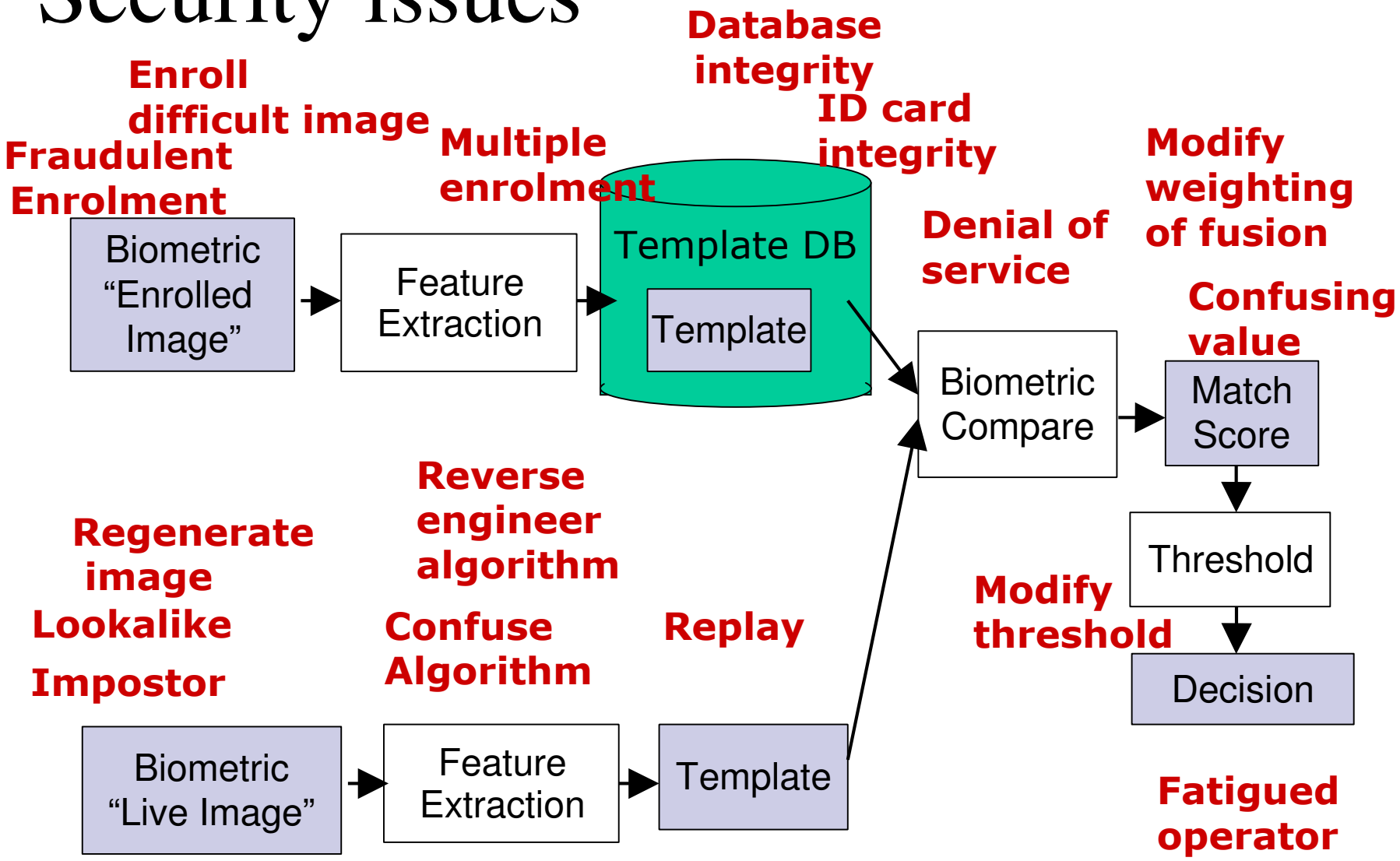
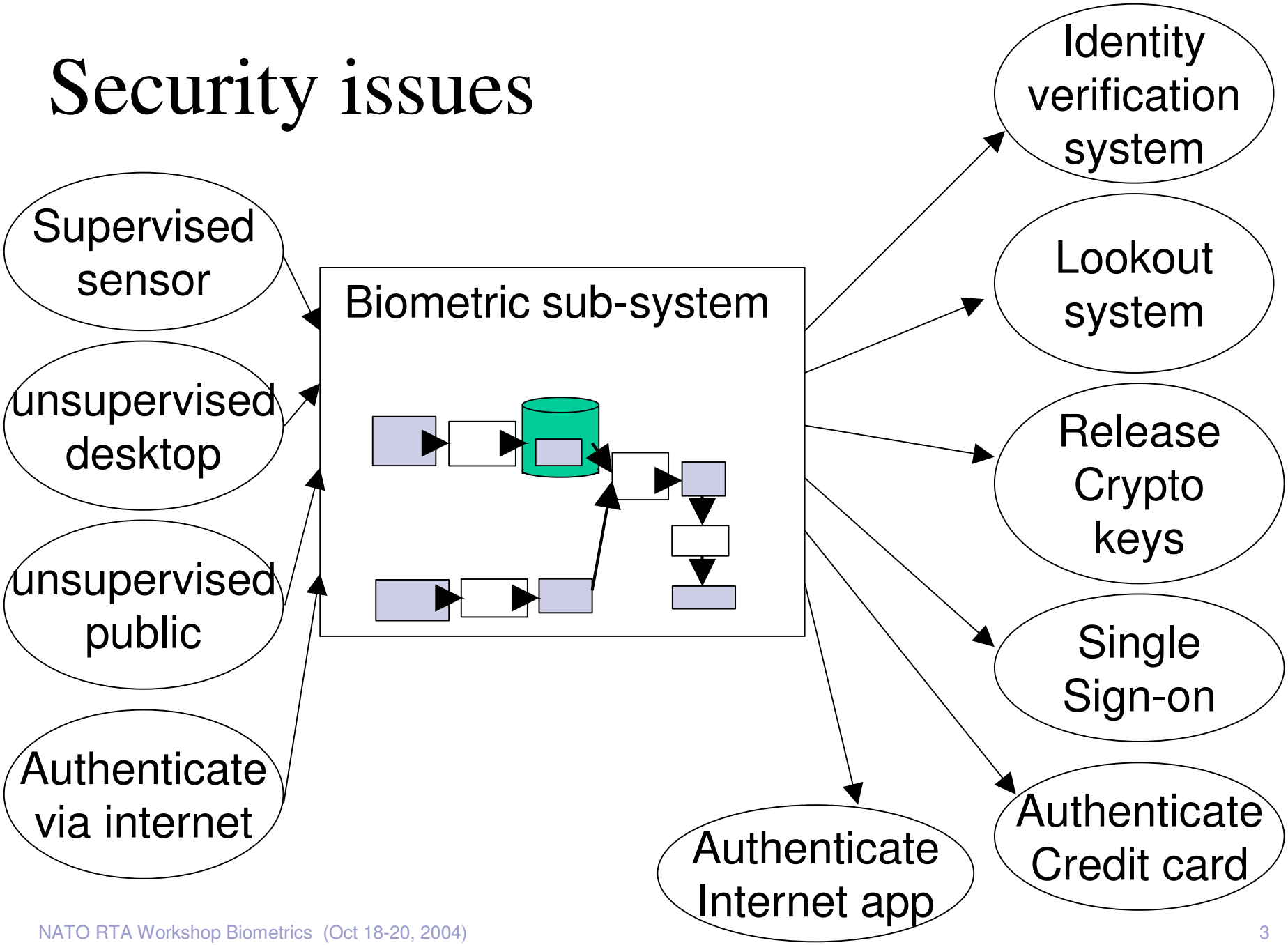
Vulnerabilities in biometric encryption systems

Andy Adler
School of Information Technology and Engineering
University of Ottawa

Security issues



Security issues



Security issues

- Biometrics only provides identity
  - Need to be coupled to a system
- These systems are also vulnerable to all of the traditional security threats
  - as well as all sorts of new ones
  - and interactions between old and new ones

Security of biometric templates

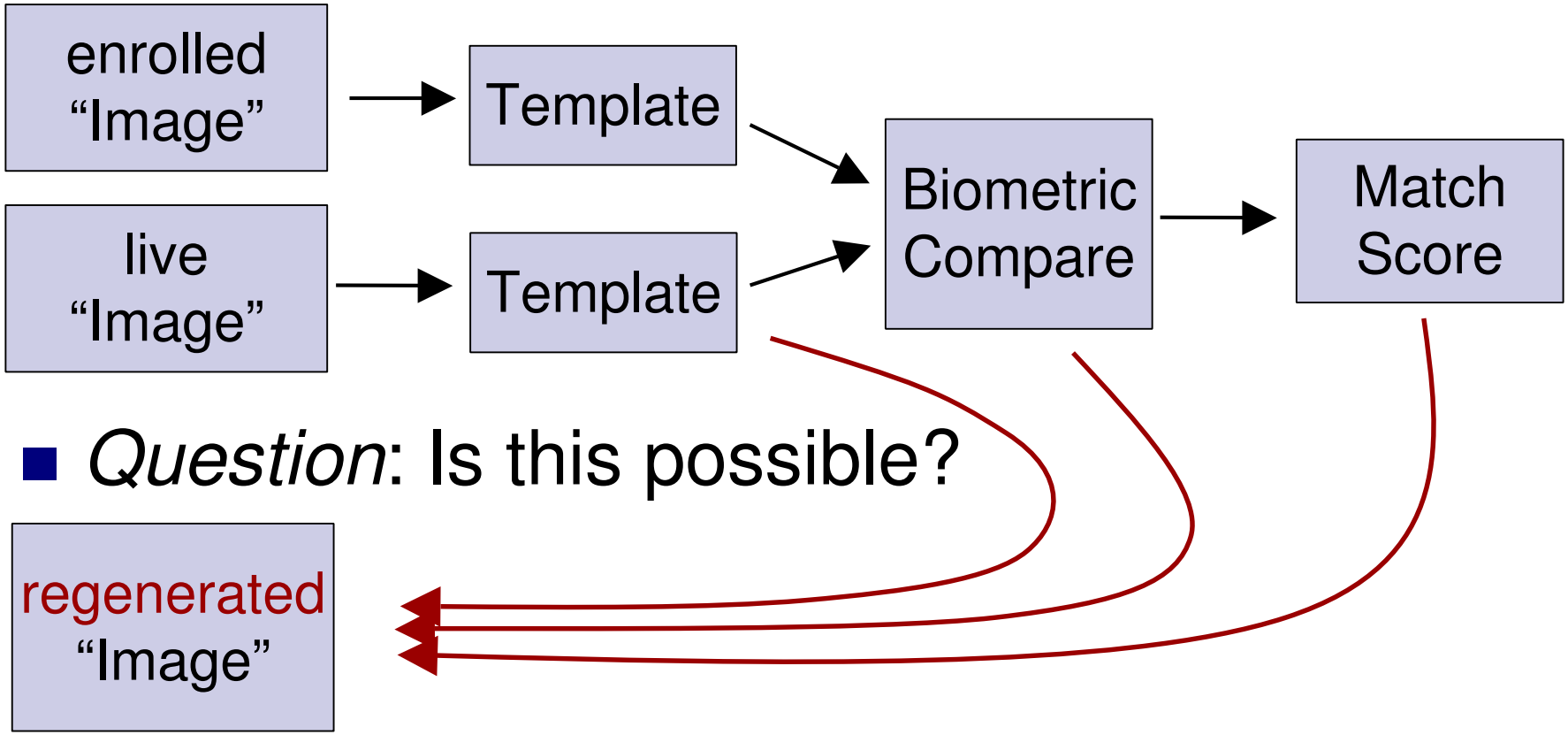
Many biometric vendors have claimed its impossible or infeasible to recreate the enrolled image from a template.

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?

Automatic image *regeneration?*

Only difficult bit.
Need an idea of a
Reasonable step

Technique: *Hill-climbing*

- Begin at a reasonable spot
- Repeat
  - Take a small random step
  - If you went up hill ➔ stay there
  - If you went down ➔ step back

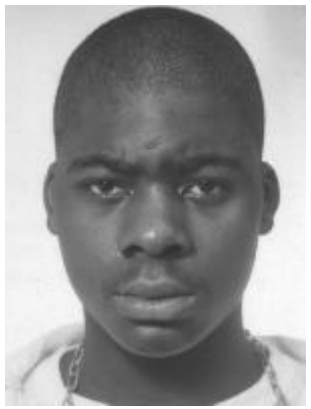
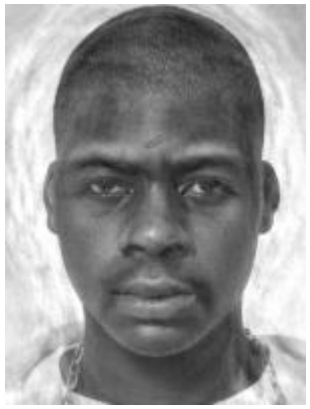
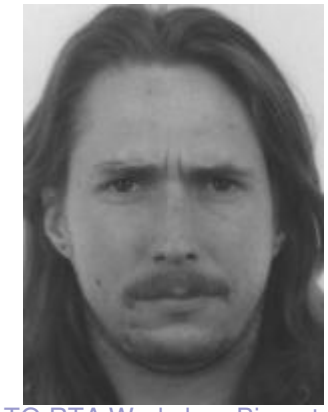
Requirement: access to a match scores

Results

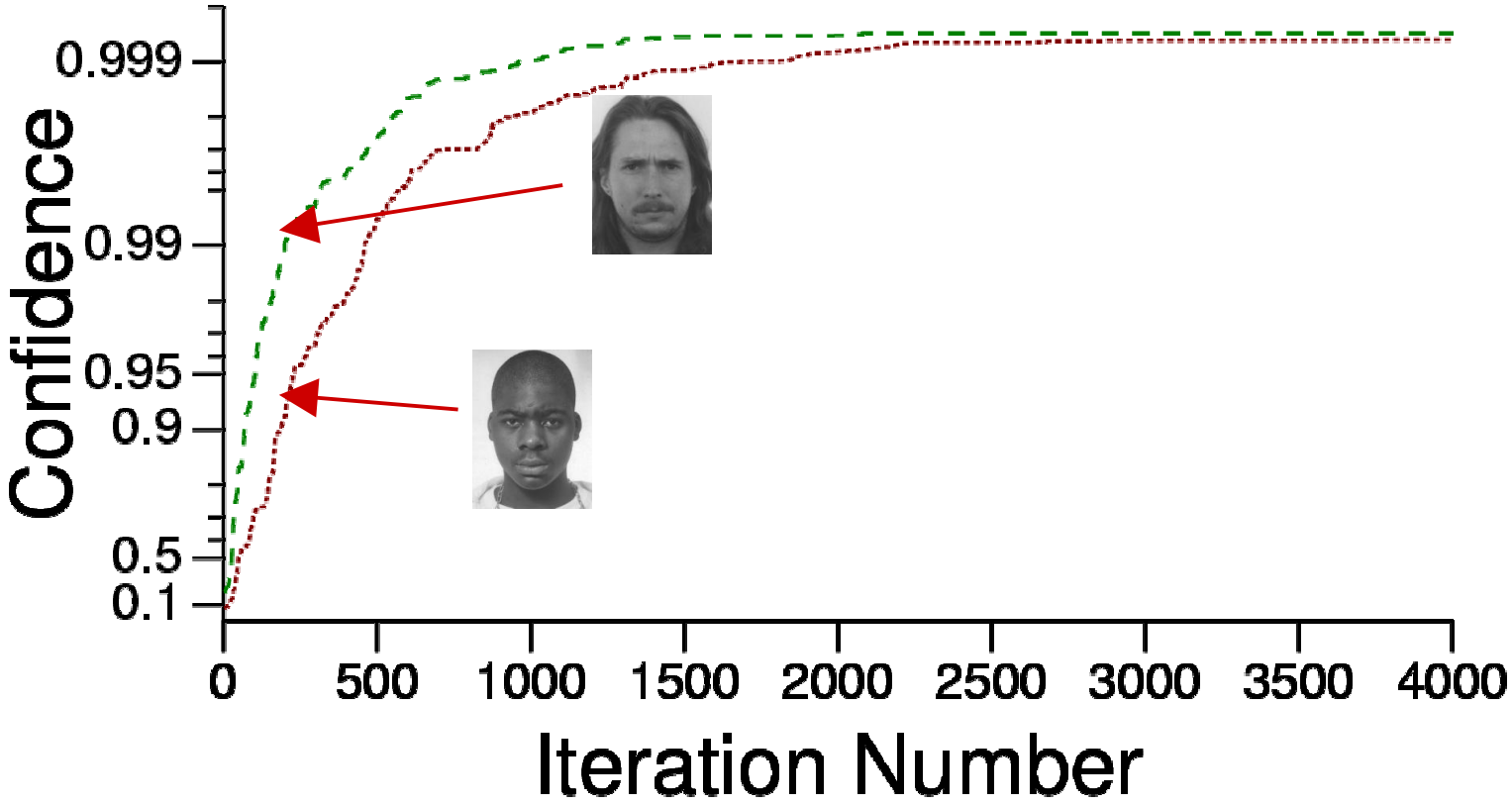
- Tests were performed against three commercial face recognition algorithms
  - Two of the vendors participated in the 2002 face recognition vendor test

- Regenerated image always compared at over 99.9% Prob.Correct Verification

Results

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

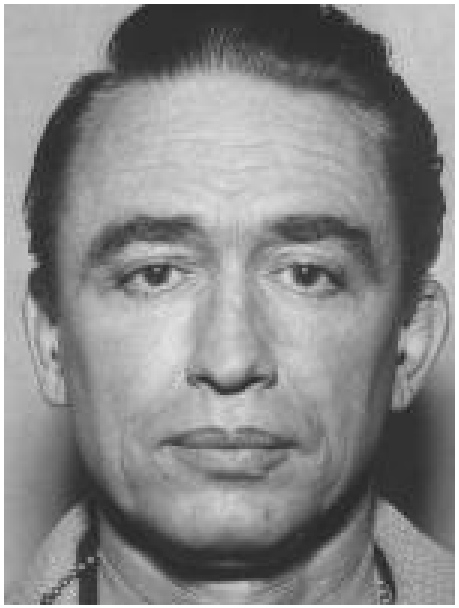
Results: Confidence vs. iteration



Confidence is the probability of correct verification for a given match score

Improved regenerated image

Average of 10
Best Estimates



Target Image

Extensions to this approach

Recently, this approach has been extended to fingerprint images

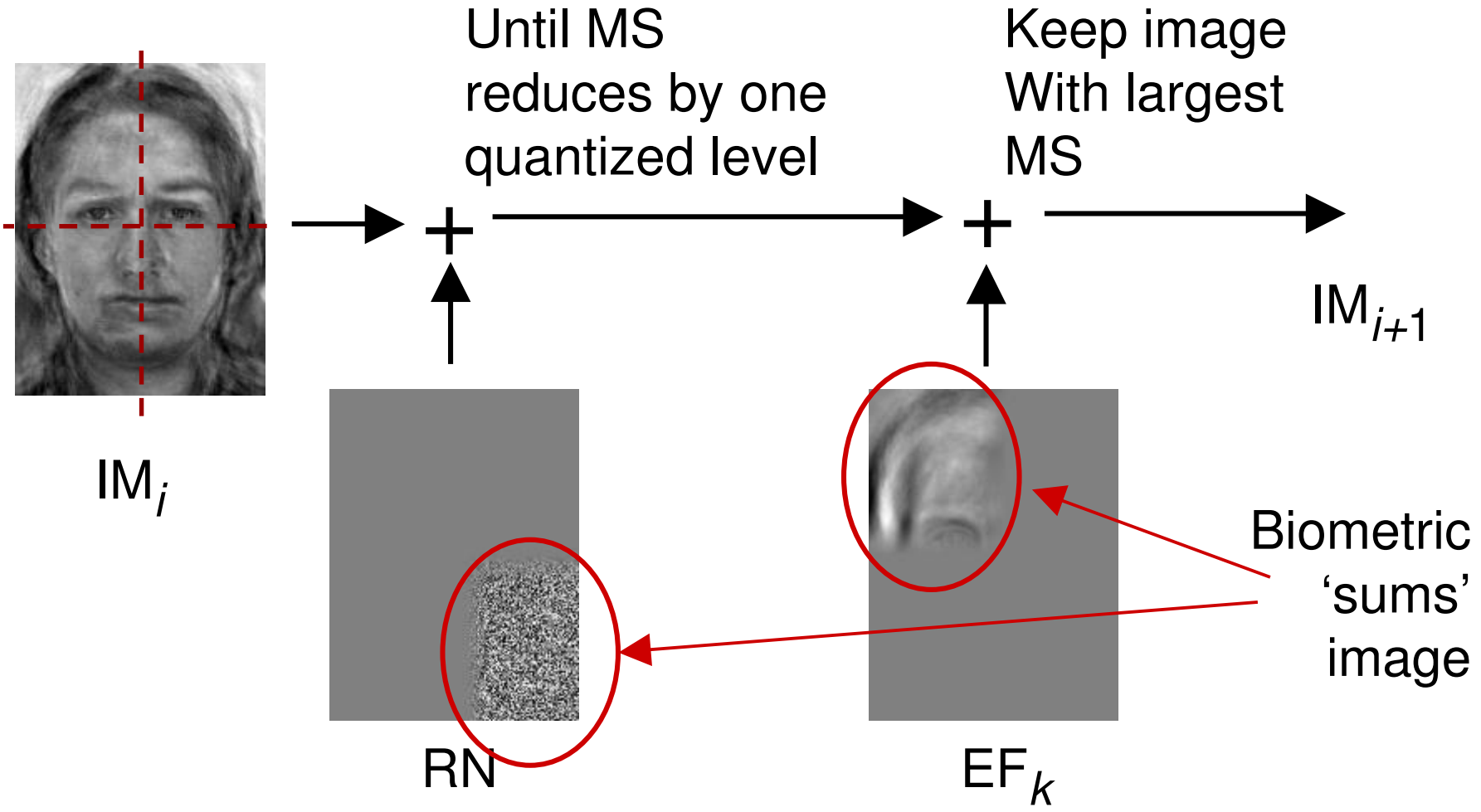
- U. Uludag *et al* developed an approach to modify a collection of minutiae
- A. Ross *et al.* has developed a fingerprint image regenerator

Protection:

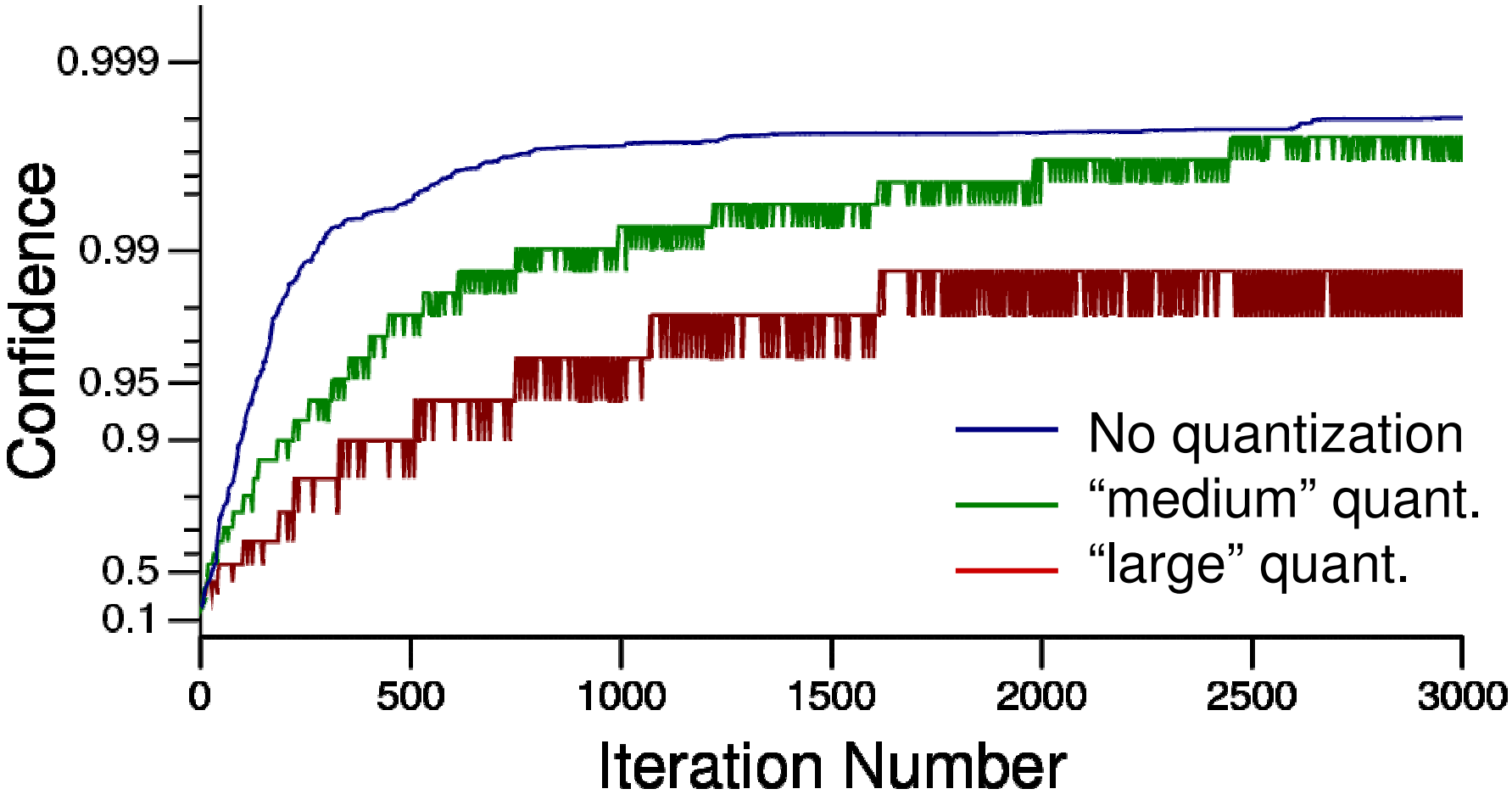
According to BioAPI

- "…allowing only discrete increments of score to be returned to the application eliminates this method of attack."
- Idea: most image modifications will not change the match score

Modified “hill-climbing”



Results: modified “hill-climbing”



Implications: image regeneration

1. Regenerate images for spoofing
   - 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 create a *match score*

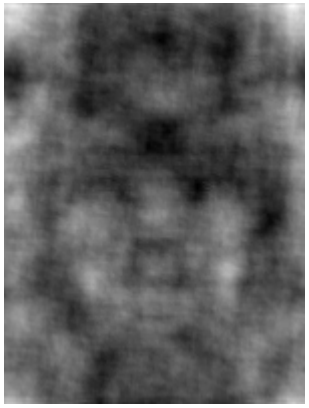
Biometric encryption (Soutar, 1998)

- Average pre-aligned enrolled image (f_0)

- Calculate template from Wiener filter

$$H_0 = F^* R_0^* / (F^* F + N^2)$$

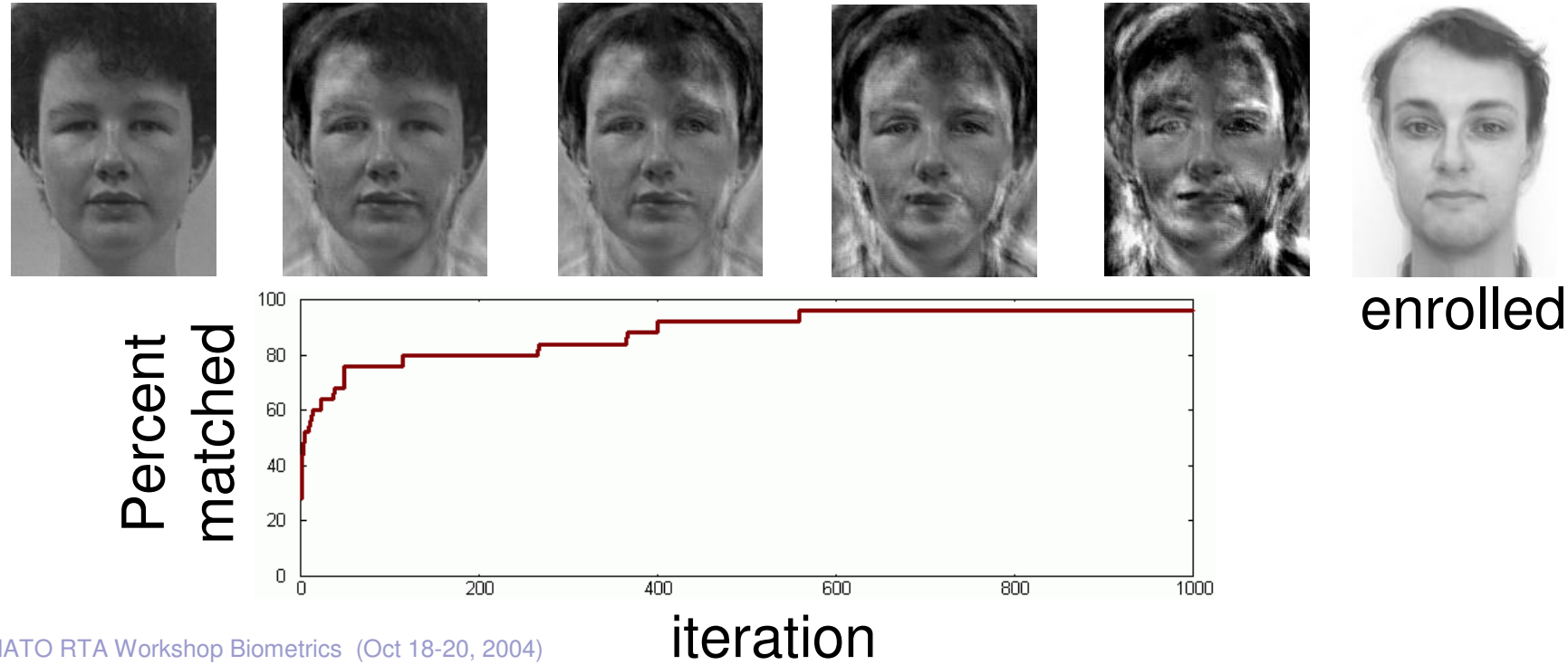
where R_0 has phase $\pm\pi/2$, ampl = 1



- Each bit of secret is linked to several bits of H_0 with same phase

Crack biometric encryption

- Construct *match-score* from number of matching elements in *link table*
- Use quantized hill climber



Summary

- There is a tendency to use results from cryptography in biometrics security
- However, biometrics images are **not** random data

- Such correlations may be exploitable in many biometric encryption systems