Biometric Security

Biometric Authentication

Biometric Applications
- Access control
- Biometric ID (e.g., e-passports)
- Password-like authentication
- Data protection
- Laptops, USB thumb drives
- Secure online transactions
- Online purchases, e-voting
- Law enforcement
- Identification
- Activity tracing

Biometric authentication is attractive
- Closely related to the identity
- Cannot be forgotten
- Not easy to forge
- Have been successfully used for a long time

Challenges
- The main challenge is the biometric templates
- Once compromised, it will be
- Easy for attackers to forge identity
- Difficult to revoke or replace
- Biometric data is noisy
- Due to sensor, feature extraction algorithm, environment, etc.
- Extremely difficult to model both the data and noise
- Conventional hash functions not applicable
- Encryption won’t help much either
- Clear template is needed for matching
- Where to store the key?
- Entropy may not be sufficient

Common Techniques
- Error Correction Codes (ECC)
- Common method for generation of helper data
- Model noise between enrollment biometric and the biometric to be verified
- Estimation / reconstruction via conventional channel decoding techniques
- Quantization
- Security gained from entropy loss (uncertainty) invoked during quantization process
- Quantization error could be used as helper data, i.e., as part of the reconstruction process
- Quantization process also eliminates noise in input signal
- Randomization
- Easy to revoke
- Increase between-class separation
- Requires user-specific randomness

Two Main Approaches

Transformation
- Empty one-way transformation
- E.g., quantization, thresholding
- Properties
- Non-invertible, robust to attacks
- Similarity preserving
- Cancelable
- Technique depends highly on the biometric considered
- Security not easy to analyze

Helper Data
- Compute user-specific helper data
- E.g., syndrome, secure sketch
- Helper data and generation method are public
- General framework that is applicable to many biometrics
- Techniques may vary to optimize performance for each biometric
- Security analysis based on information-theory is possible

Transformation Architecture

Helper Data Architecture

Our approaches:

1- Quantization-based Secure Sketch

Main results
- For any well-formed quantizer family, we can always bound the relative entropy loss
- Well-formed: no quantizer in the family loses too much information (say, having too large a quantization step)
- Safest: relative entropy loss is the smallest
- This result is consistent with intuition
- Useful to guide practical designs

2- Robust One-way Transformations

Main results
- Performance
- Zero EER for two-case scenario (EER is where FRR=FAR)
- Performance is as good as the case where only features are used for the worst case scenario
- Scalability (no need for re-training for user addition/deletion)
- Careful design hides the original data efficiently
- Revocable when user-specific information is compromised

3- Geometric Transformation for Fingerprints

Main results
- Performance
- Very compact
- Requires alignment or pairing
- Combination of two noises:
  - White noise: small perturbation
  - Replacement noise: removal/addition

Research Opportunities

- Requires efforts from multiple disciplines
- Performance improvement
- For continuous data, how to find the optimal quantizer in practice?
- Preprocessing
- Multi-biometrics - How to combine the strengths of different biometrics?
- Multi-factor
- Standardization

More on the topic
