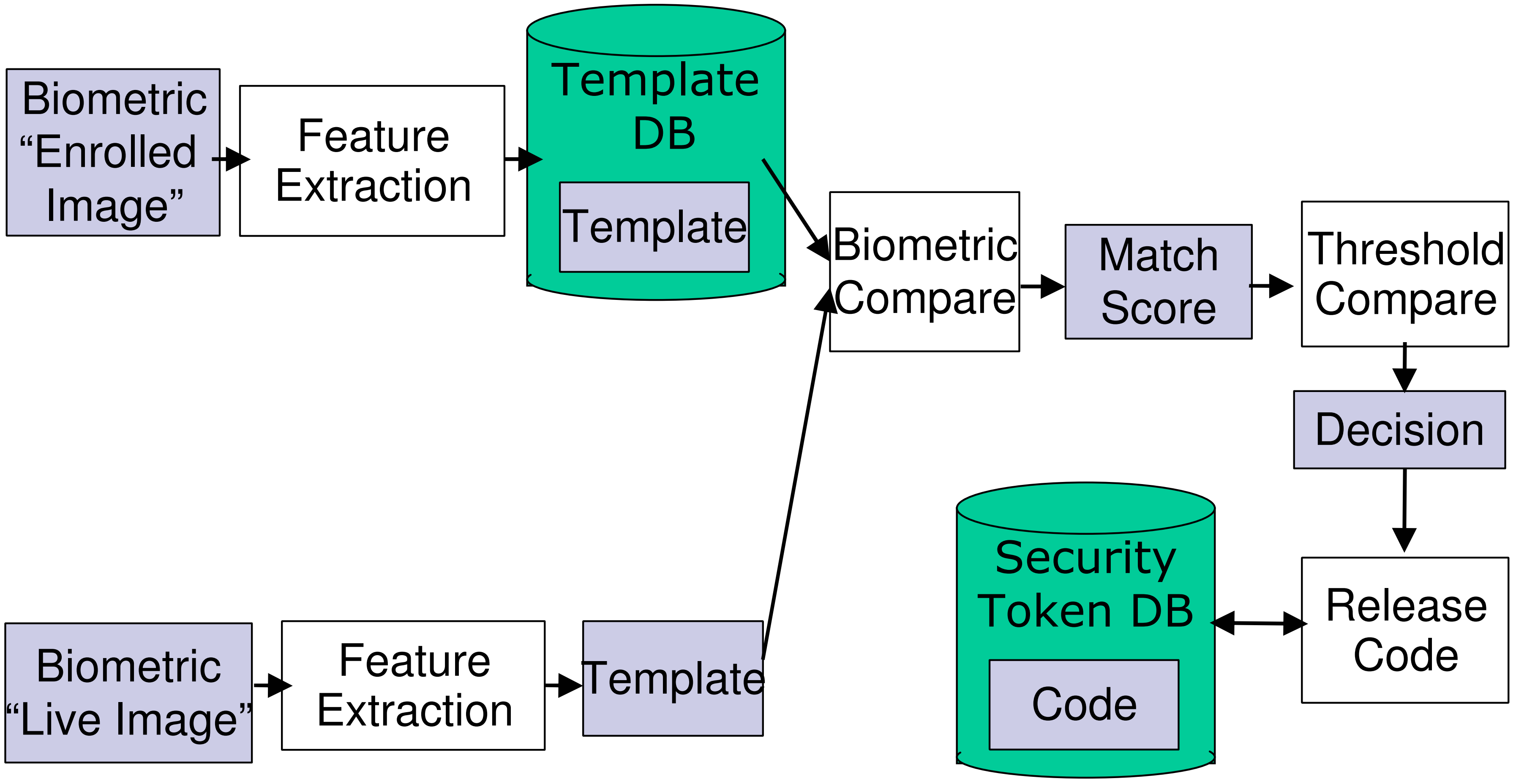
Vulnerabilities in biometric encryption systems

Andy Adler

School of Information Technology and Engineering

University of Ottawa

Traditional Biometric Verification

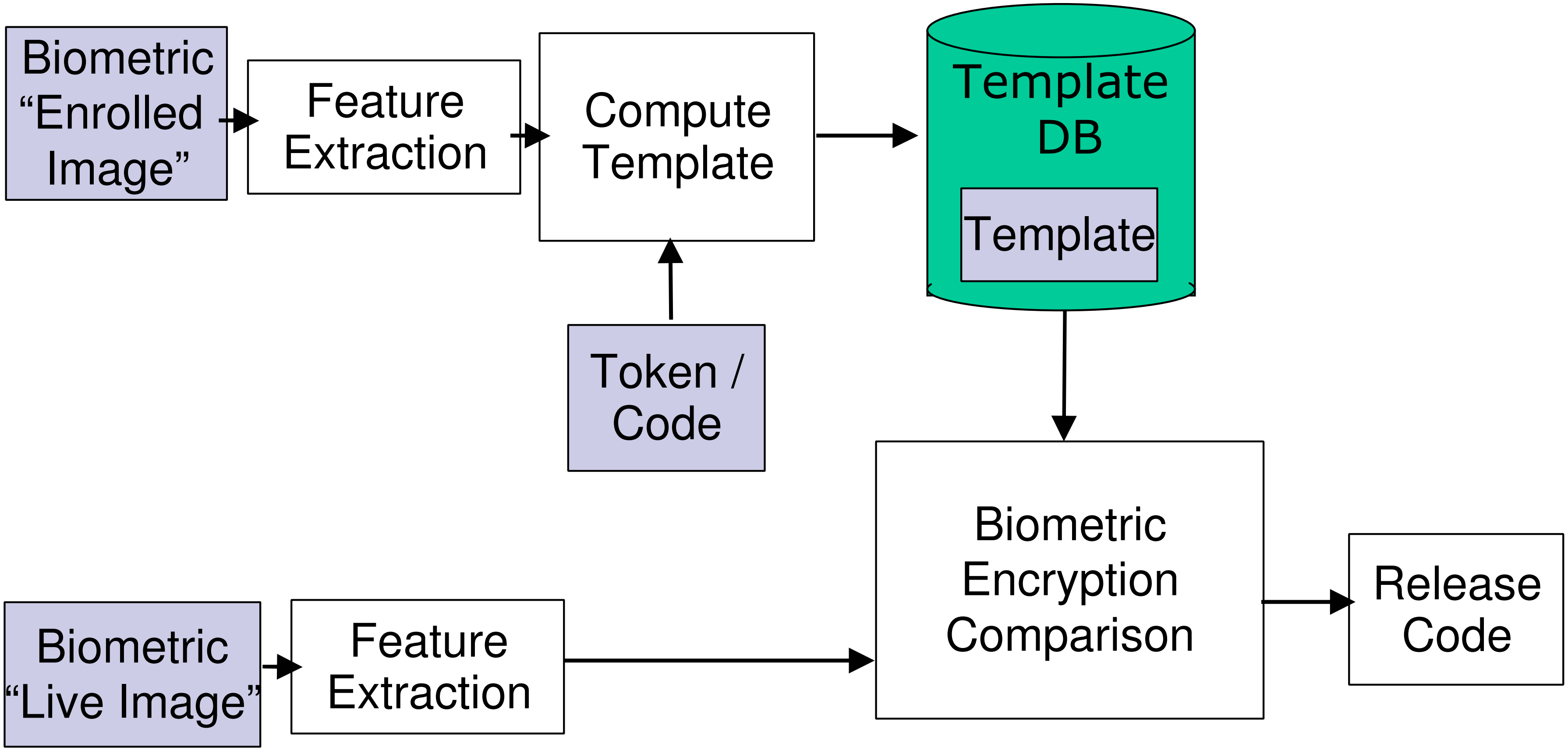


Traditional Biometric Verification

Issues

- Templates and Tokens must be available unencrypted, somewhere
- Crack of biometric system will allow release of Tokens
- Biometric cannot be directly used as a password replacement
- Privacy Issue: system admin will have access to biometric templates

Biometric Encryption Systems



Biometric Encryption Systems

Advantages

- Token is bound to biometric
- Neither template nor token are available unencrypted
- Improved Privacy and Security

Disadvantages

- Biometric Feature variability
- Reduced FAR/FRR performance

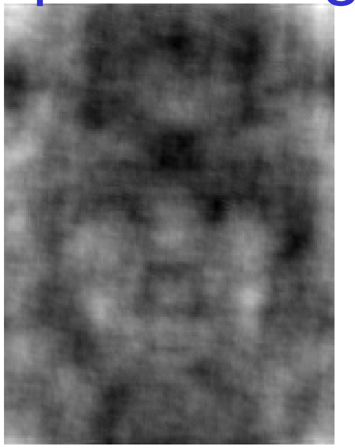
Algorithm: Soutar et al. (1998)

Original algorithm for fingerprints (modified for face)

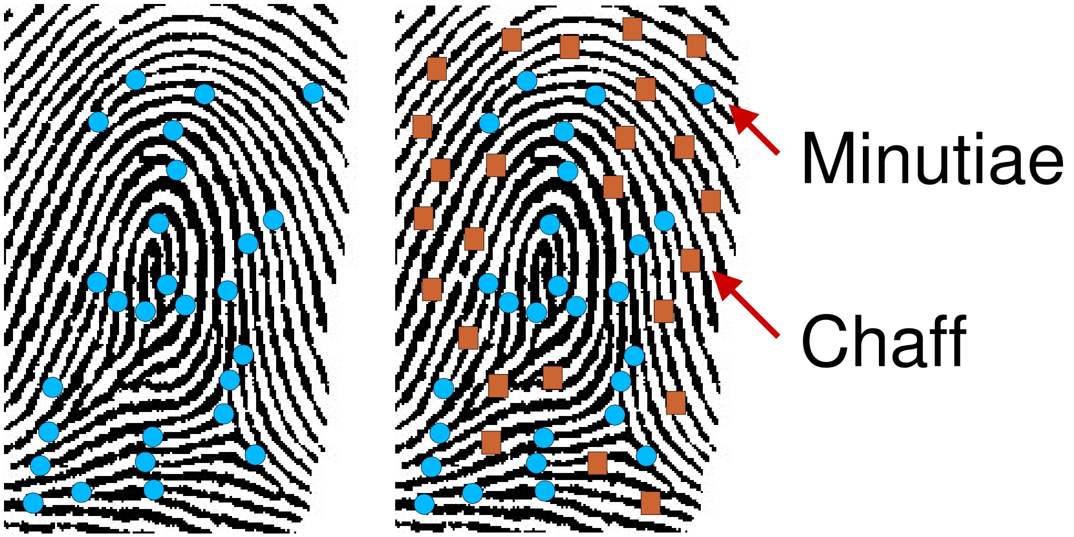
- Average pre-aligned enrolled image (f_0)
- Calculate template from Wiener filter
  $$H_0 = F^* R_0^* / (F^* F + N^2)$$
  where R_0 has phase ±π/2, ampl = 1
- Each bit of secret is linked to several bits of H_0 with same phase

Enrolled Image

Template Image



Algorithm: Clancy et al.(2003)



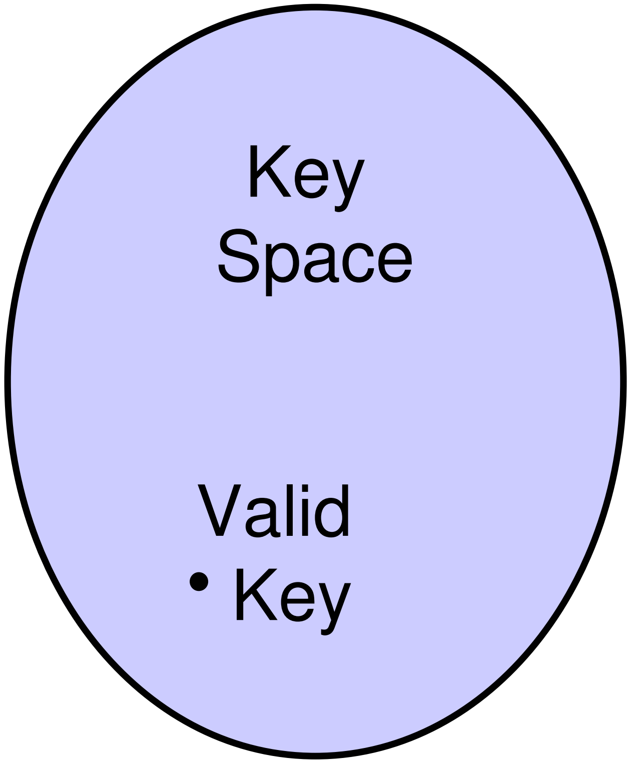
Enrollment

- Add ‘chaff’ to minutiae in template
- Encode token using Fuzzy Vault Scheme

Decryption

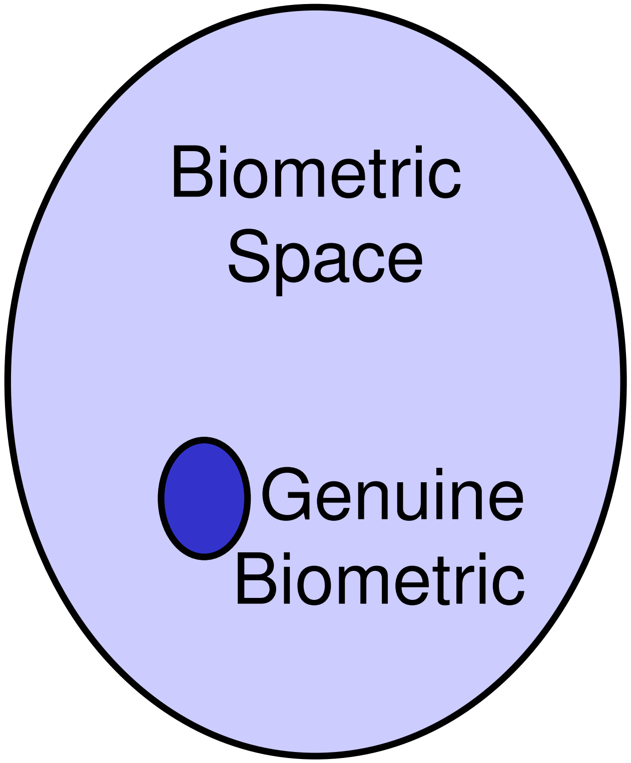
- Using live fingerprint, estimate correct minutiae
- Given enough correct minutiae (and few chaff), Fuzzy Vault will decrypt token

Traditional Encryption



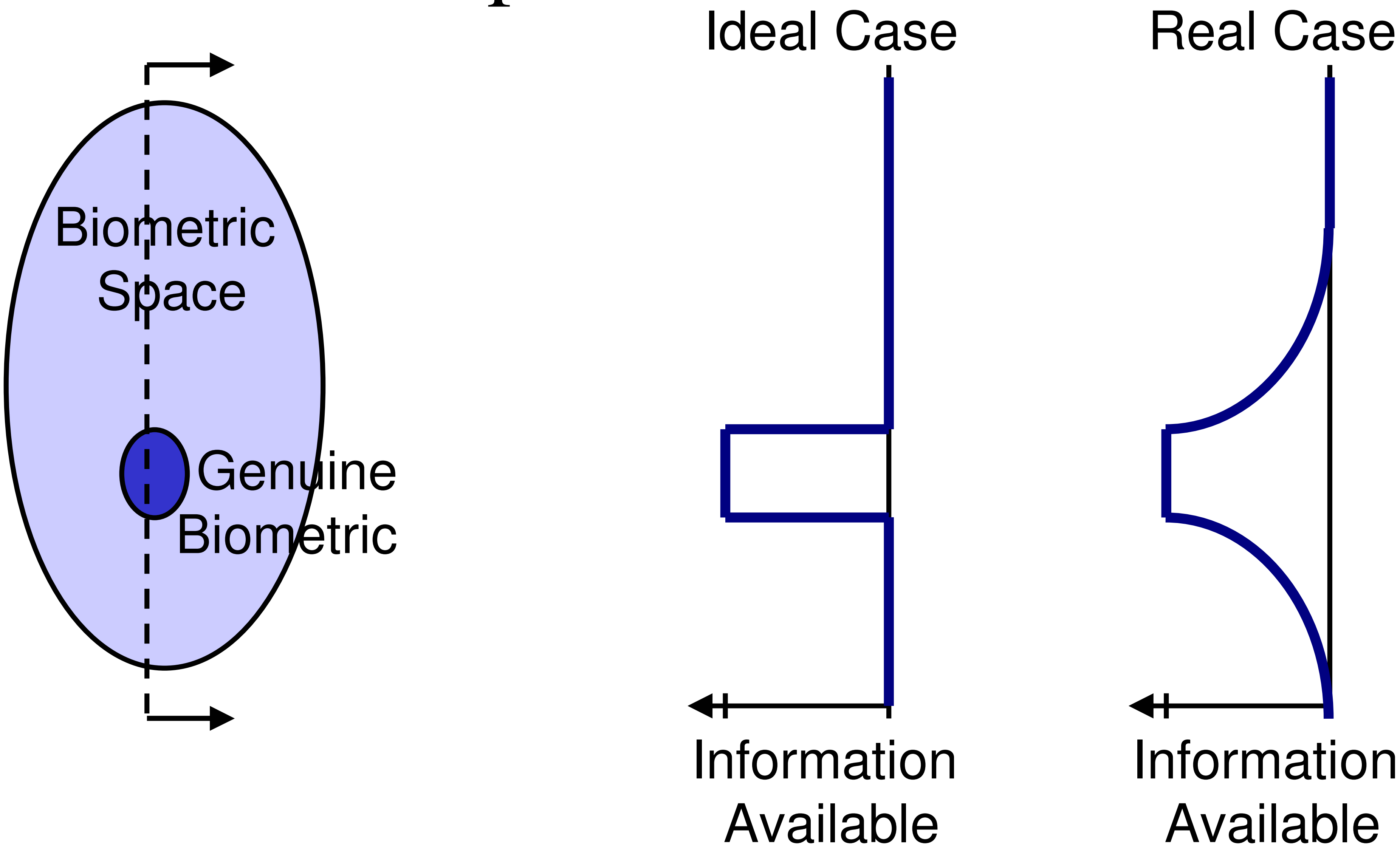
Valid Key is a single point in Key Space

Biometric Encryption



Genuine Biometric is a region is Biometric Space

Biometric encryption: Attack concept



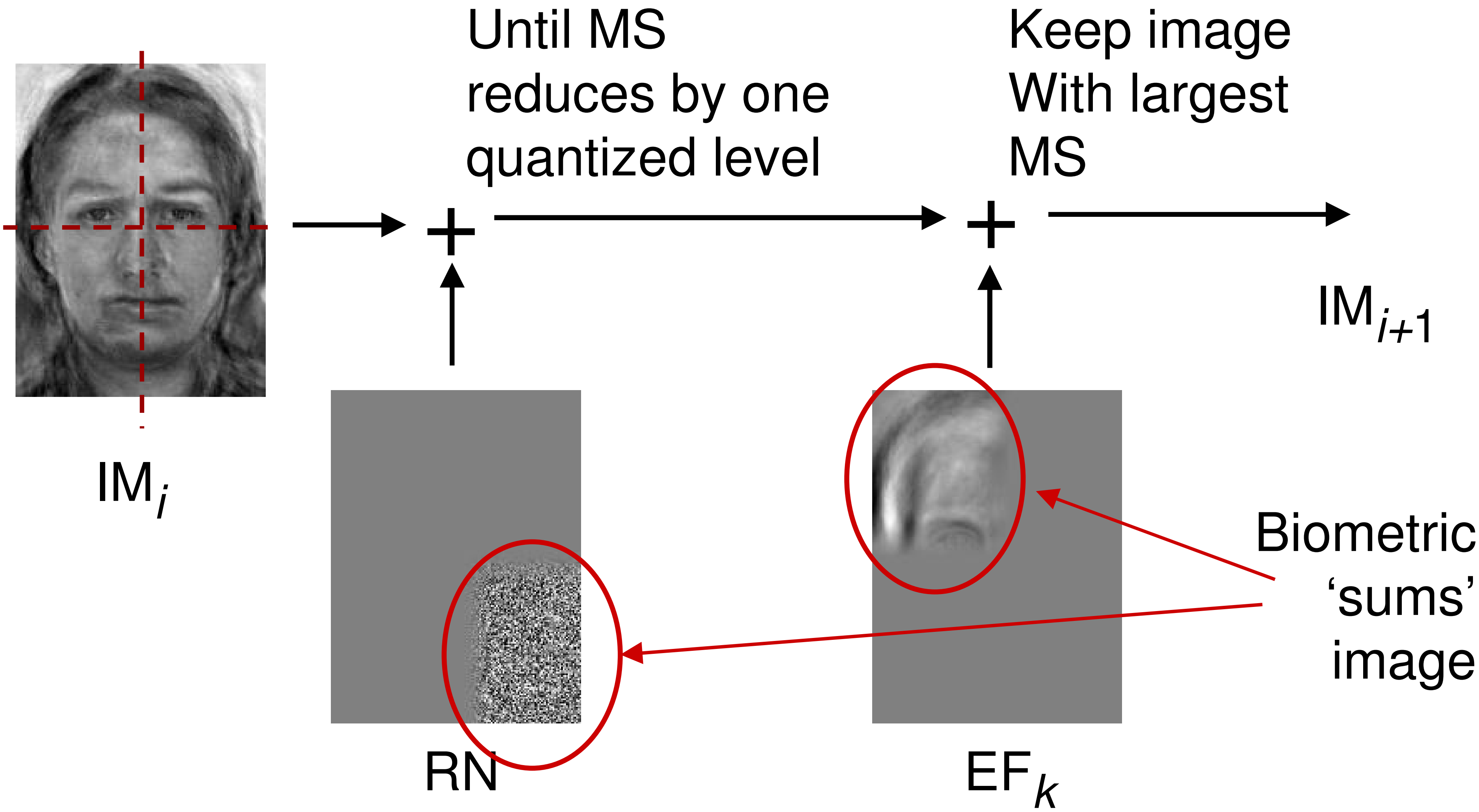
Hill-Climbing

- If biometric comparison releases information on partial match, then “Hill-climbing” is possible
- Concept (iterate over steps):
  - Take a step (ie. Modify Biometric Image)
  - If step climbs hill (more info) stay there
  - If step goes down (less info) step back

Why sloping sides to match curve?

- Very difficult to design ideal algorithm
  - □ Since images vary
    Enrolled image + Δ => release key
  - □ However
    Enrolled image + Δ + ε => no release
- Current schemes based on Error Correcting Codes (ECC's)
  - □ Hamming Distances (Soutar et al.)
  - □ Reed-Solomon ECC (Clancy et al.)
- ECC's inherently give a measure of the distance to the nearest code point -> which is a *match score*

Hill-climbing for quantized data



Until MS
reduces by one
quantized level

Keep image
With largest
MS

IM_i

IM_{i+1}

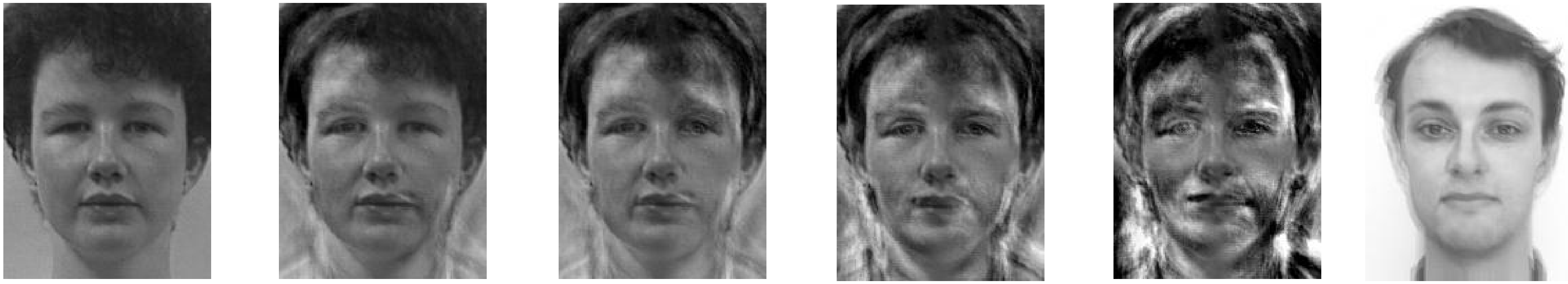
RN

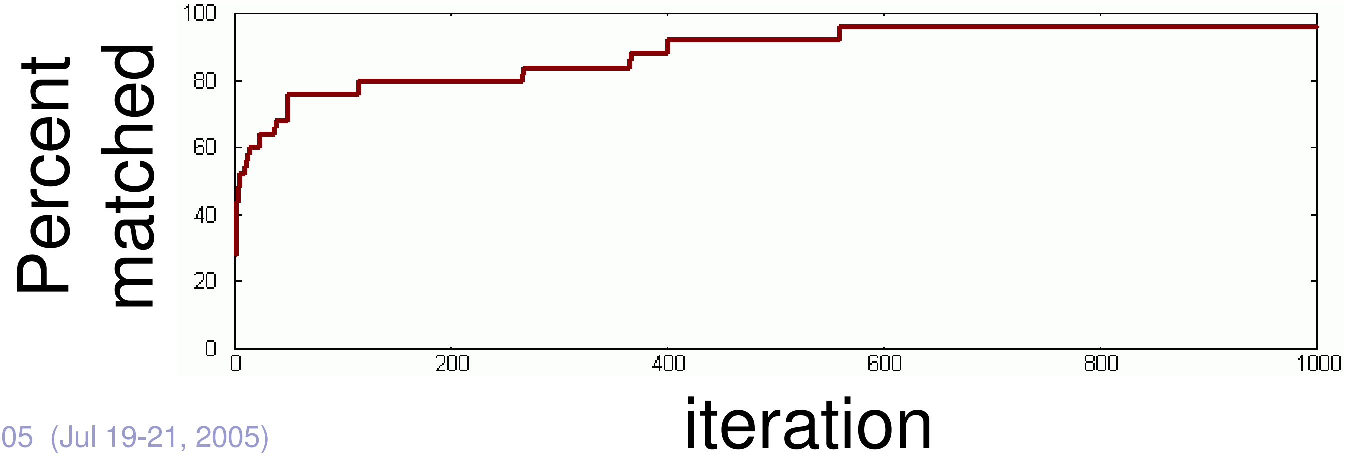
EF_k

Biometric
'sums'
image

Example attack: algorithm of Soutar et al. (Modified for face)

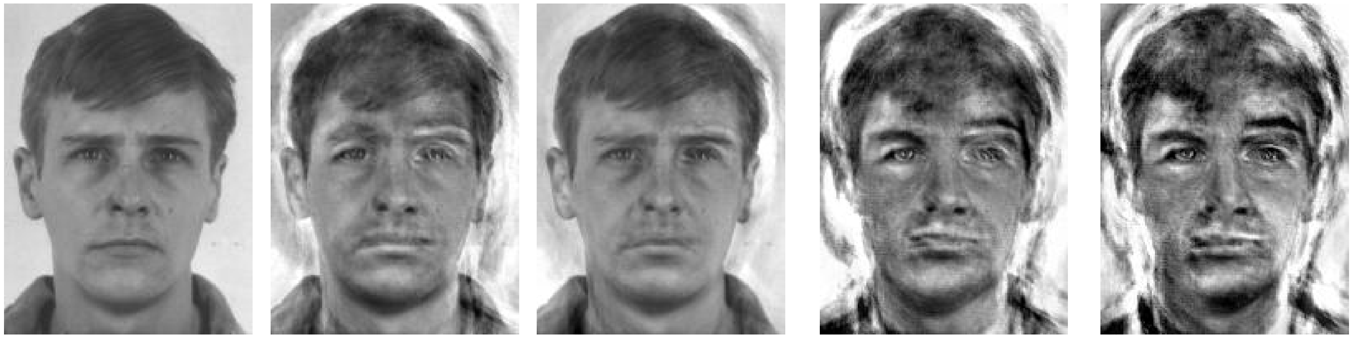
- Construct *match-score* from number of matching elements in *link table*
- Use quantized hill climber



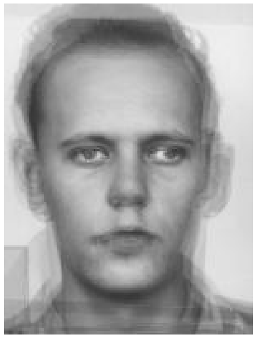


Results

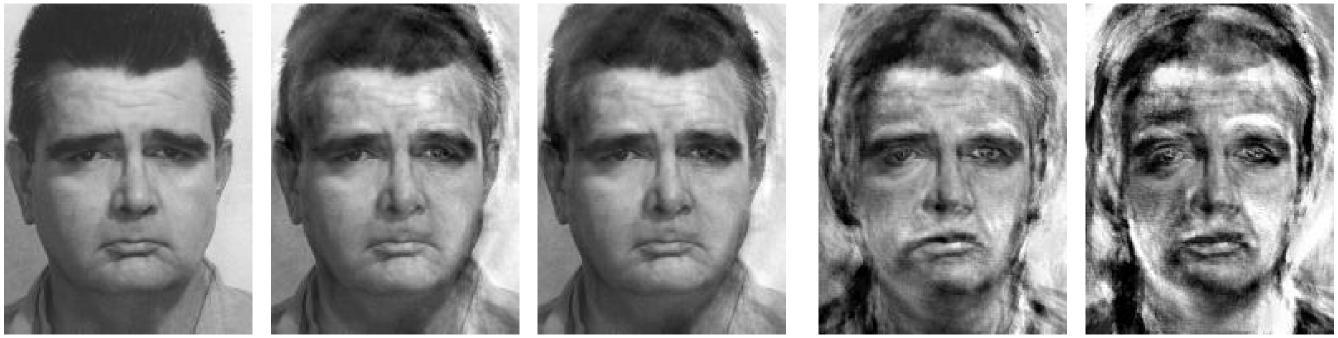
Initial Image #1



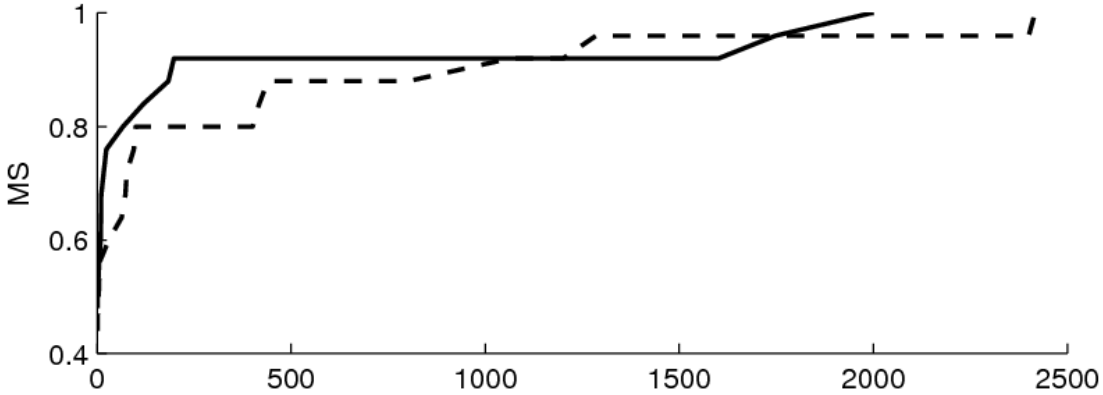
Enrolled Image



Initial Image #2



Match Score versus Iteration Number



Summary

- Biometric Encryption schemes show significant promise to address security and privacy issues
- Little work has been done to attack these schemes
- This paper shows one general attack scheme based on Hill-Climbing

- 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