

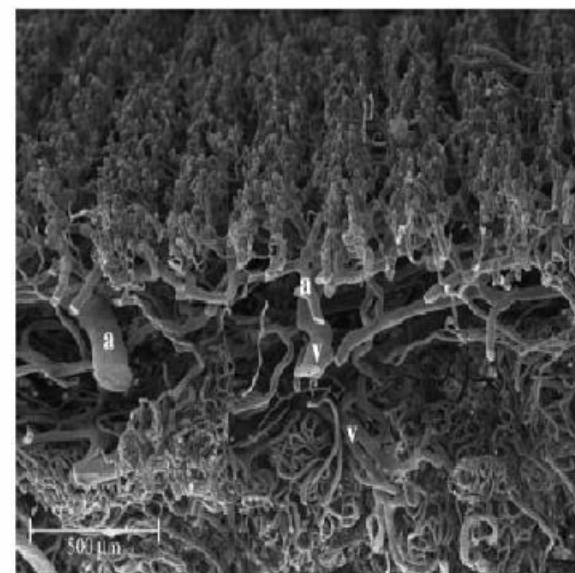
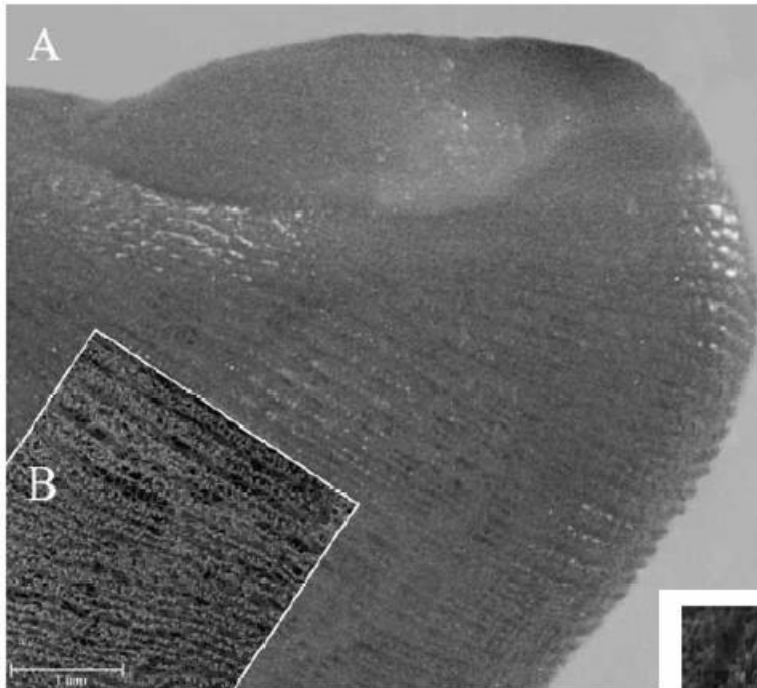
Biometrics: Machines recognizing people

Biometrics & Authentication Technologies: security issues

Andy Adler

Systems and Computer Engineering, Carleton

Finger anatomy



*From S. Sangiorgi et al.,
"Microvascularization of the human digit
as studied by corrosion casting," J. Anat.
204, 123 – 131 (2004)*

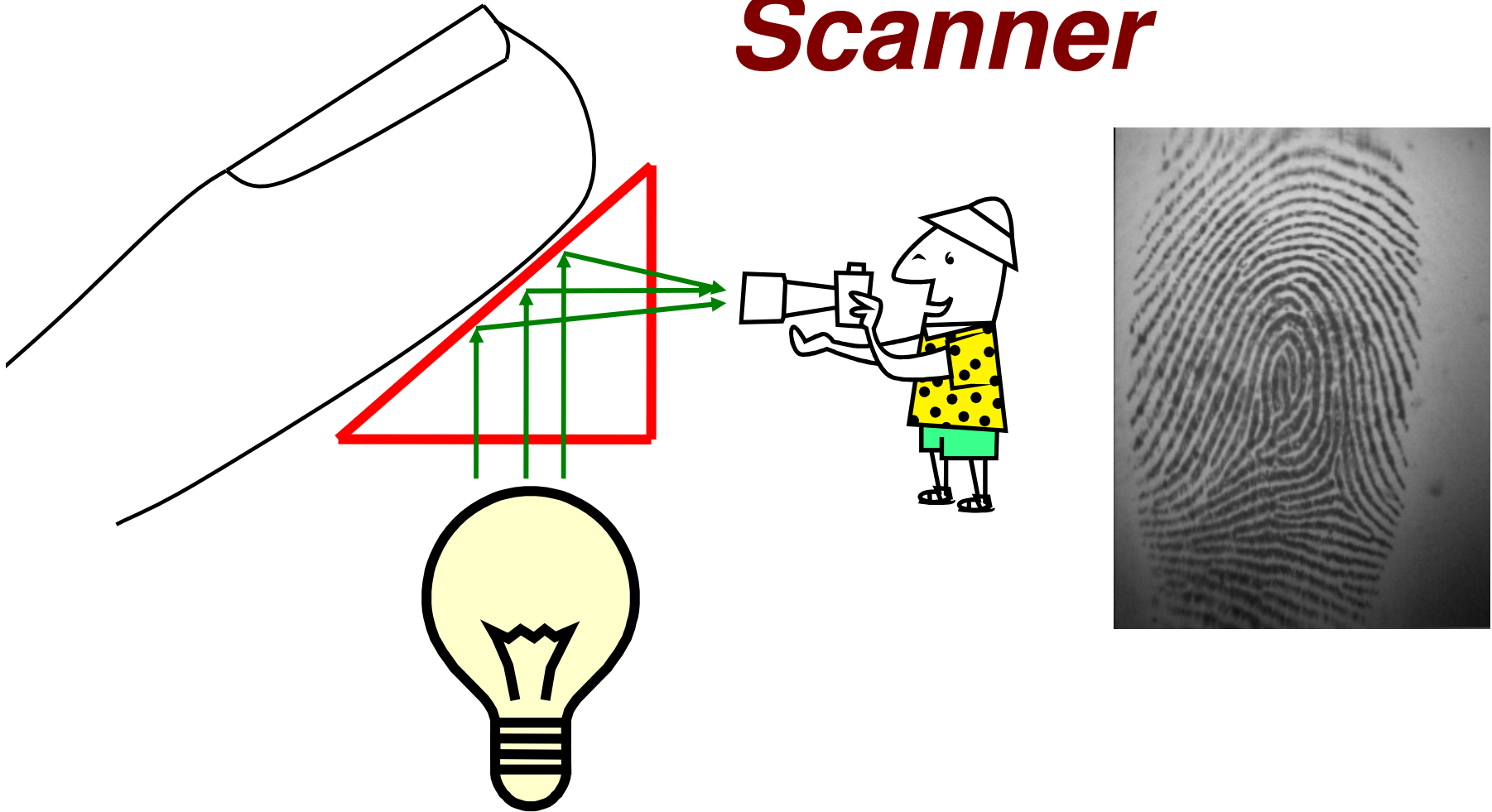
Fingerprint: ***Rolled ink***



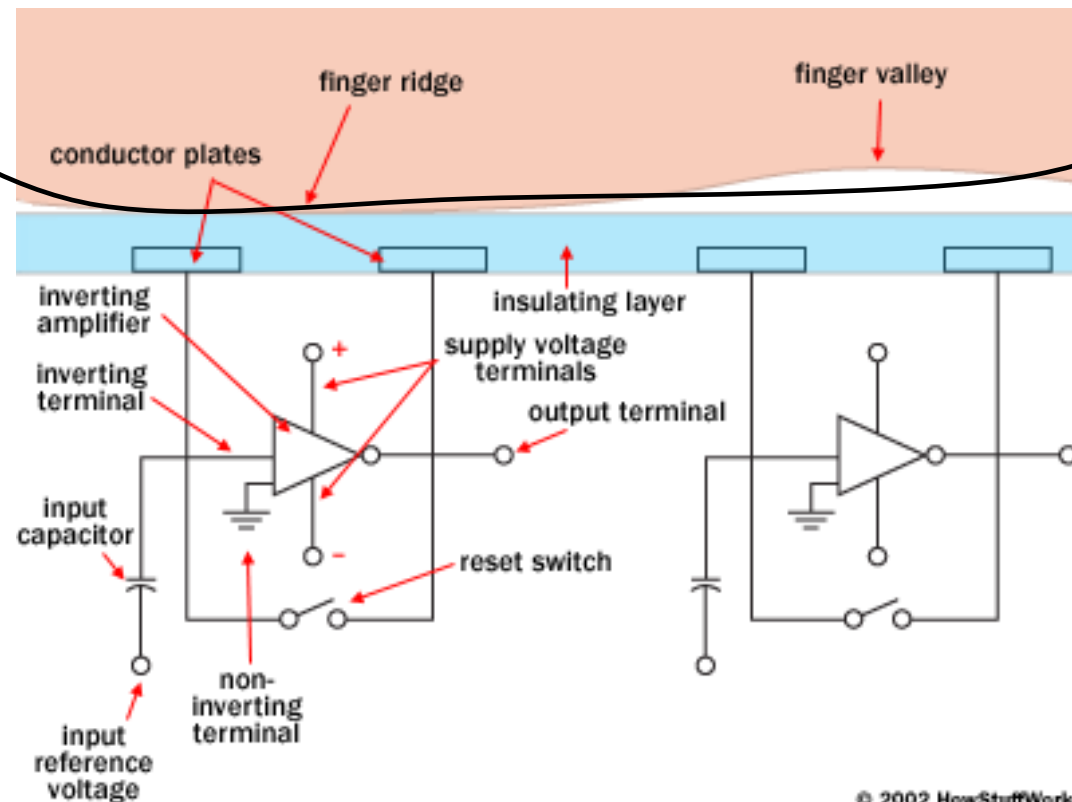
Ink Roller



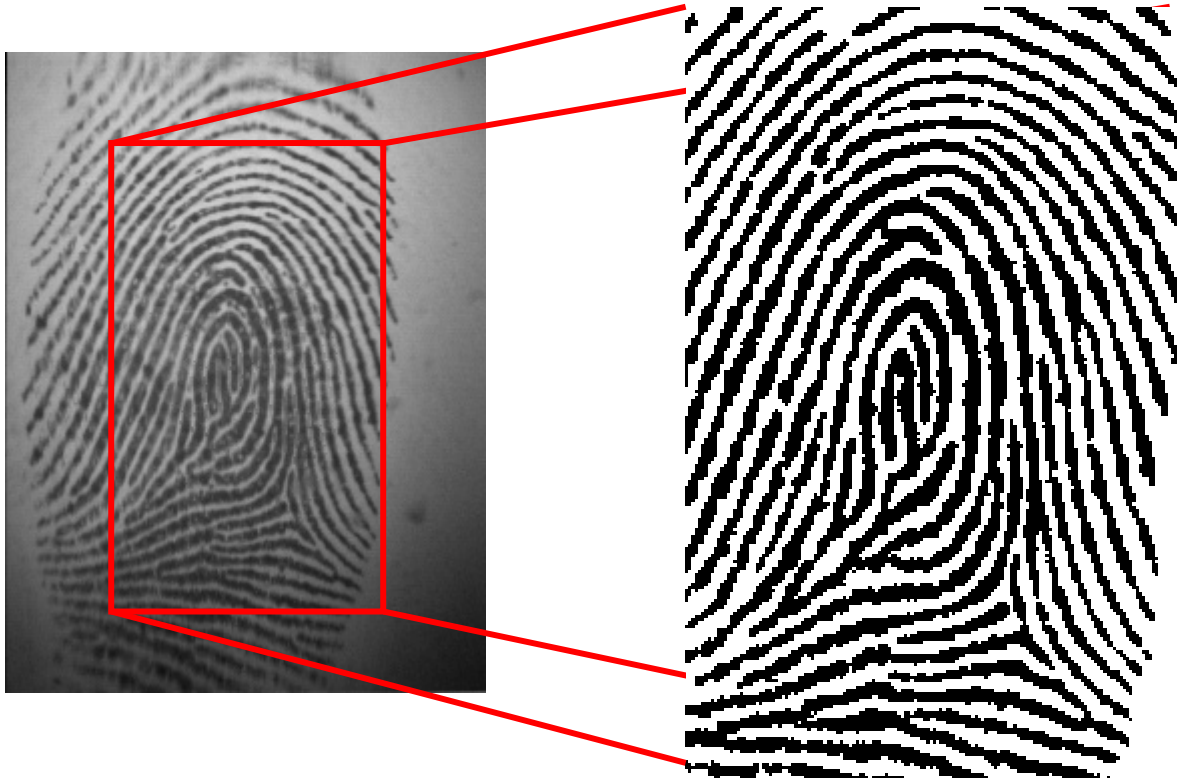
Fingerprints: *Optical Scanner*



Fingerprints: *Capacitive scanner*



Cleaned fingerprint



Get features: *minutiae*



Fingerprint: *Compare*



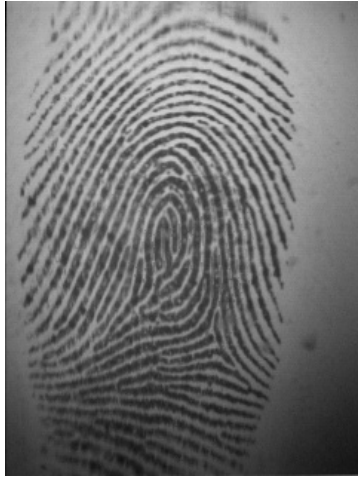
**Optical
Scanner
1998**



**Capacitive
Scanner
2004**

Get features: *minutiae*

1998



Compare
and
Decide

2004



Fingerprint examples

Thumbs from my family



Age 4

Age 6

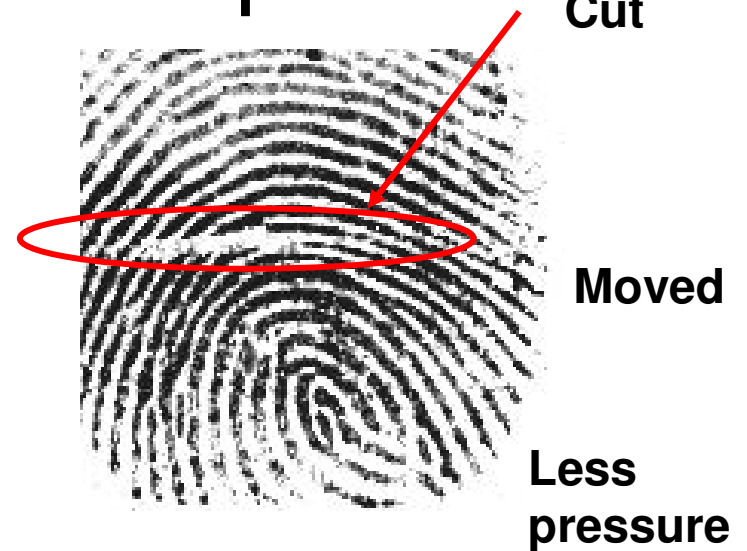
Age 34

Age 35

Age 65

Are fingerprints unique?

What do you mean by unique?



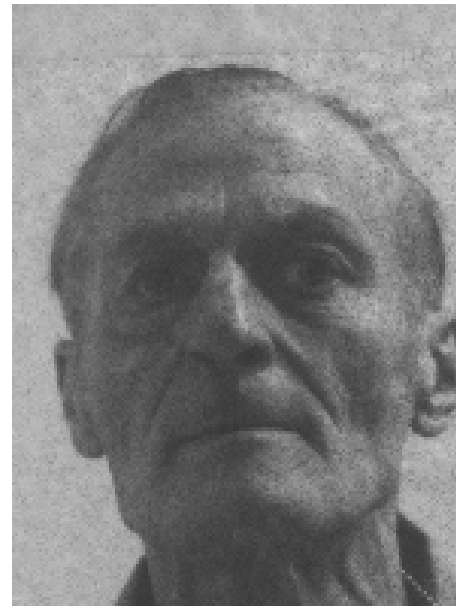
Real Question:

Are fingerprints distinguishable?

What does Unique mean?

- No differences at all
 - But then fingers change every day
- Detectably different
 - But our detection algorithm keep getting better
- How informative is a fingerprint
 - “the decrease in uncertainty about the identity from a biometric measurement”

Face Recognition:



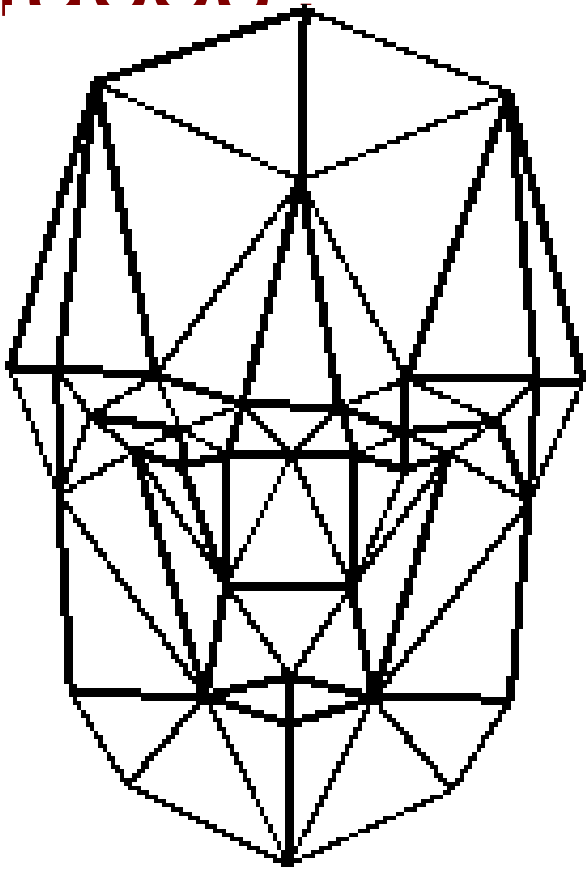
same person?

Same
person?

Yes

- I have just demonstrated a massively parallel face recognition computer
- Question:
Are computers better or worse than people at faces?

How do computers recognize faces?

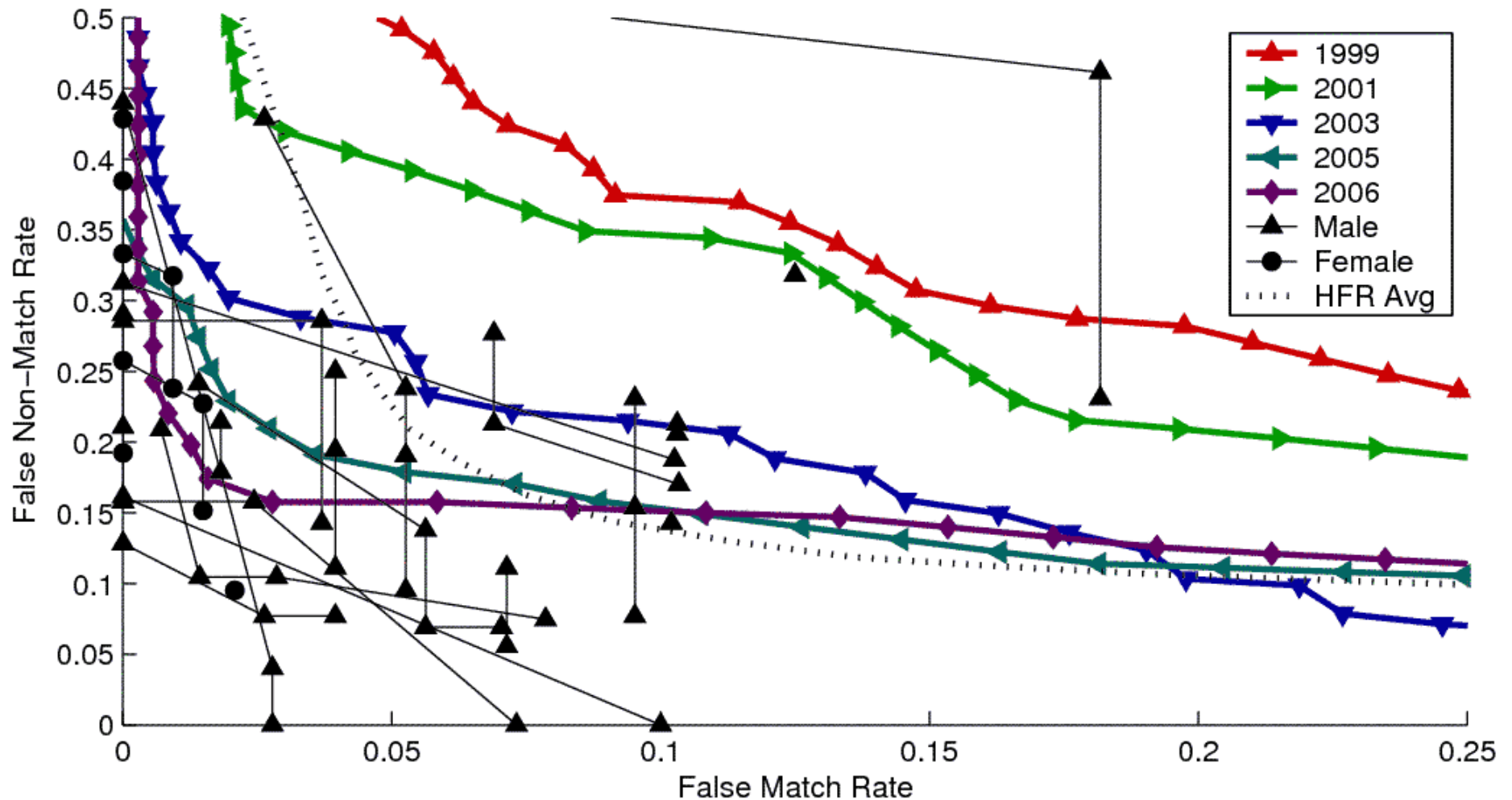


Landmarks

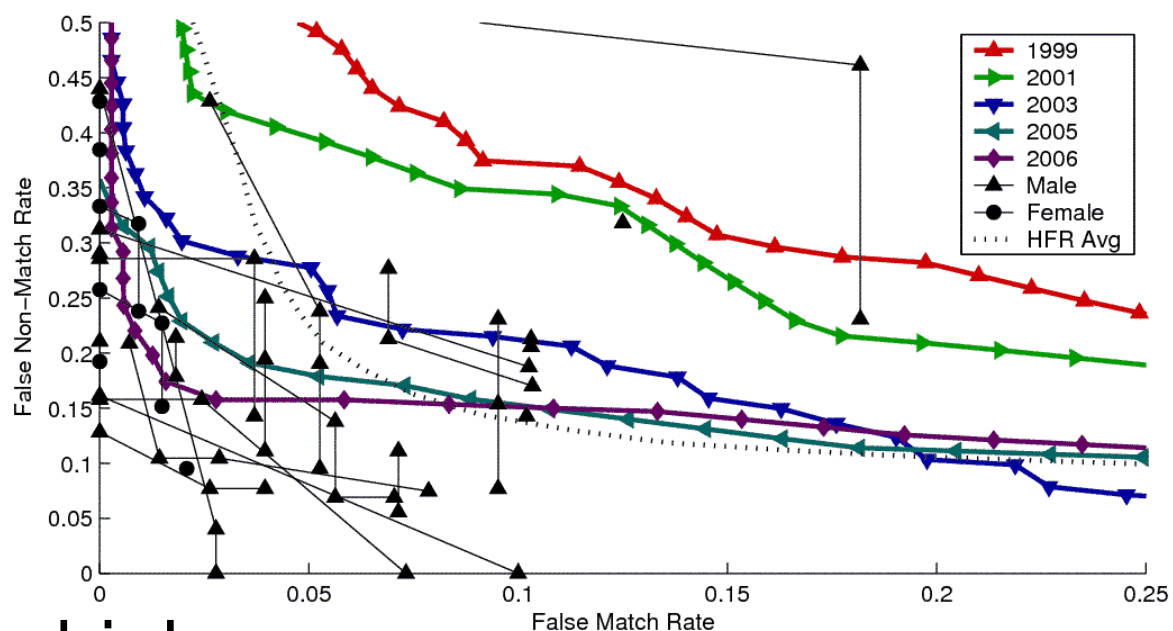


Eigenfaces

Today's FR algs are better than half of people

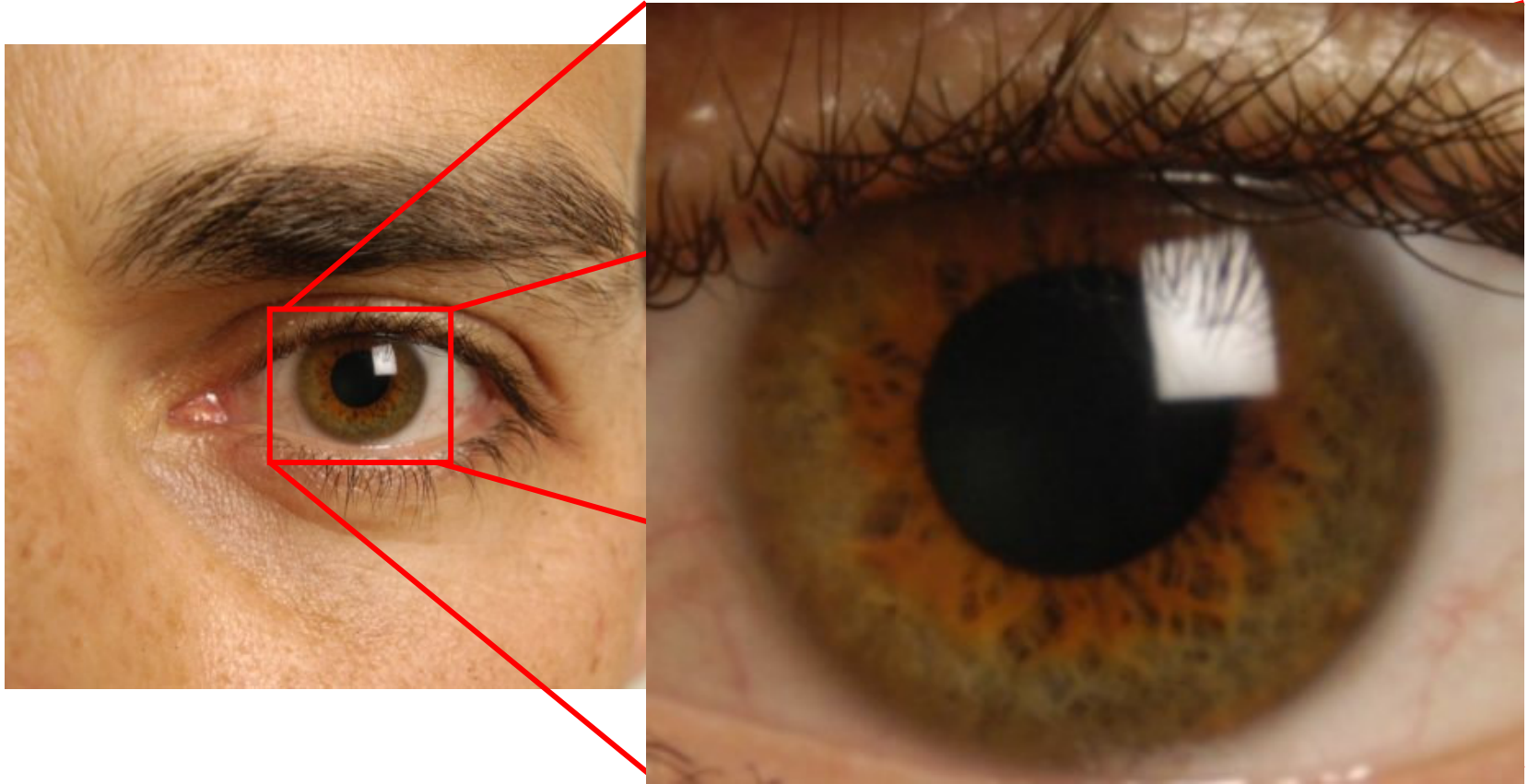


Results

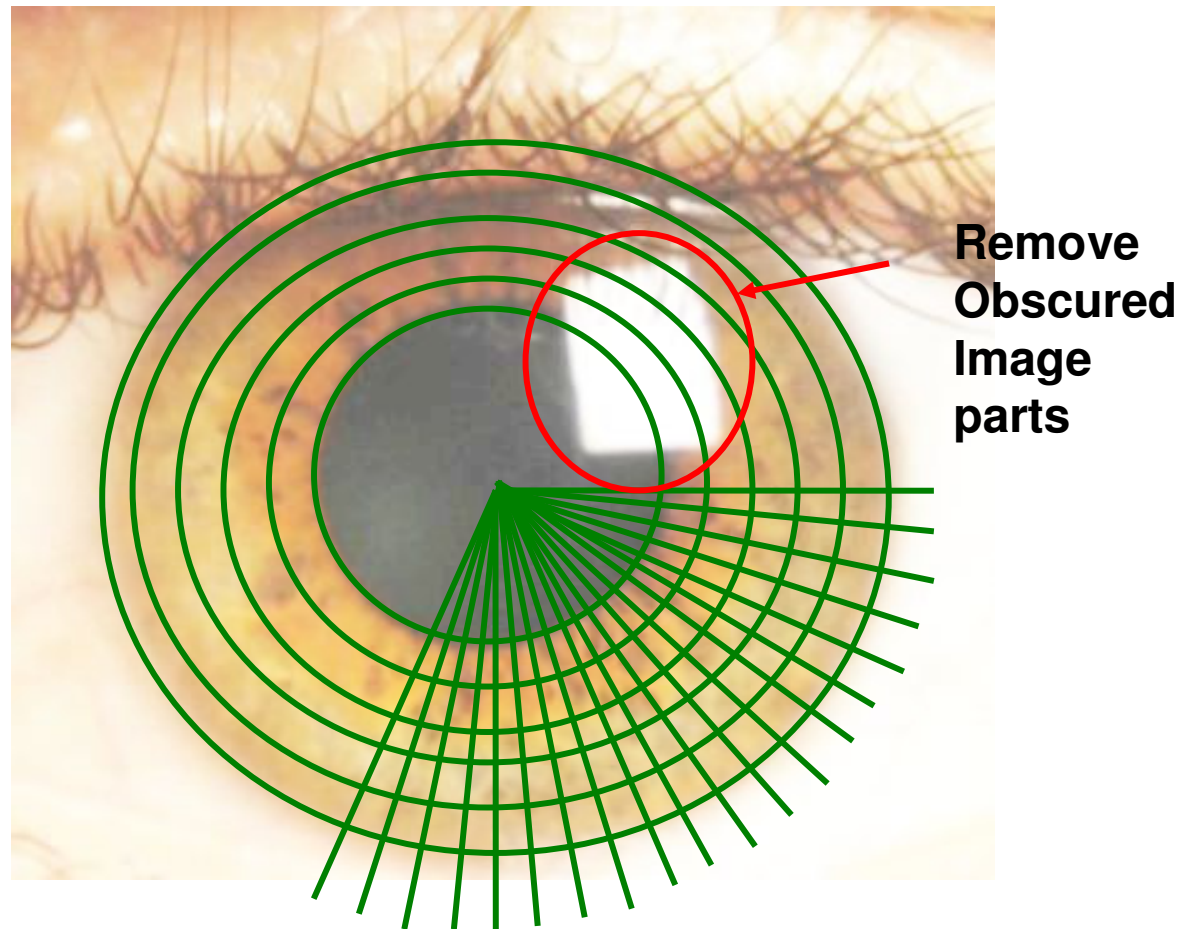


- Error rates are high
- Significant improvement in SW 1999-2006
- Most recent algs outperform about half of people
- No significant difference male/female

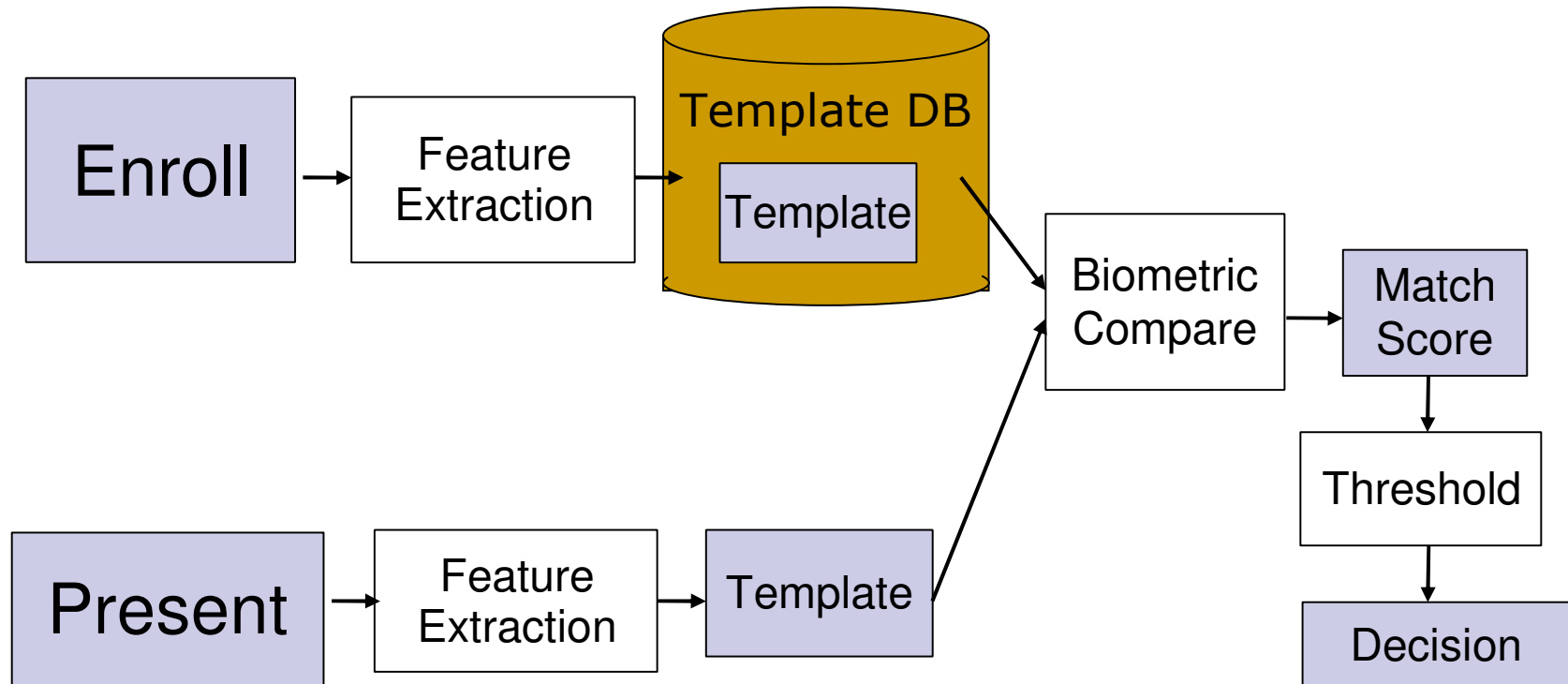
Iris



Iris: *Processing*



How is this used?



What can go wrong?

Very approximate values! Depends on all sorts of things

	Face	Finger	Iris
Failure to enroll	0%	3%	7%
Failure to acquire	3%	10%	10%
False Match	1%	10ppm	10ppm
False non-match	5%	1-5%	1-5%

Biometrics Vulnerabilities

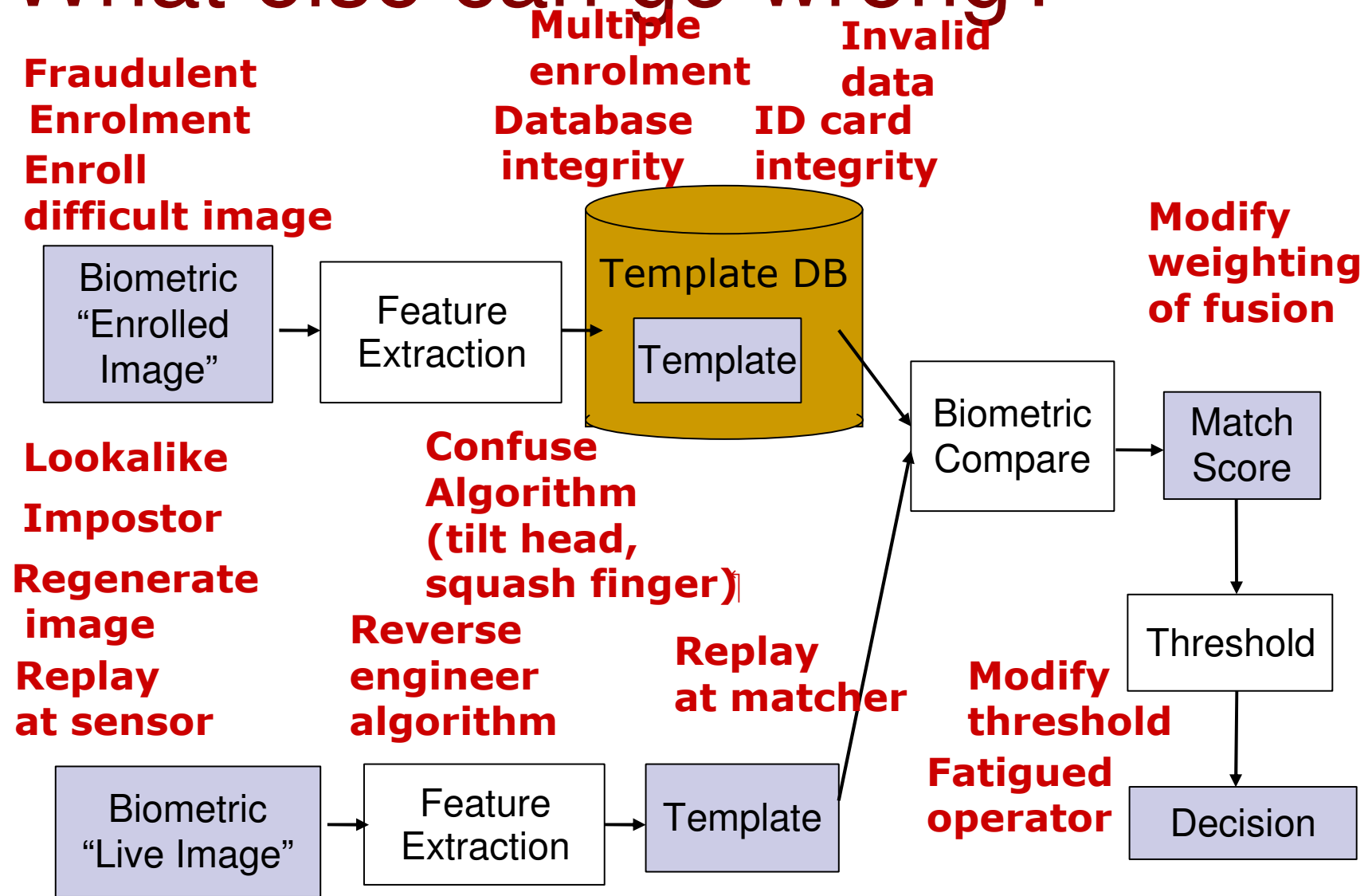
Taxonomy (from Maltoni et al, 2003):

- ❑ Circumvention
- ❑ Covert acquisition
- ❑ Collusion / Coercion
- ❑ Denial of Service

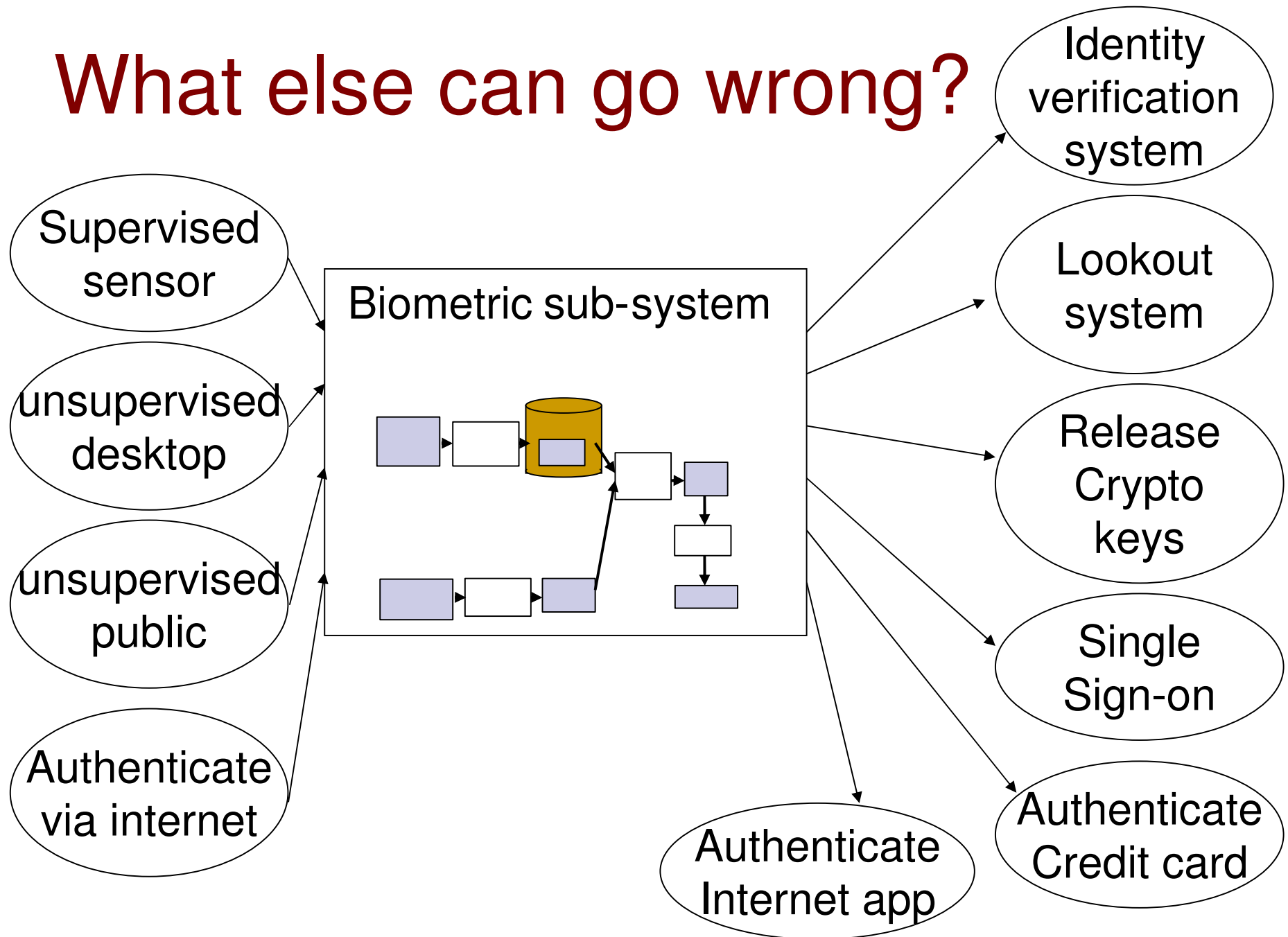
Biometrics Security Issues

- Biometrics are not secrets
- Biometrics cannot be revoked
- Biometrics have secondary uses

What else can go wrong?



What else can go wrong?


























Spoofting



Who manages registration?

<i>Who</i>	<i>What</i>	<i>Example</i>
Government	Passport	Iris for fast passenger processing
Industry	Credit card	Voiceprint. Callback to validate sales
Individual	Cell Phone	User locks phone with fingerprint

	<i>Vulnerable</i> 	Pass- port	Credit Card	Cell phone
	<i>Secure</i> 			
Theft				
Duplication				
Theft and modification		$\frac{1}{2}$	$\frac{1}{2}$	
Registration fraud		$\frac{1}{2}$		
Spoofing		$\frac{1}{2}$	$\frac{1}{2}$	
Phishing				
“Dumpster Diving”				
Secondary use of data		$\frac{1}{2}$		
Privacy worries				

More details / my research ...

Biometrics Security

- Biometric uniqueness / entropy
- Biometric template protection
- Flaws in biometric encryption

information content of a biometric measurement?

Or

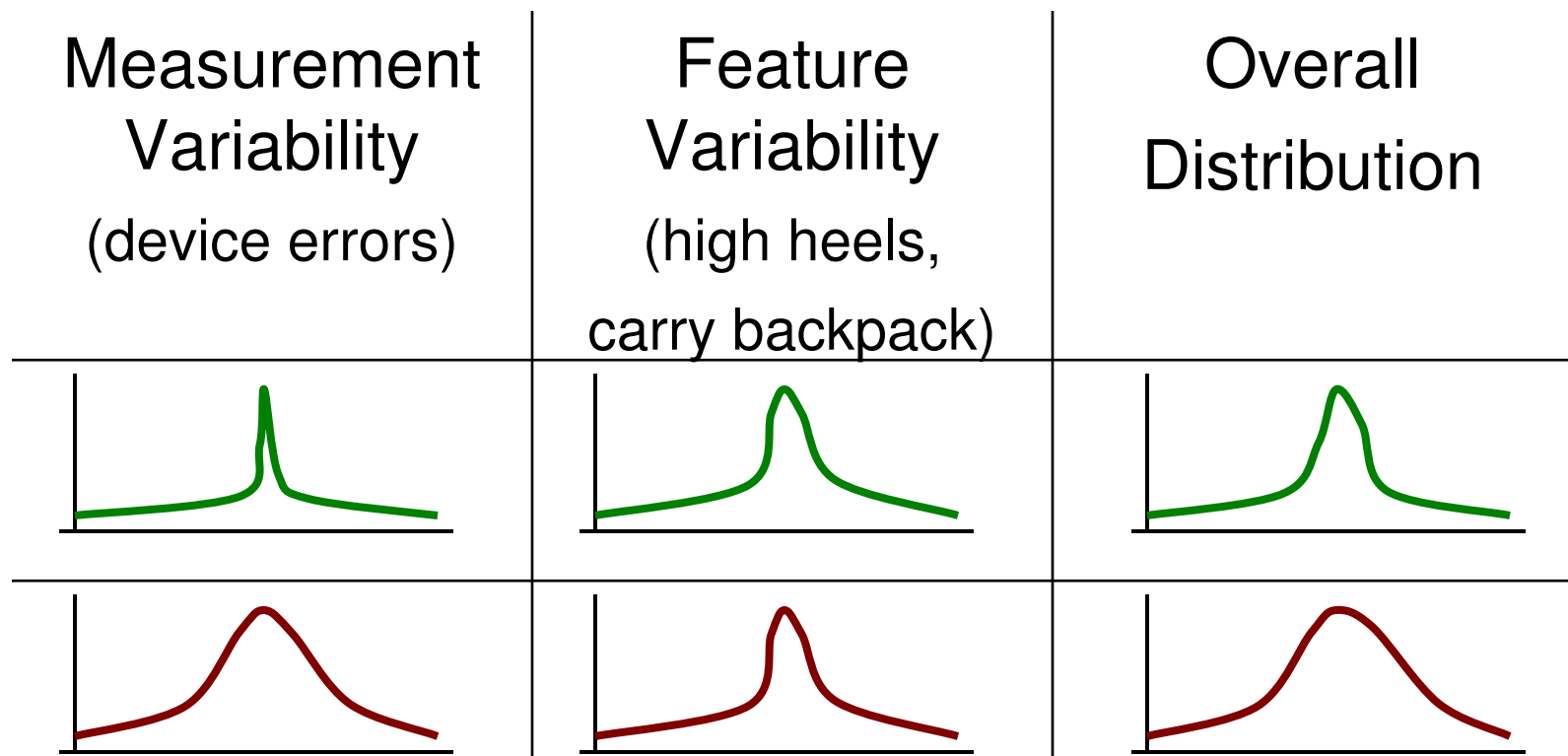
- How much do we learn (about identity) from a biometric image

Or

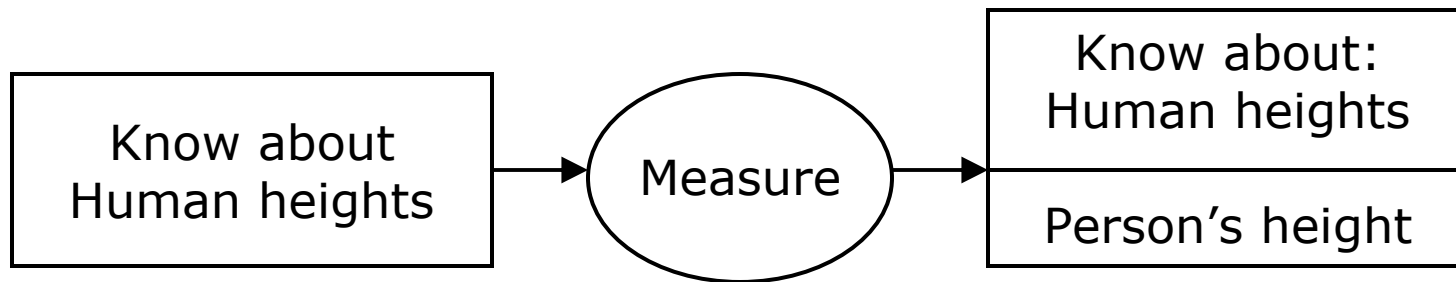
- How much privacy do we lose on releasing a biometric image

Example: measure *Height*

- **Measure #1** (at doctor's office, ie. accurate)
- **Measure #2** (via telescope, ie. inaccurate)



Example: measure *Height*



- How much information learned?

	Average (5½' tall)	Tall (7½' tall)
Measure #1	Low	Quite a lot
Measure #2	Almost zero	Low

Proposed measure:

relative entropy $D(p||q)$

- Given biometric feature vector \mathbf{x}
- Distributions
 - intra-person distribution, $p(\mathbf{x})$
 - inter-person distribution, $q(\mathbf{x})$
- $D(p||q)$ measures inefficiency of assuming q when true distribution is p

Or,

- $D(p||q)$ measures extra information in p than q

Applications: *biometric*

- Meta algorithm
 - Evaluate a new biometric feature
- Biometric Performance limits
 - Template size limits
 - Inherent match performance limits
- Feasibility of Biometric Encryption
 - Limits to Key Length

Applications: *abstract*

- Quantify privacy
 - What is the privacy risk due to the release of certain information?
 - What is the privacy gain in obscuring faces?
- Uniqueness of biometrics
 - Approach to address: “Are faces / fingerprints / irises unique?”

Biometric template security

It is claimed to be impossible or infeasible to recreate the enrolled image from a template.

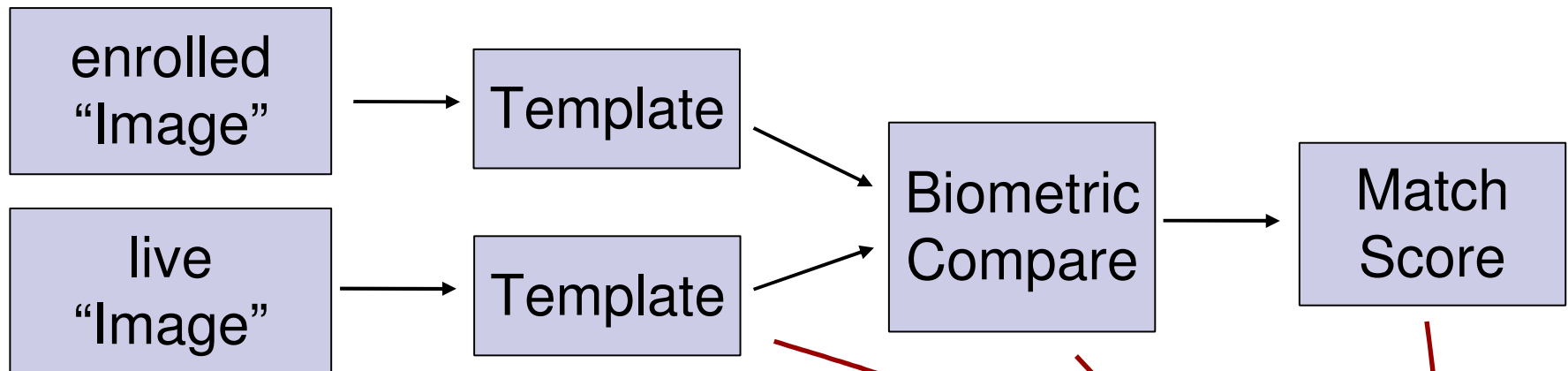
Reasons:

- ❑ templates record features (such as fingerprint minutiae) and not image primitives
- ❑ templates are typically calculated using only a small portion of the image
- ❑ templates are much smaller than the image
- ❑ proprietary nature of the storage format makes templates infeasible to "hack".

Images can be regenerated

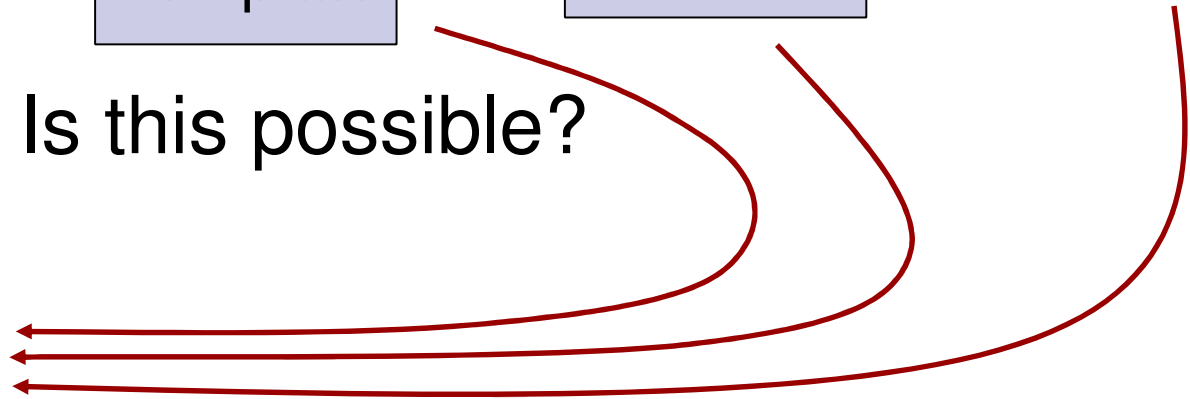
...?

- Typical Biometric processing



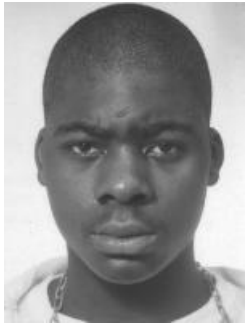








- *Question:* Is this possible?

regenerated
"Image"



Hill-climbing: begin with a guess, make small modifications; keep modifications which increase the match score

Results:

	Initial Image	Iteration 200	Iteration 600	Iteration 4000	Target Image
A					
B					

Improved regenerated image



Average of 10
Best Estimates



Target Image

- Recently, this approach has been extended to fingerprint images (Uludag, Ross, Capelli)

Implications: image regeneration

1. Privacy Implications

- ❑ ICAO passport spec. has templates encoded with public keys in contactless chip
- ❑ ILO seafarer's ID has fingerprint template in 2D barcode on document

Implications: image regeneration

2. Reverse engineer algorithm

- Regenerated images tell you what the algorithm 'really' considers important

Target

Alg. #1

Alg. #2

Alg. #3 doesn't care about nose width



Implications: image regeneration

3. Crack biometric encryption

Biometric encryption seeks to embed a key into the template. Only a valid image will decrypt the key

- Since images vary
Enrolled image + Δ => release key
- However
Enrolled image + Δ + ϵ => no release

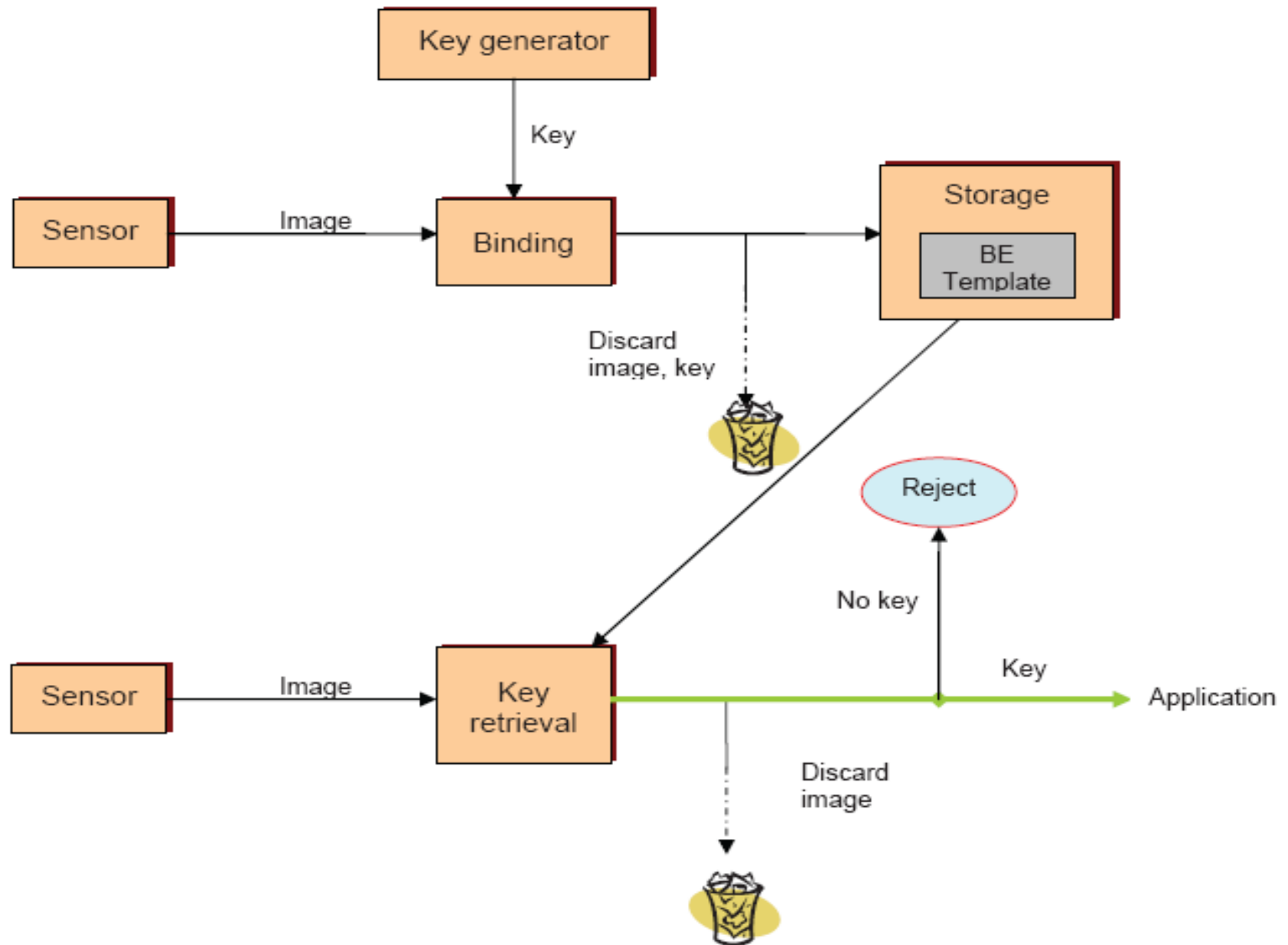
If we can get a measure of how close we are, then we can get a *match score*

Biometric Encryption

- Recent paper by Ontario Information and Privacy Commissioner
 - “Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy”
 - A. Cavoukian, A. Stoianov

My concern:

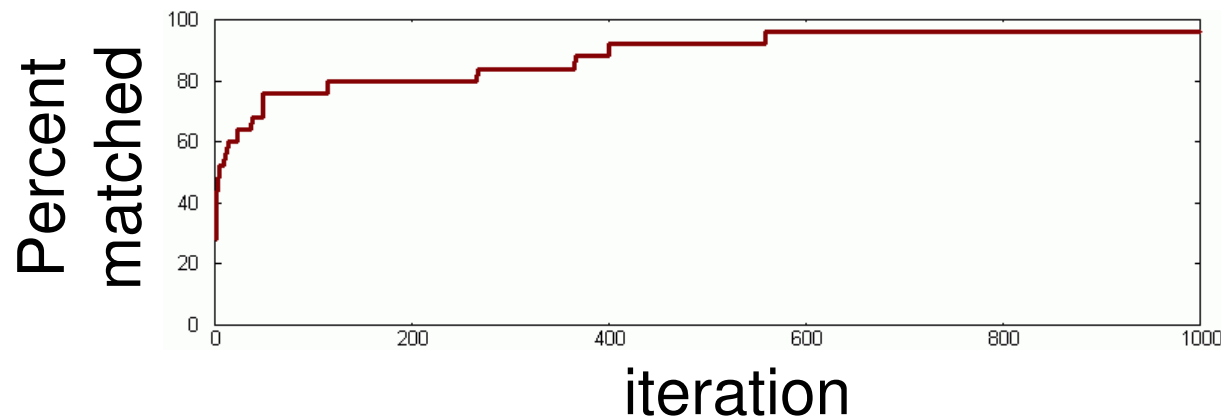
- Biometric Encryption (and biometric cryptographic schemes in general) only offer benefits if they are cryptographically secure.



From: http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

Crack biometric encryption

- Construct *match-score* from number of matching elements in *link table*
- Use quantized template reconstructor



enrolled

Fuzzy Vaults for fingerprints

(Clancy, 2003)



Raw Fingerprint



With minutiae



With added "chaff"

Collusion Attack

- Users' fingerprints may be associated with many vaults.
 - Ex: In the smart card implementation, users will likely carry multiple smart cards associated with different companies, each locked with the same fingerprint.
- Fuzzy Vault is insecure when the same fingerprint is used to lock multiple vaults

Biometrics in Canada (Gov't)

- Passports
- Immigration
- Customs
- Defence
- Natural Resources
- Public Safety
- RCMP

Epilogue: Our future?

Operator: "Thank you for calling Pizza Hut."

Customer: "One All-Meat Special..."

Operator: "Thank you, Sir. Your voice print verifies with your National ID Number: 6102049998"

Customer: (Sighs) "I'd like to order an All-Meat Special pizza..."

Operator: "I don't think that's a good idea, sir."

Customer: "Whaddya mean?"

Operator: "Sir, your medical records indicate that you've got very high blood pressure and cholesterol. Your Health Care provider won't allow such an unhealthy choice."

Customer: "Darn. What do you recommend, then?"

Epilogue:

Operator: "You might try our low-fat Soybean Yogurt Pizza. I'm sure you'll like it"

Customer: "What makes you think I'd like something like that?"

Operator: "Well, you checked out 'Gourmet Soybean Recipes' from your local library last week, sir."

Customer: "OK, lemme give you my credit card number."

Operator: "I'm sorry sir, but I'm afraid you'll have to pay in cash. Your credit card balance is over its limit."

Customer: "@#%/\$@&?#!"

Operator: "I'd advise watching your language, sir. You've already got a July 2012 conviction for cussing ... "