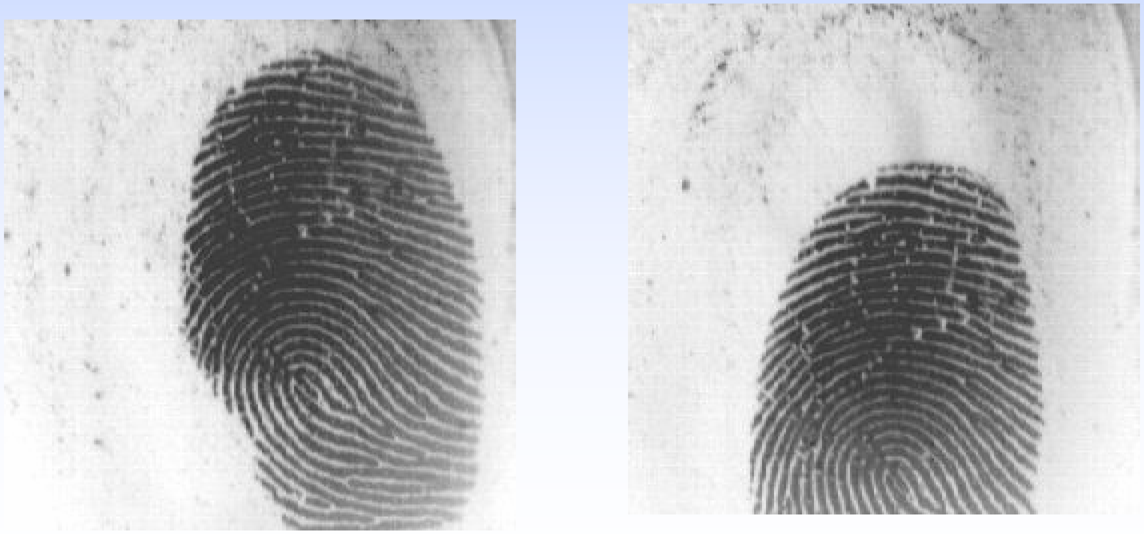
Deformation-Based Spoof Detection

Live finger

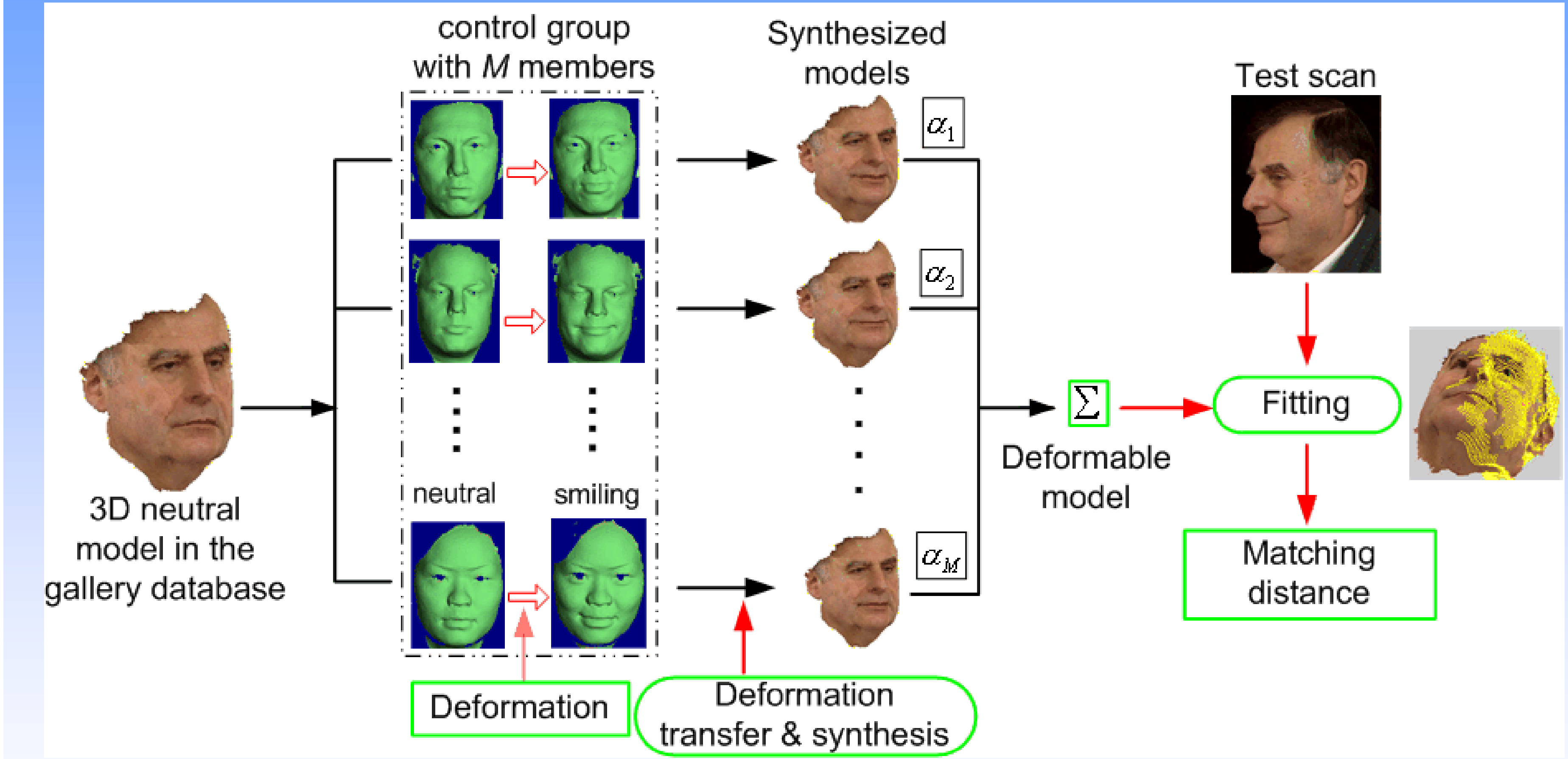


http://www.cim.mcgill.ca/~vleves/homepage/

Gummy finger

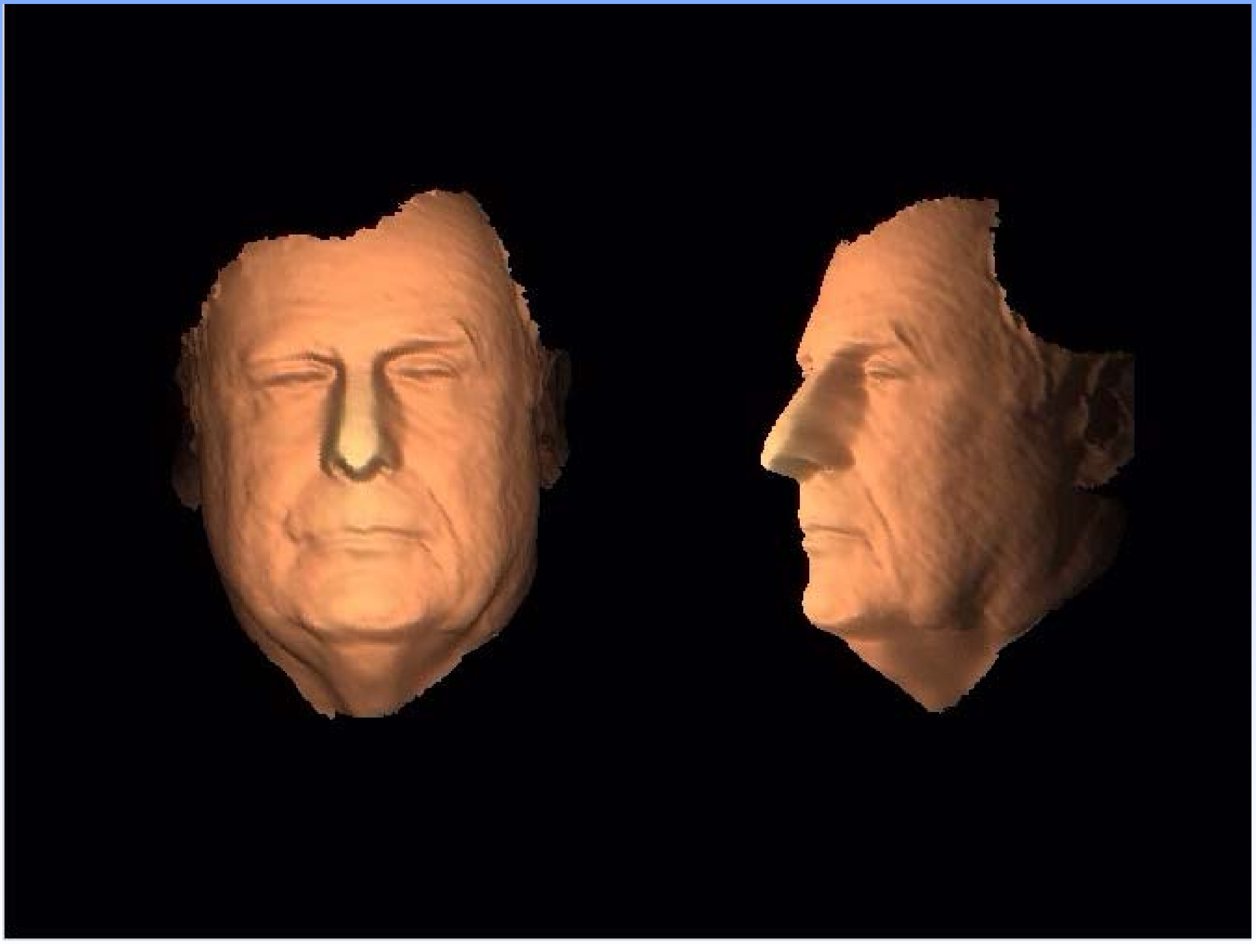


Deformation Modeling



Lu and Jain, "Deformation Modeling for Robust 3D Face Matching," Proc. CVPR, June 2006.

Deformable Model



Examples of the deformable model with varying weights (α_i)

Video Surveillance

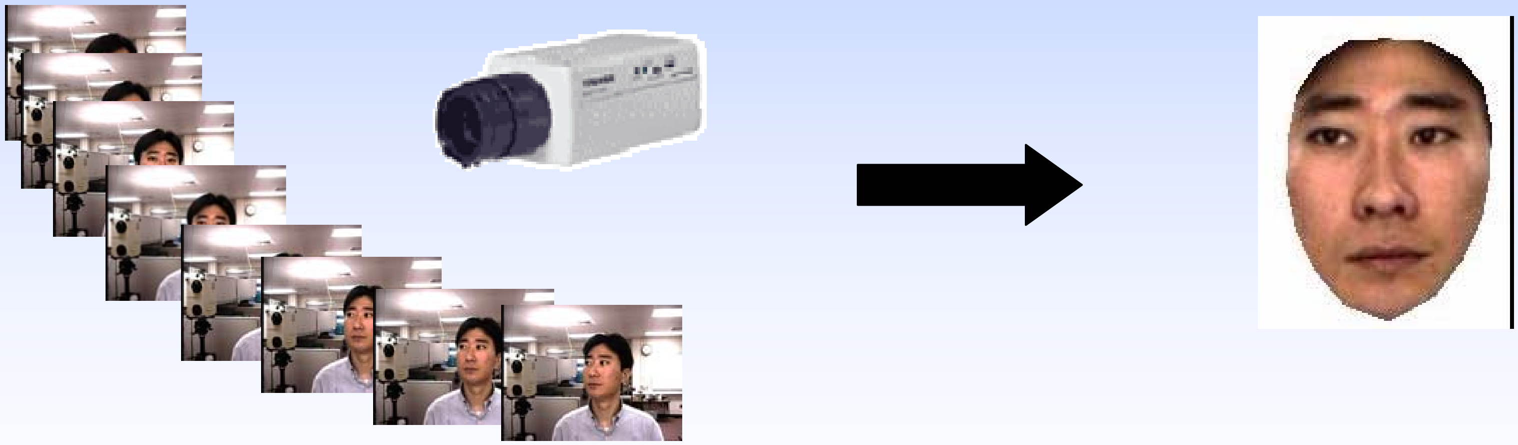
Face recognition in video

- Applications in covert surveillance system
- Video contains rich information (multiple frames) that can provide better face recognition performance

- Challenges
  - The same face in a video undergoes substantial variations in pose & illumination; frontal face recognition does not work
  - Raw videos frames in surveillance systems do not contain sufficient information for subject identification

Motivation

- 3D model reconstruction from video
  - Large pose & lighting variations can be compensated



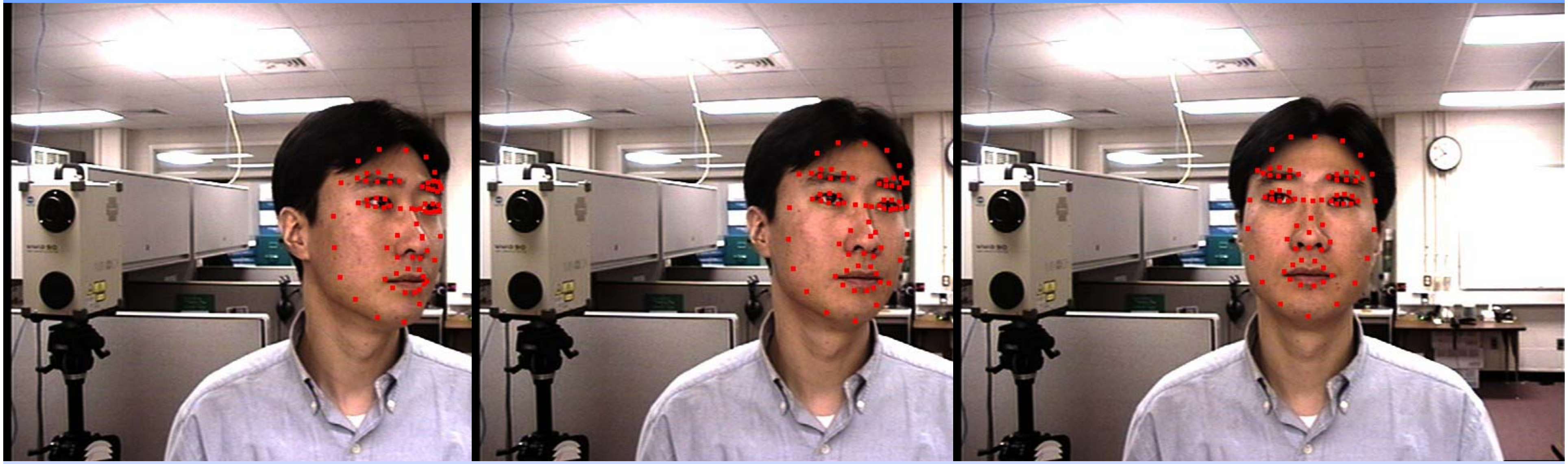
Automatic Facial Landmark Detection

- 72 landmarks using Active Appearance Model (AAM) on a Video with 60 frames

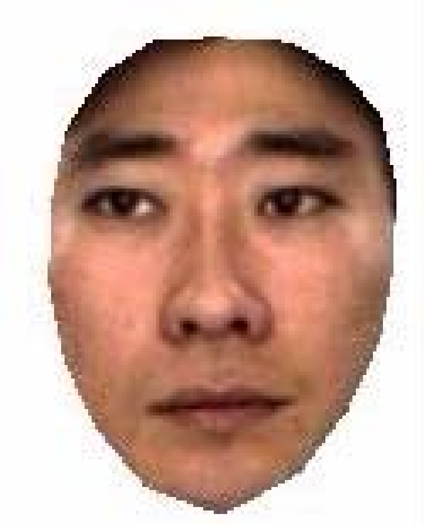
Landmark detection without temporal coherency

Landmark detection with temporal coherency (estimated feature points at current frame are used as the initial state for the next frame)

SfM with Real Data



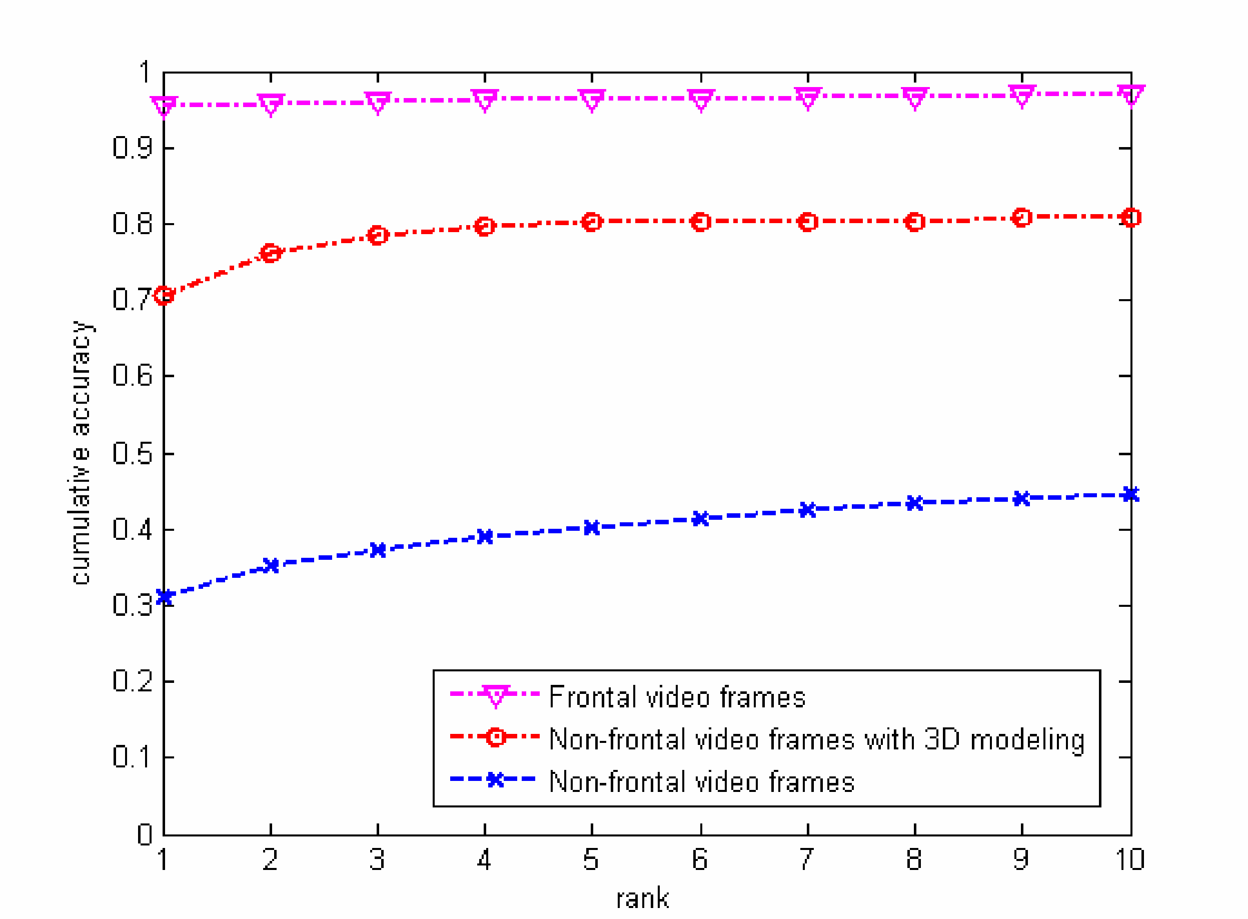
Example 2D images with feature points tracking



Reconstructed 3D model after texture mapping (from 60 images at about –45° to +45° yaw)

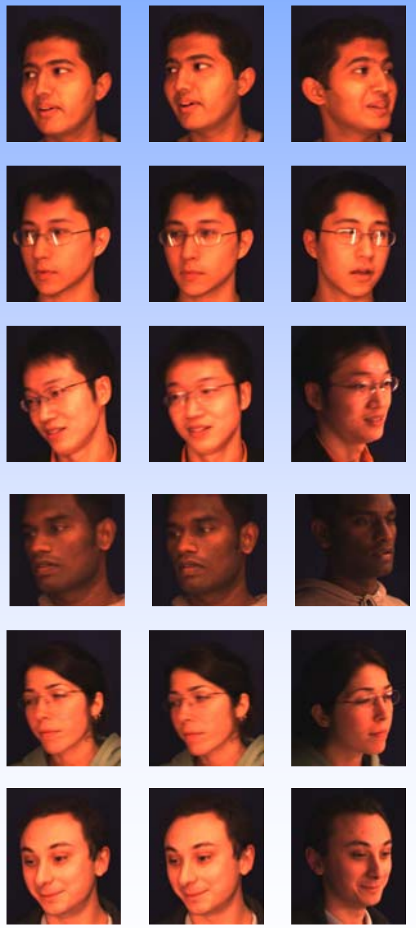
Face Recognition

- 207 Subjects from FIA database are used
- FaceVACS from Cognitec is used to obtain the matching scores

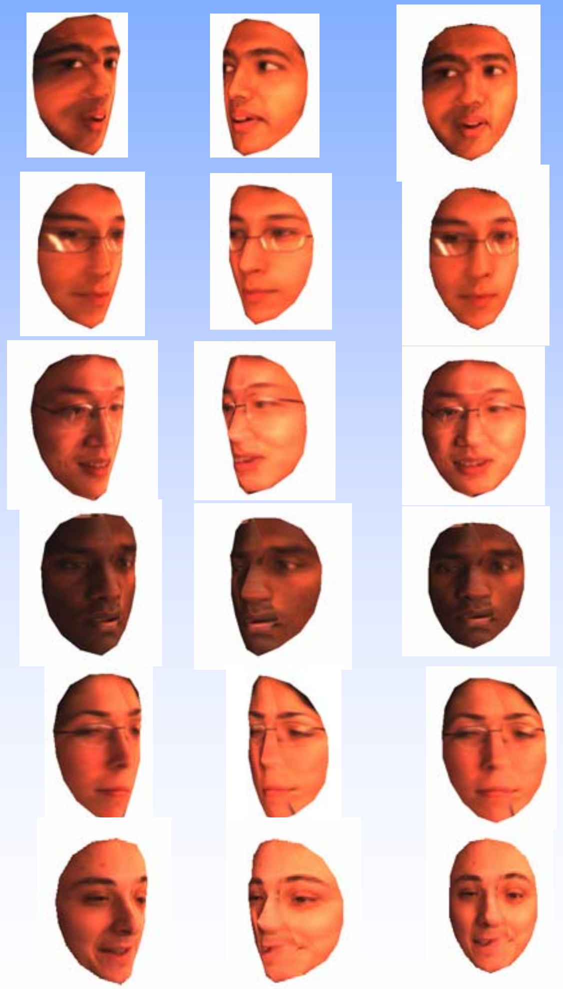


Matching Results

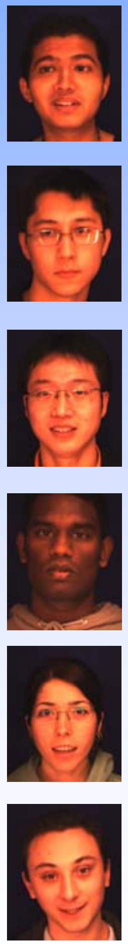
- Six subjects in video (a) are not correctly matched with corresponding image in gallery (c)
- Using 3D face models (b), video frames are correctly matched



(a)
Example frames in the original video
(Frontal views are not included)

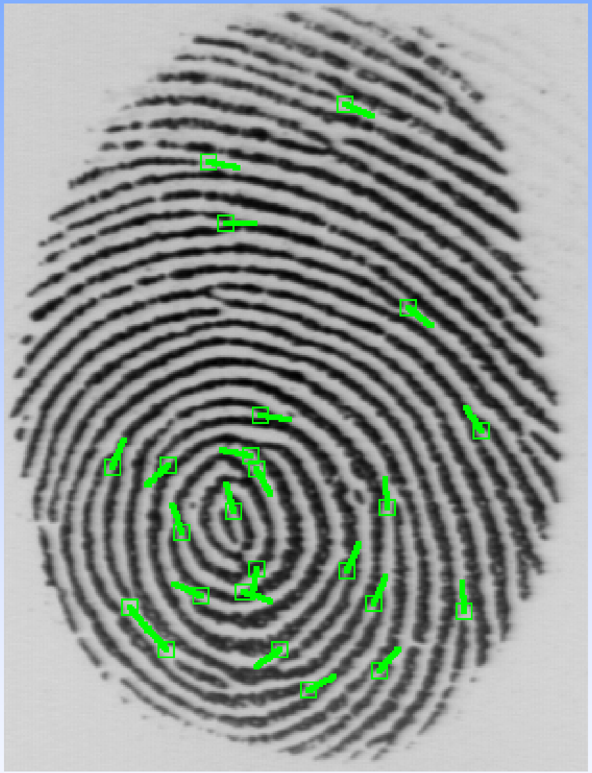


(b)
Reconstructed 3D face model

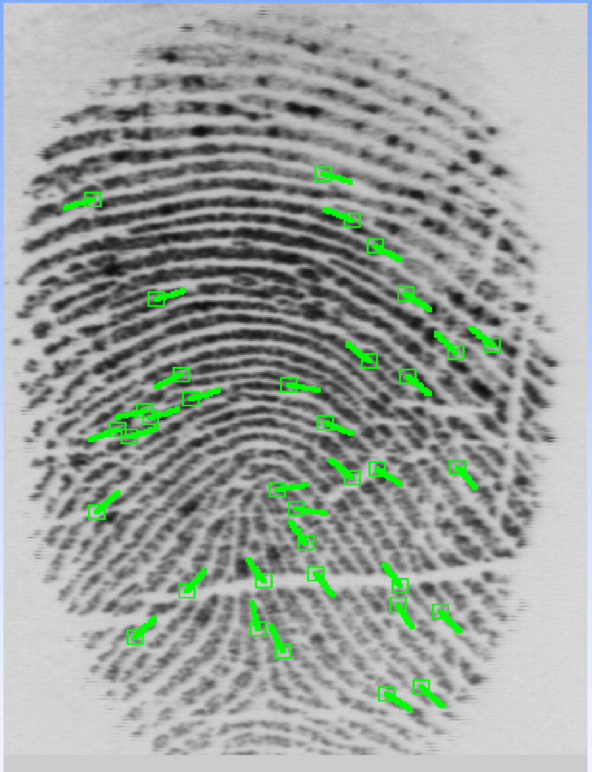


(c)
Example images in the
gallery database

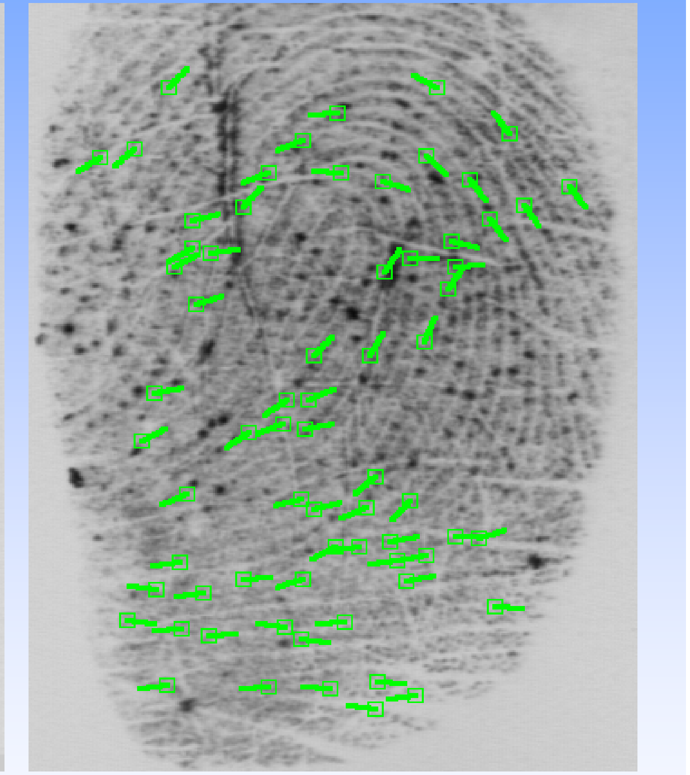
Noisy Images



Quality Index = 0.96
False Minutiae = 0



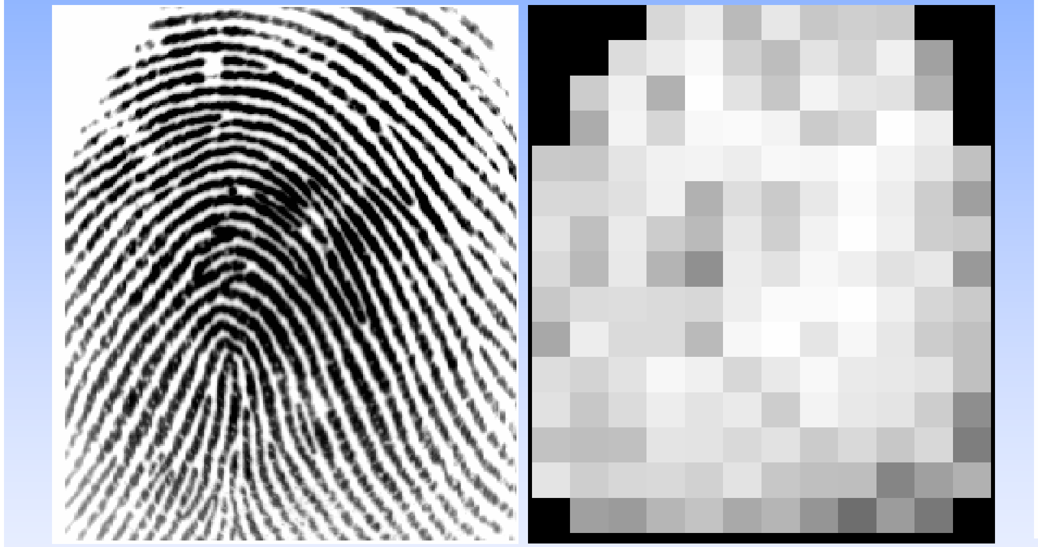
Quality Index = 0.53
False Minutiae = 7



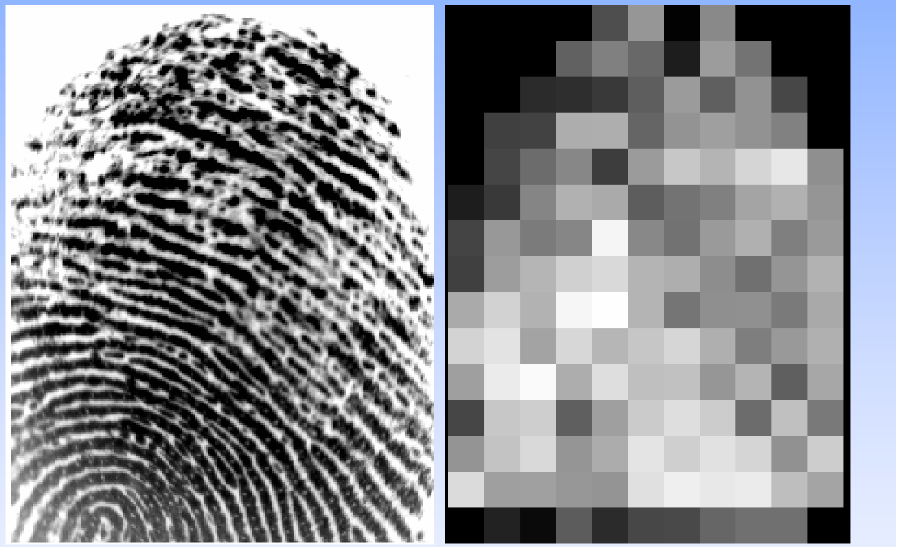
Quality Index = 0.04
False Minutiae = 27

Fingerprint Quality

- Partition the image into blocks and estimate local quality* (γ), $0 \leq \gamma \leq 1$



Quality map for a good image

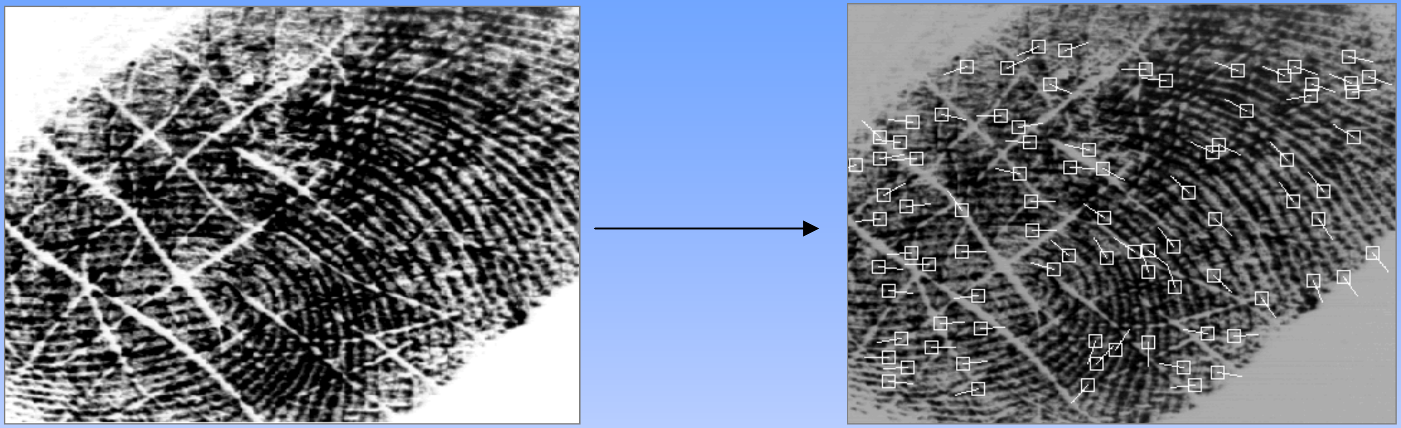


Quality map for a poor image

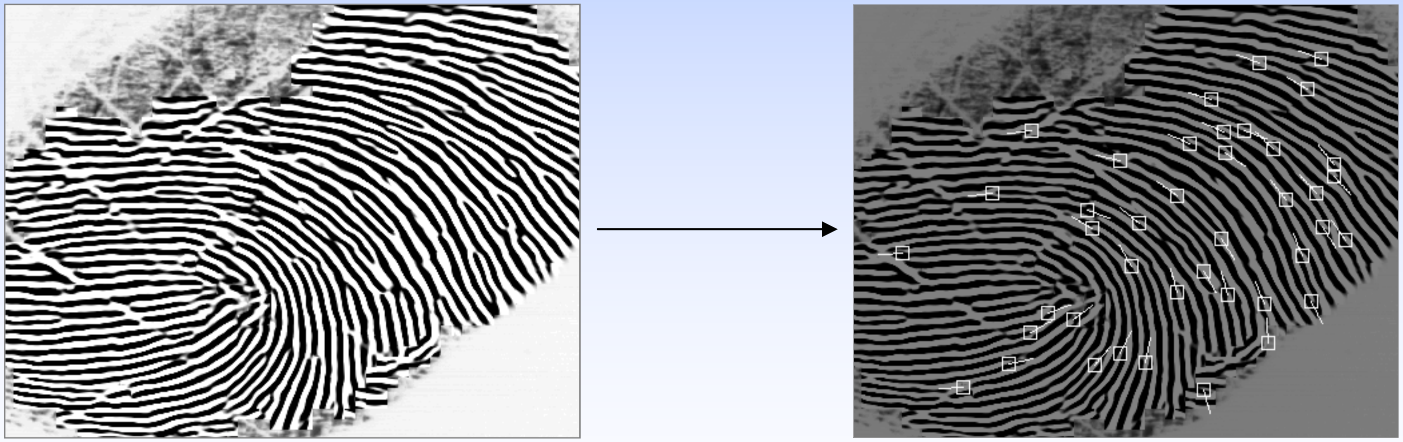
Note: Brighter pixels indicate better quality

[*] Y. Chen, S. Dass and A. Jain, "Fingerprint Quality Indices for Predicting Authentication Performance", *Proc. of AVBPA*, pp. 160-170, Rye Brook, NY, July 2005

Image Enhancement



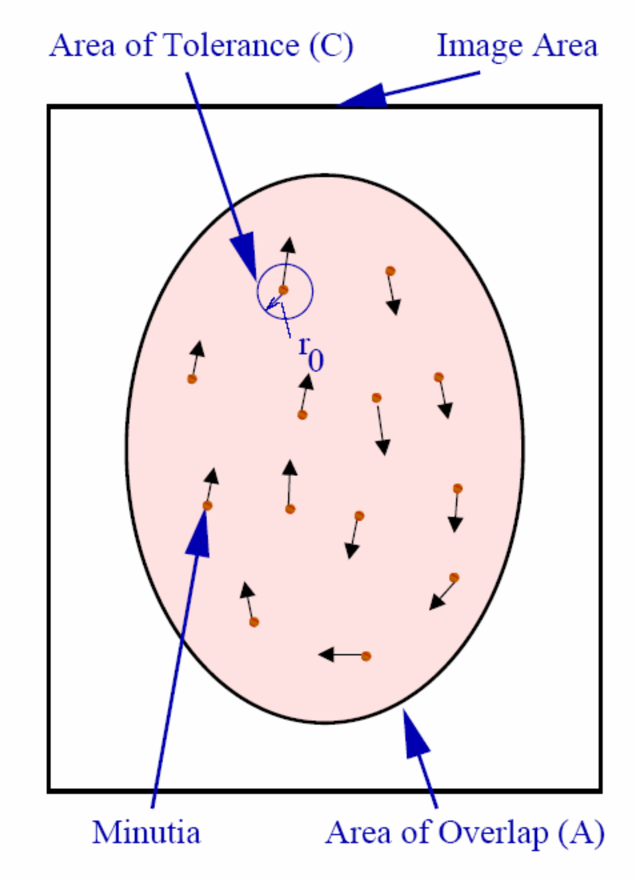
Minutiae extraction before enhancement



Minutiae extraction after enhancement

Are Fingerprints Unique?

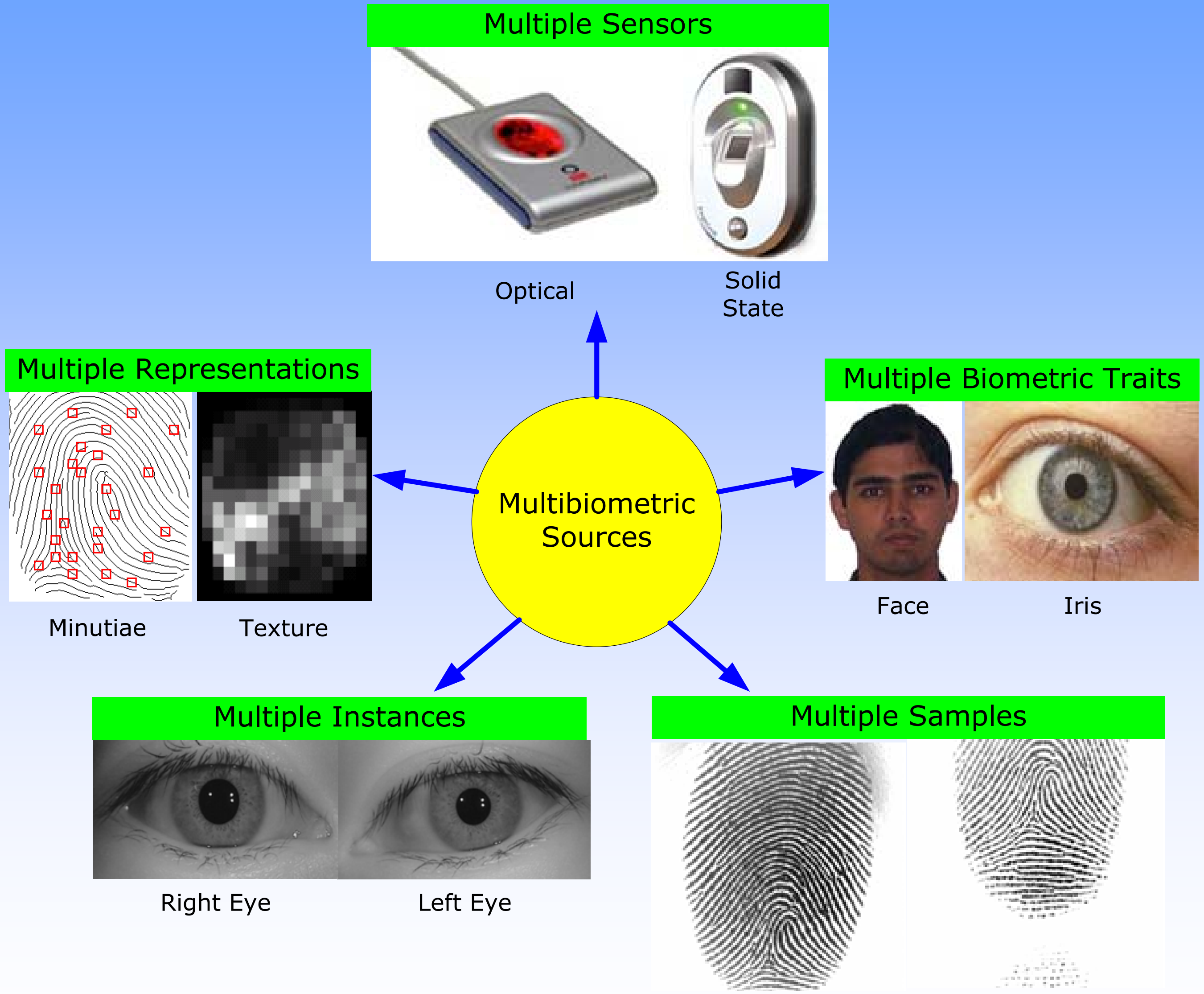
- "Two Like Fingerprints Would be Found Only Once Every 10^{48} Years" *Scientific American, 1911*
- Given two fingerprints with m & *n* minutiae, what is the probability they will share *q* minutiae?



1. m=n=52, q=12
   PRC = 4.4 x 10^{-3}
   (Observed value = 3.5 x 10^{-3})
2. m=n=52, q=26
   PRC = 3.4 x 10^{-14}

M = A/C=413 (NIST-4 database)

Multibiometrics



Multiple Sensors

Optical

Solid State

Multiple Representations

Minutiae

Texture

Multibiometric Sources

Multiple Biometric Traits

Face

Iris

Multiple Instances

Right Eye

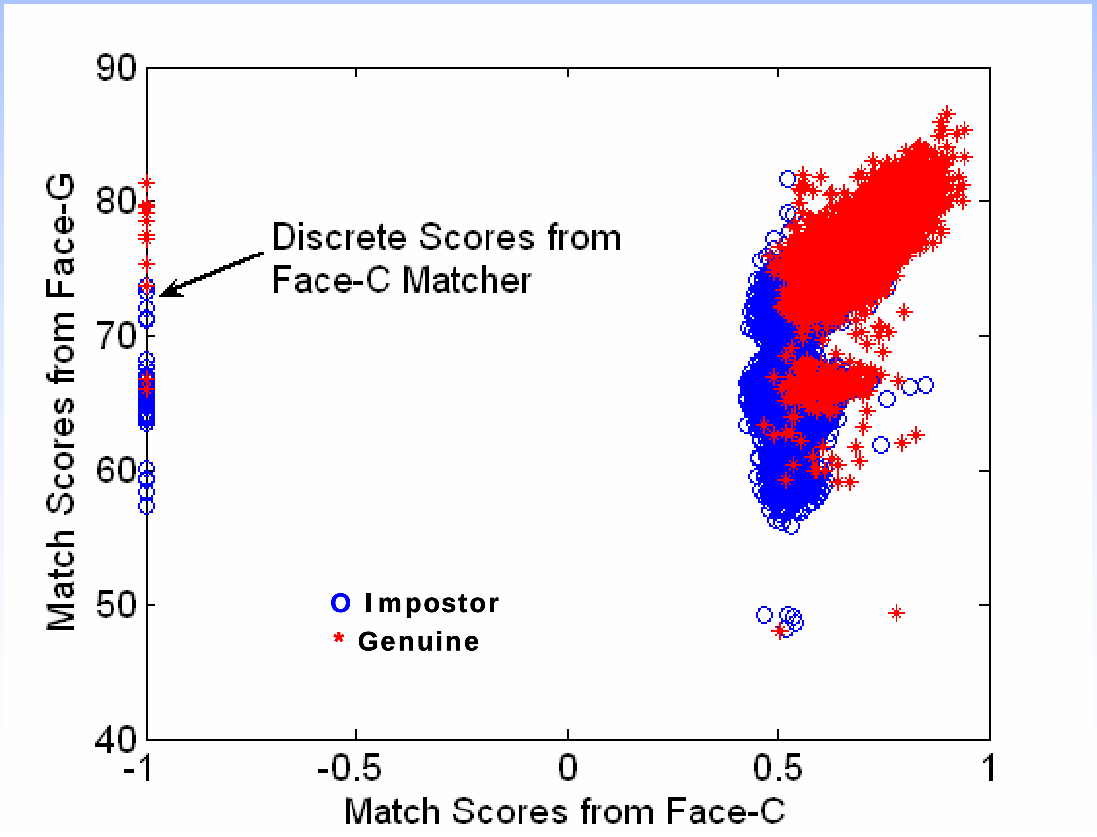
Left Eye

Multiple Samples

A. Ross, K. Nandakumar and A. K. Jain, Handbook of Multibiometrics, Springer, 2006

Match Score Fusion

- Score ranges are different; C: [-1,1], G: [0,100]
- Statistical distributions are different. In addition, they have continuous and discrete components
- Scores from the matchers are correlated



Match scores from the two face matchers in NIST-BSSR1 database

Likelihood Ratio Based Fusion

- Let $\boldsymbol{S} = (S_1, S_2, \ldots, S_K)$ be the match scores for K modalities. Likelihood ratio test to minimize FRR for a given FAR (NP rule)
  - Decide "genuine" if

$$FS(\mathbf{S}) = \frac{P(\mathbf{S} \mid genuine)}{P(\mathbf{S} \mid impostor)} \geq \eta$$

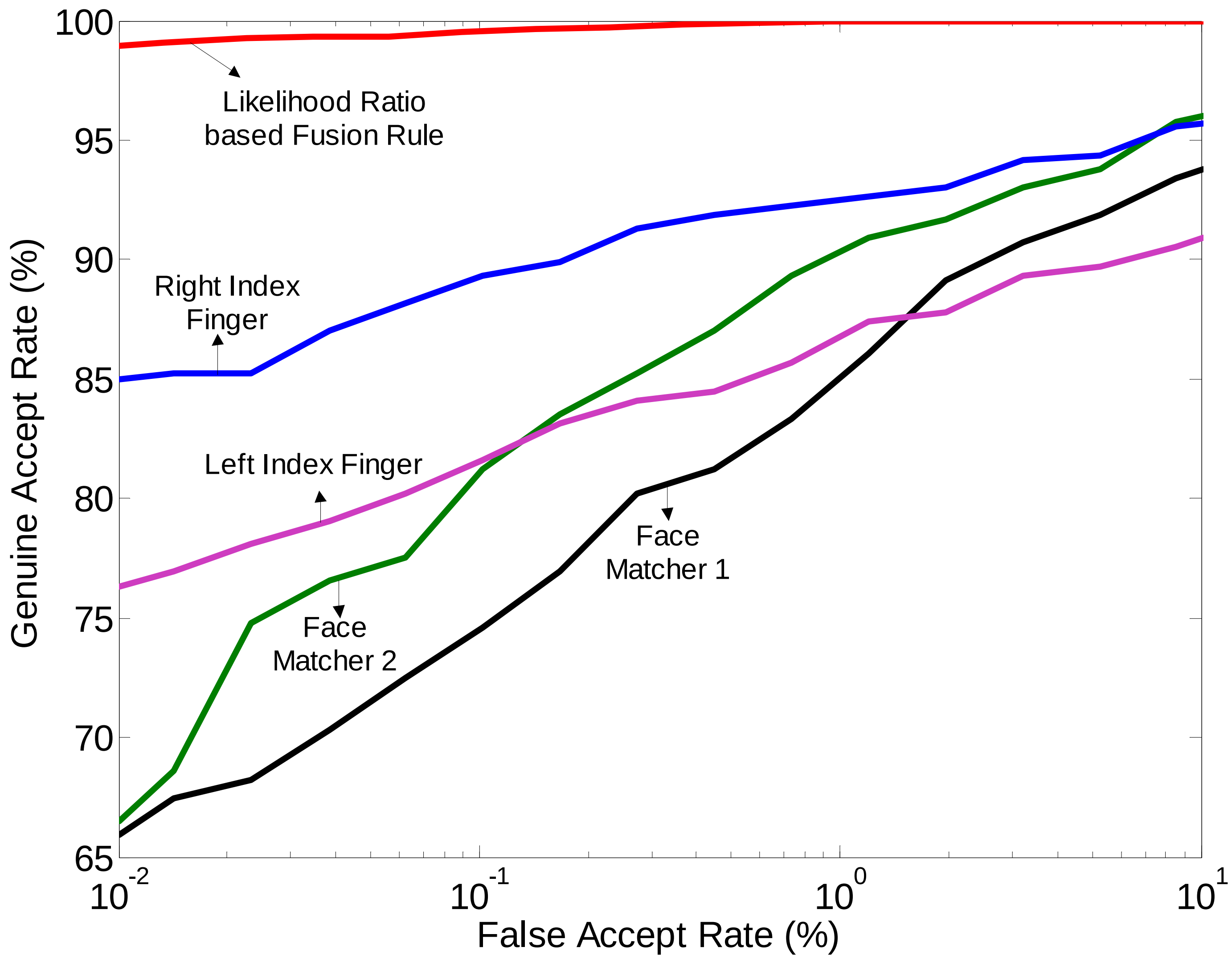
where η is determined by the given FAR

- For independent matchers, LR test reduces to product rule

$$PFS(\mathbf{S}) = \prod_{k=1}^{K} \frac{P(S_k \mid genuine)}{P(S_k \mid impostor)} \geq \eta$$

S. Dass, K. Nandakumar and A. Jain, "A Principled Approach to Score Level Fusion in Multimodal Biometric Systems", *Proc. of AVBPA,* pp. 1049-1058, Rye Brook, NY, July 2005

Fusing Multiple Modalities



Quality-based Fusion

- Estimate joint density of match score and image quality to assign weights to individual matchers
- Let **Q** = (Q_1, Q_2, …, Q_K) be the quality vector associated with the K-dimensional match vector
- Quality-based fusion (QF) rule decides "genuine" if

$$QFS(\mathbf{S},\mathbf{Q}) = \frac{P(\mathbf{S},\mathbf{Q} \mid genuine)}{P(\mathbf{S},\mathbf{Q} \mid impostor)} \geq \eta$$

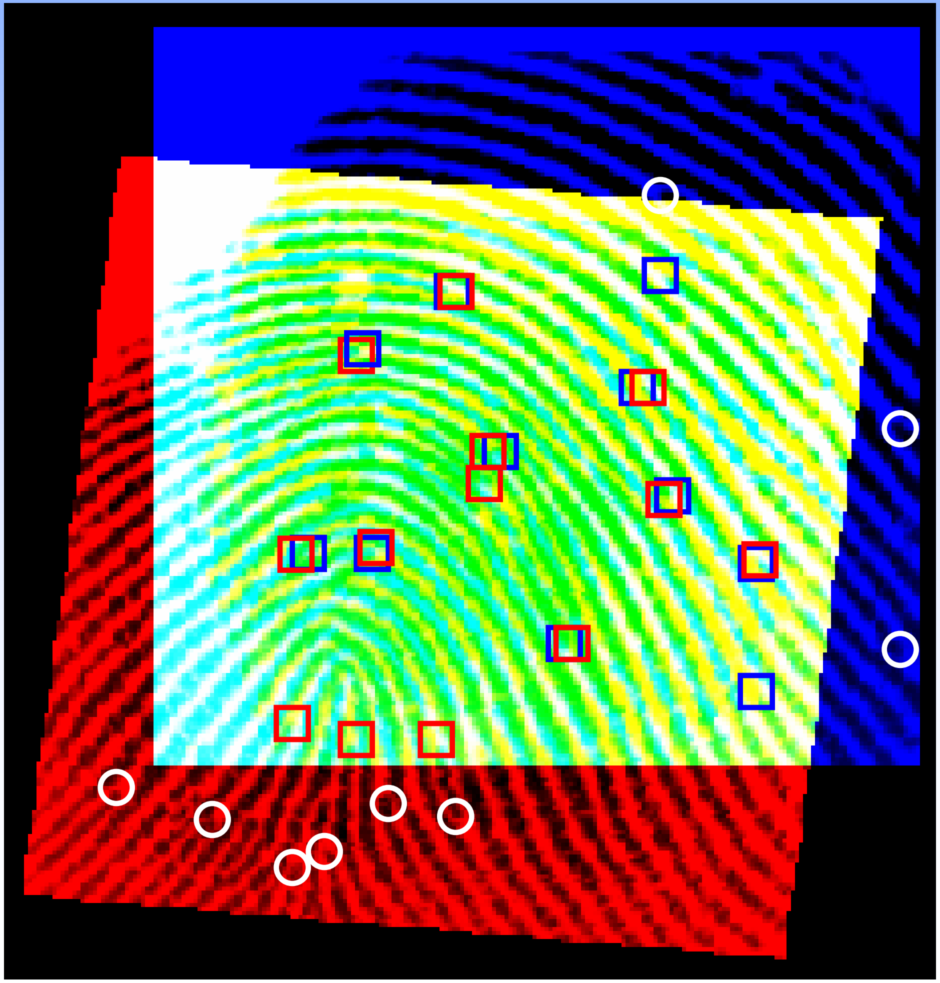
- If K matchers are independent, the QF rule is simplified as

$$QPFS(\mathbf{S},\mathbf{Q}) = \prod_{k=1}^{K} \frac{P(S_k, Q_k \mid genuine)}{P(S_k, Q_k \mid impostor)} \geq \eta$$

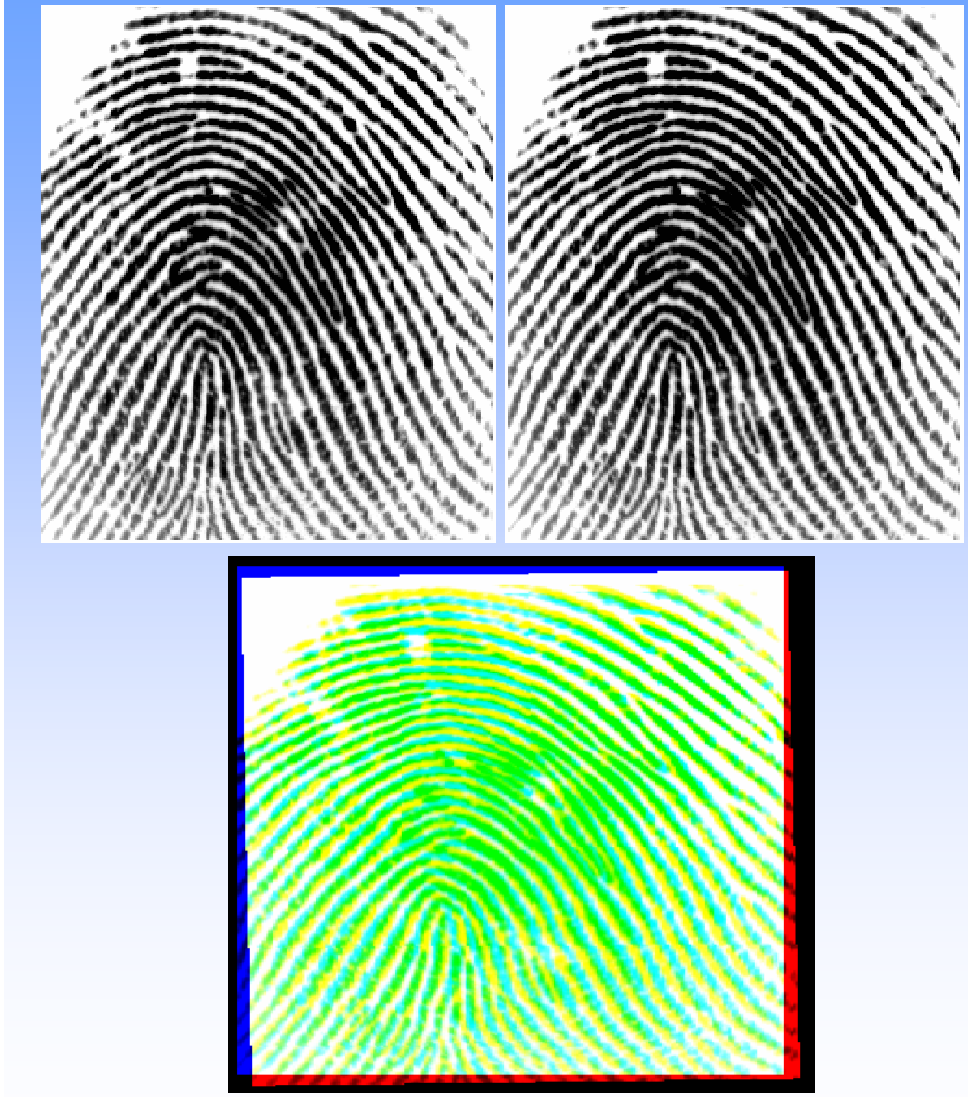
This decision rule is known as quality-based product fusion

Pair-wise Fingerprint Quality

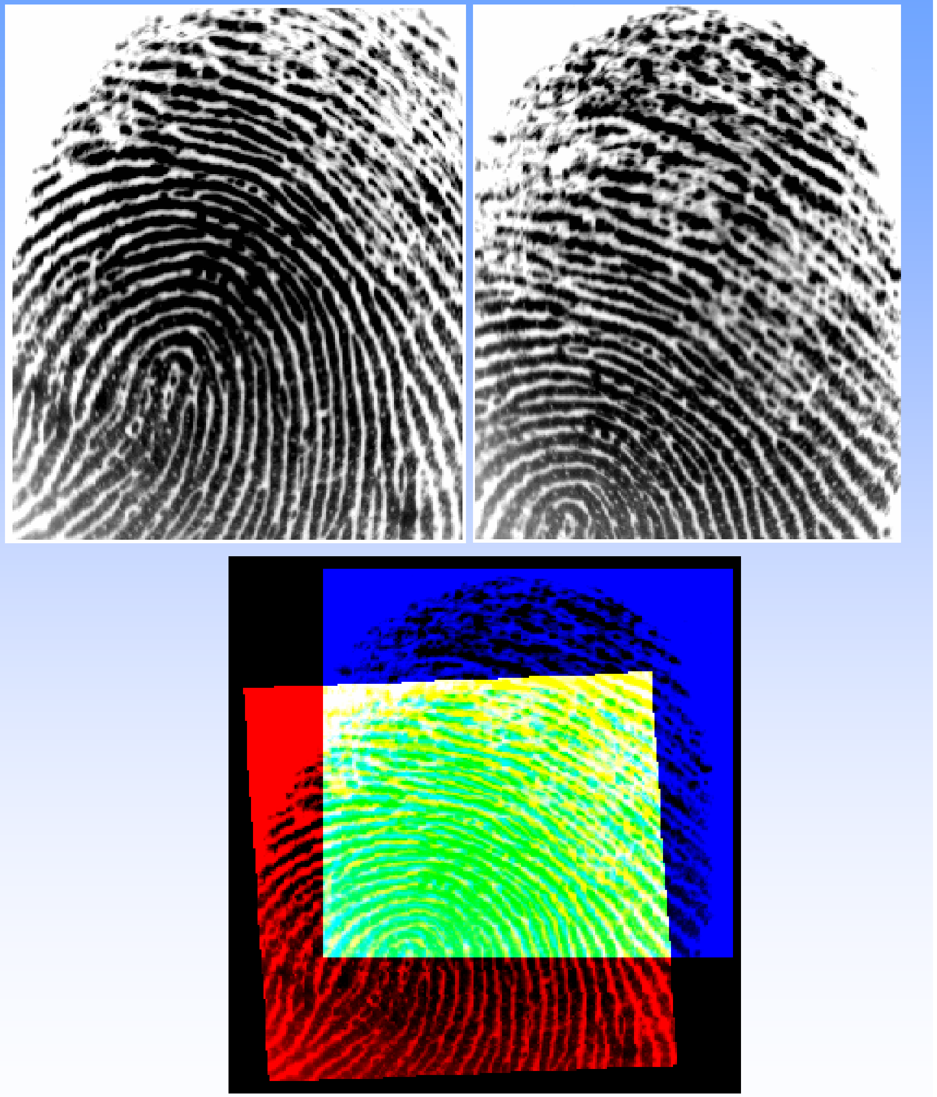
Pair-wise (template & query) is function of minutiae quality in the overlapping region and area of overlap



Fingerprint Quality Examples



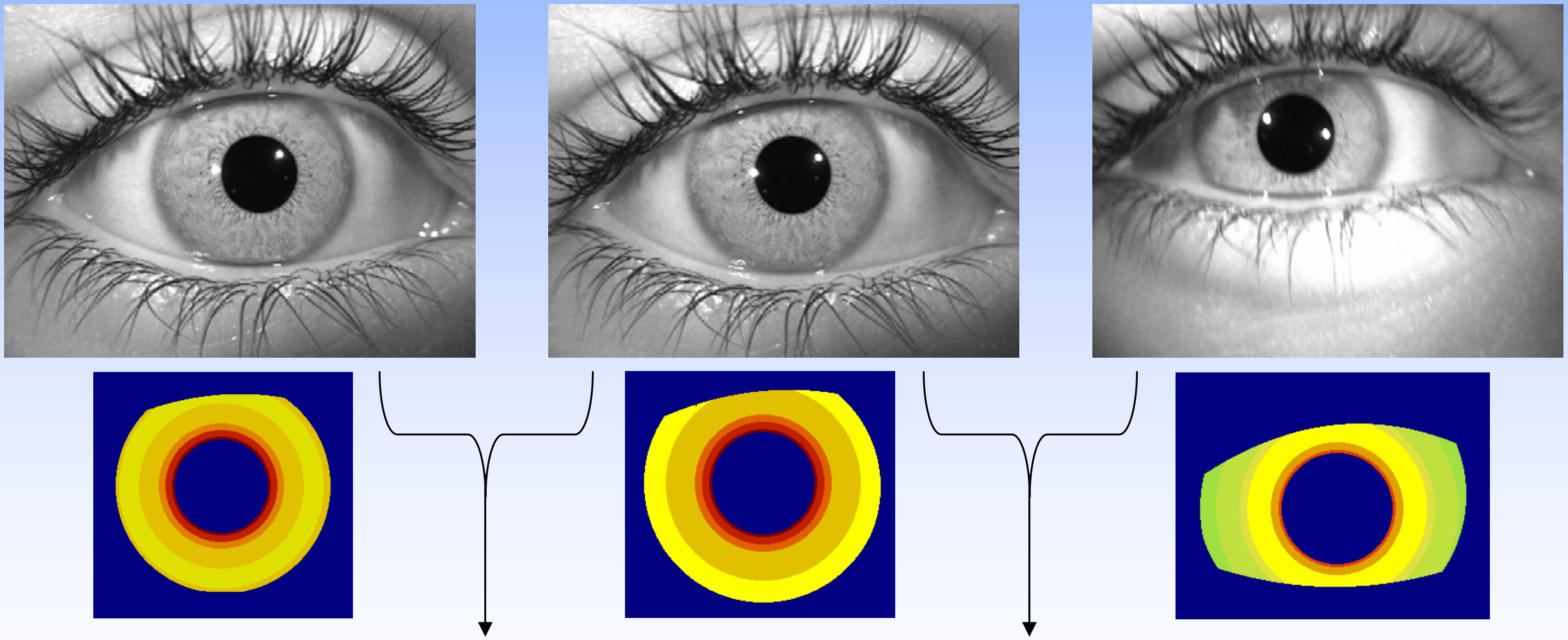
Good quality pair ($Q_{\text{finger}}=0.90$)



Poor quality pair ($Q_{\text{finger}}=0.28$)

Pair-wise Iris Quality

- Iris local quality* is defined using 2-D wavelet transform in local windows
- Correlation of local quality vectors of template and query is defined as the quality of the pair

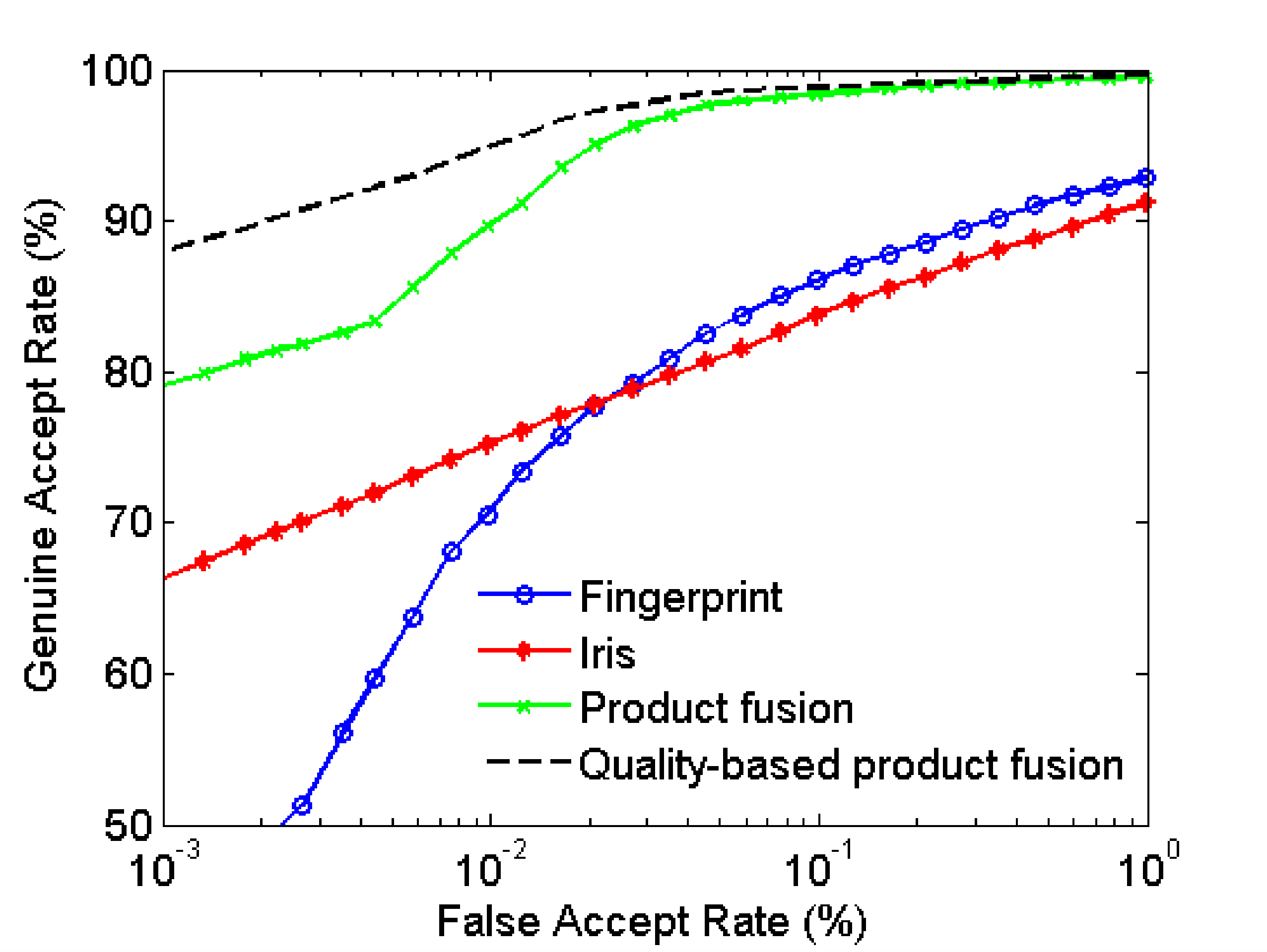


Good quality pair (Q_{iris}=0.80) Poor quality pair (Q_{iris}=0.42)

* Y. Chen, S. Dass and A. Jain, "Localized Iris Image Quality Using 2-D Wavelets", Proc. of ICB, pp. 373-381, Hong Kong, Jan. 2006

Fusion of Fingerprint and Iris

- WVU joint multimodal database; 320 subjects, 5 samples/modality/subject; 20-fold cross-validation



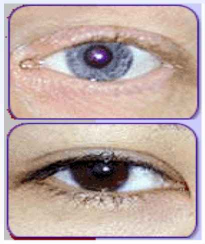
Soft Biometrics

Soft biometrics provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate them

Ethnicity, Skin Color, Hair color

(Sub-Saharan African, Indian, Southern European, and Northwest European)

http://anthro.palomar.edu/adapt/adapt_4.htm
© Corel Corporation, Ottawa, Canada



Eye color

http://ology.amnh.org/genetics/longdefinition/index3.html
© American Museum of Natural History, 2001

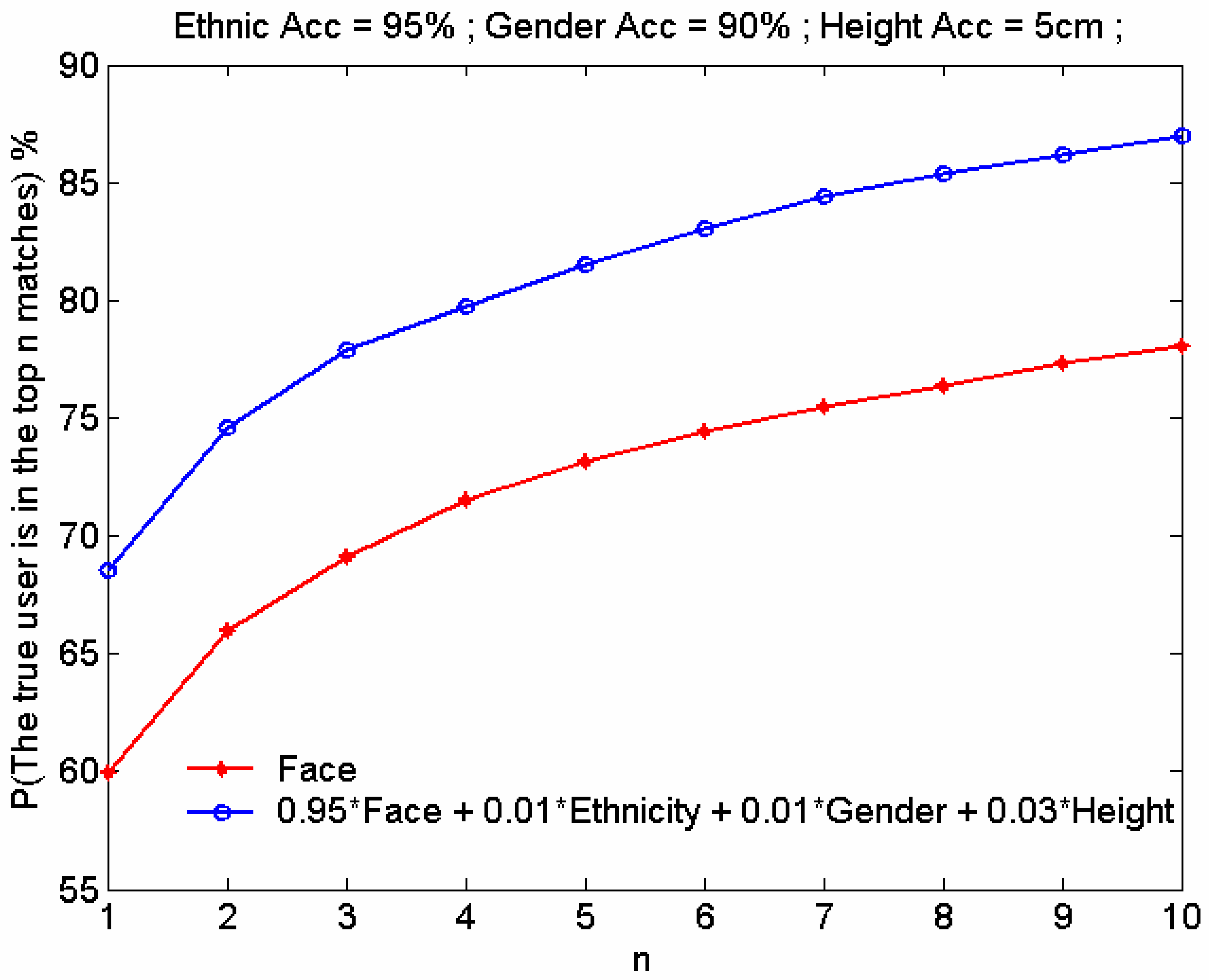
Height

http://www.altonweb.com/history/wadlow/p2.html
© Alton Museum of History and Art

Weight

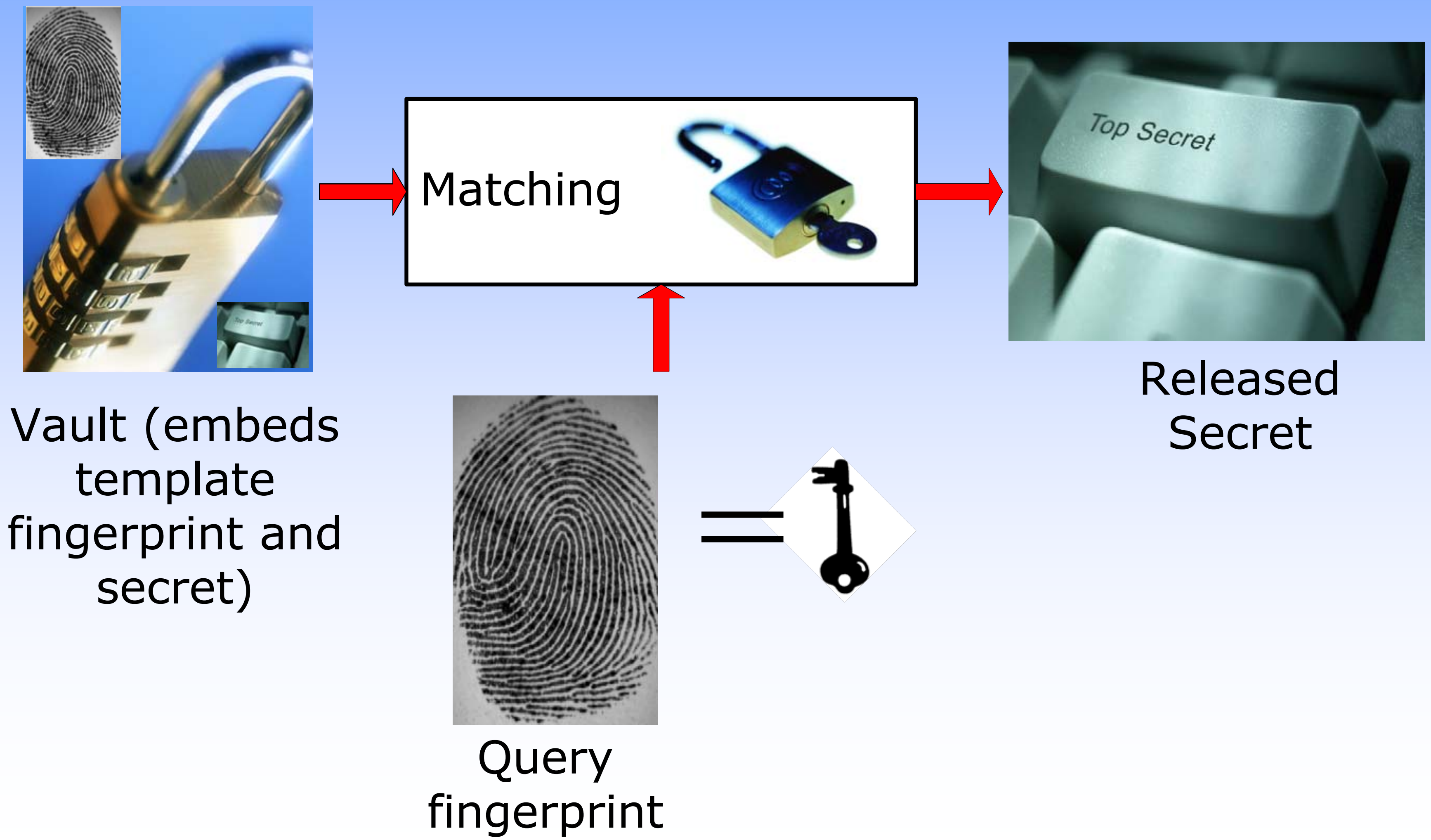
http://www.laurel-and-hardy.com/goodies/home6.html © CCA

Combining Face & Soft Biometrics



Biometric Cryptosystem

Secure an encryption key with fingerprint so only the authorized user can access the secret



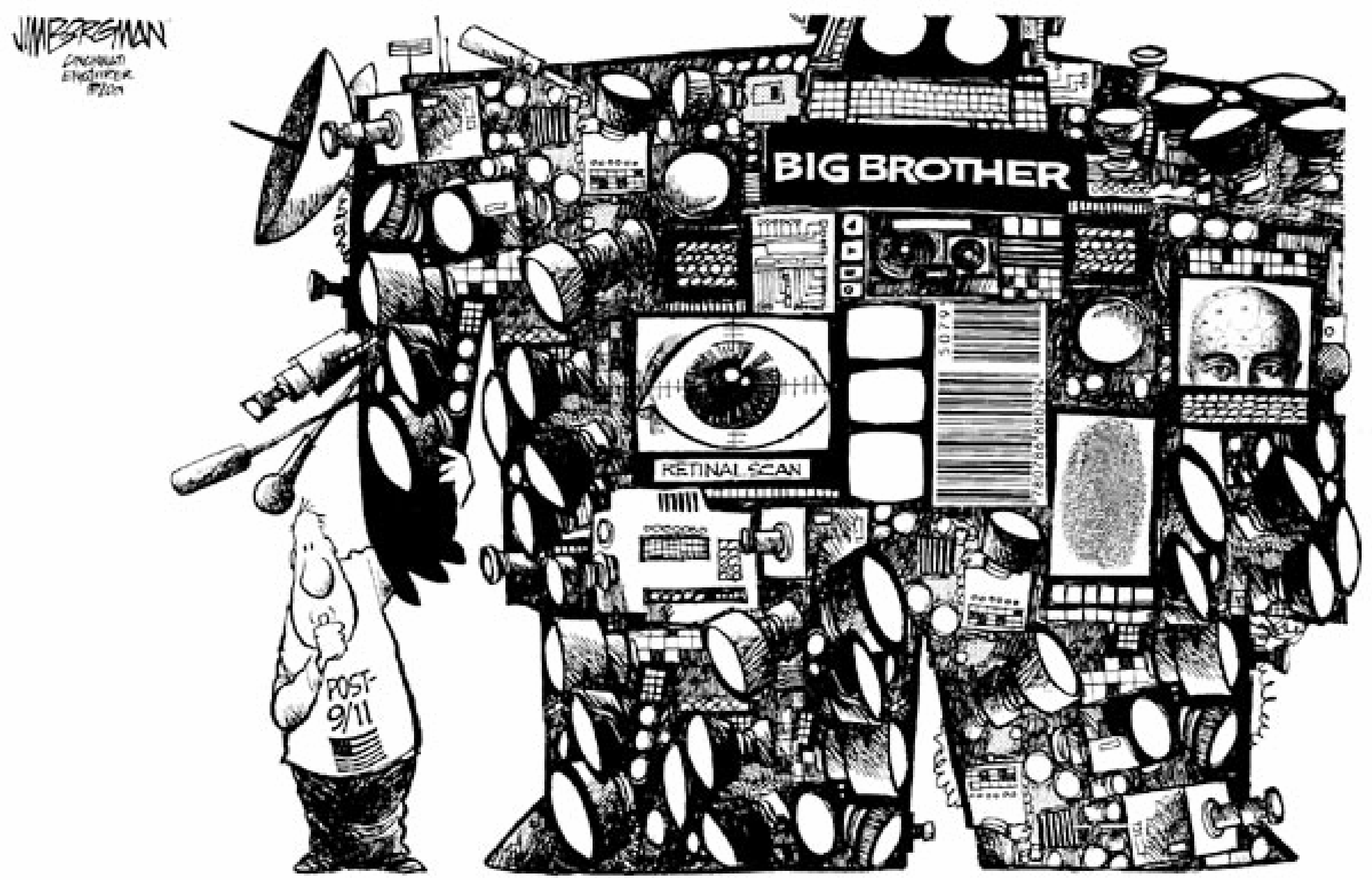
Vault (embeds template fingerprint and secret)

Matching

Released Secret

Query fingerprint

Big Brother


JIMBORGMAN
CINCINNATI ENQUIRER
BIG BROTHER
RETINAL SCAN
POST-9/11

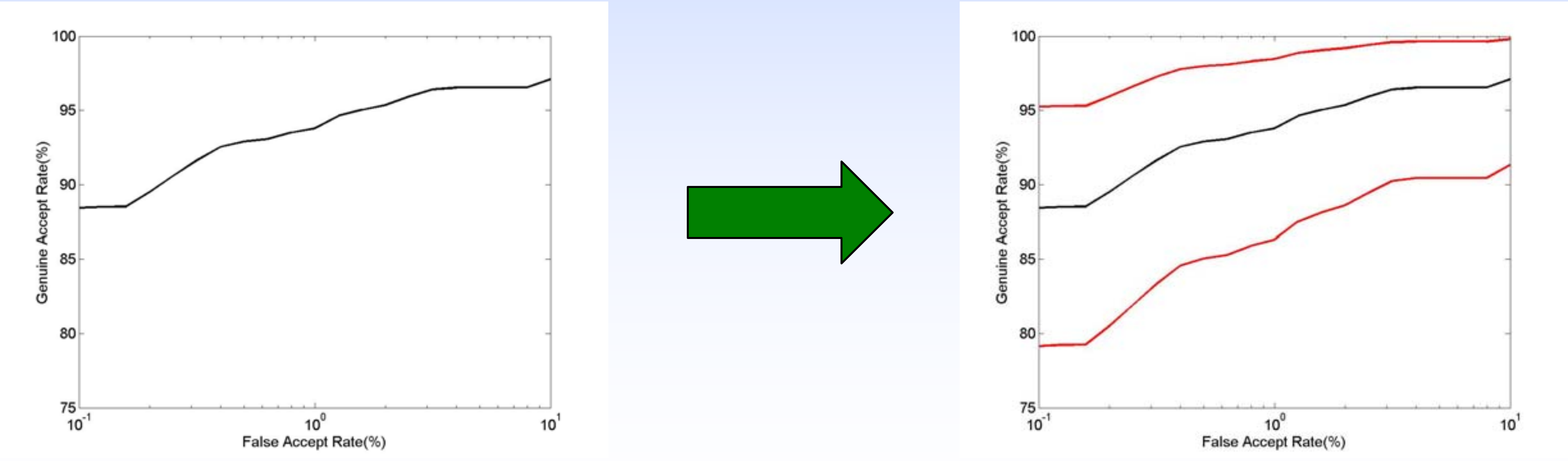
Sample Size Requirements

Motivation: To validate the claimed performance of a biometric authentication system given by ROC_0, say.

Biometric data: Collect biometric data from N users with K acquisitions per user. The challenge is that the K acquisitions per user are correlated. Validation techniques need to take into account this correlation.

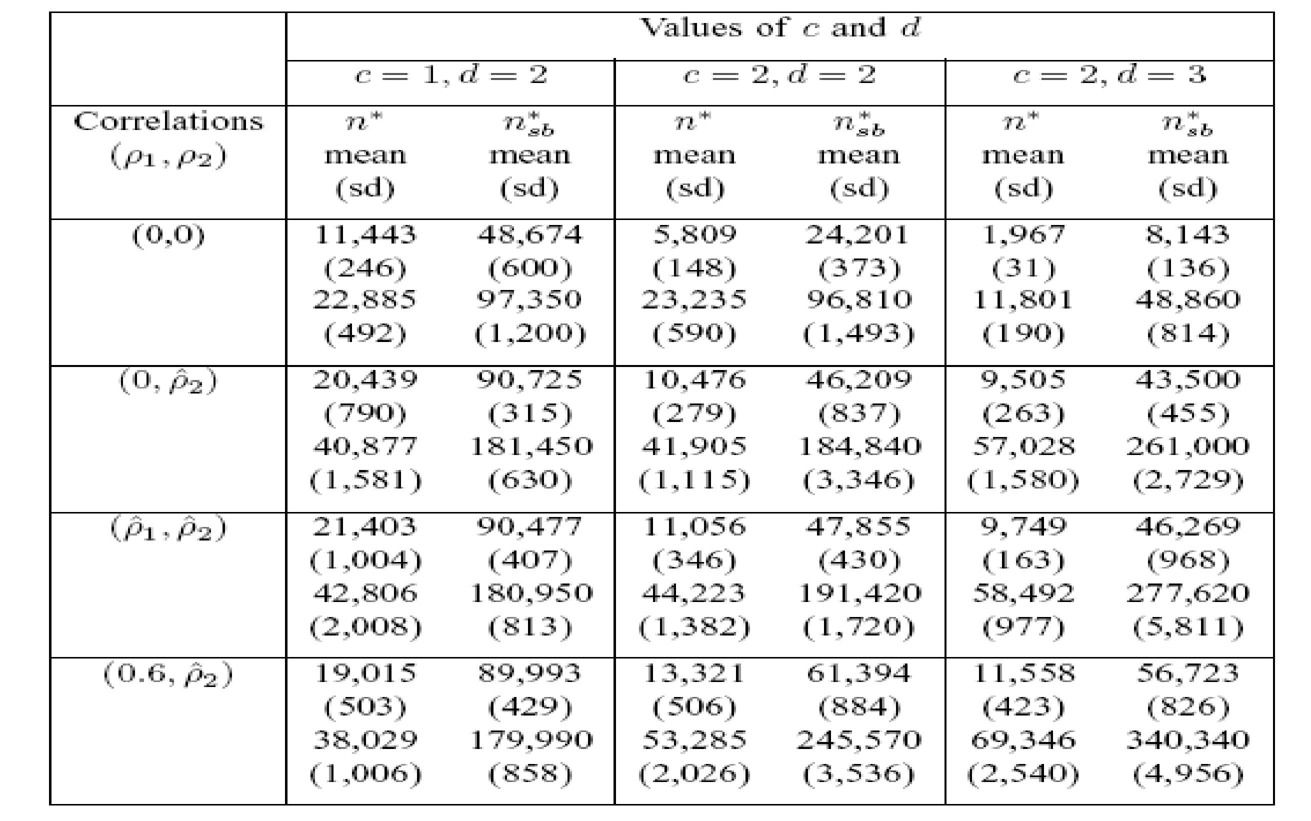
Validation Tool: Construct 100(1-α)% confidence bands for ROC_0. Accept ROC_0 if

$$LB(p) \leq ROC_0(p) \leq UB(p) \text{ for all } p \text{ in } [C_0,C_1];$$



Sample Size Requirements

Sample size needed to obtain a confidence interval at 95% level and 1% width (*c* = no. of fingers; d = no. of impressions/finger



	Values of c and d					
	$c = 1, d = 2$		$c = 2, d = 2$		$c = 2, d = 3$	
Correlations (ρ_1, ρ_2)	n^* mean (sd)	n^*_{sb} mean (sd)	n^* mean (sd)	n^*_{sb} mean (sd)	n^* mean (sd)	n^*_{sb} mean (sd)
(0,0)	11,443	48,674	5,809	24,201	1,967	8,143
	(246)	(600)	(148)	(373)	(31)	(136)
	22,885	97,350	23,235	96,810	11,801	48,860
	(492)	(1,200)	(590)	(1,493)	(190)	(814)
$(0, \hat{\rho}_2)$	20,439	90,725	10,476	46,209	9,505	43,500
	(790)	(315)	(279)	(837)	(263)	(455)
	40,877	181,450	41,905	184,840	57,028	261,000
	(1,581)	(630)	(1,115)	(3,346)	(1,580)	(2,729)
$(\hat{\rho}_1, \hat{\rho}_2)$	21,403	90,477	11,056	47,855	9,749	46,269
	(1,004)	(407)	(346)	(430)	(163)	(968)
	42,806	180,950	44,223	191,420	58,492	277,620
	(2,008)	(813)	(1,382)	(1,720)	(977)	(5,811)
$(0.6, \hat{\rho}_2)$	19,015	89,993	13,321	61,394	11,558	56,723
	(503)	(429)	(506)	(884)	(423)	(826)
	38,029	179,990	53,285	245,570	69,346	340,340
	(1,006)	(858)	(2,026)	(3,536)	(2,540)	(4,956)

As correlation increases, the required sample size increases

Summary

- Biometric technology provides a strong method of linking persons to identity records
- Biometric traits cannot be easily shared, misplaced, or forged offering better security and accountability
- Improves enterprise security and reduces fraud
- But these systems are not foolproof
- Government mandates mean that biometrics will have profound influence on our daily lives
- How will biometrics technology evolve? It will depend on performance, added value of technology, user acceptance & credibility of service provider

"I'm sorry, but someone else with that identity is already here."