

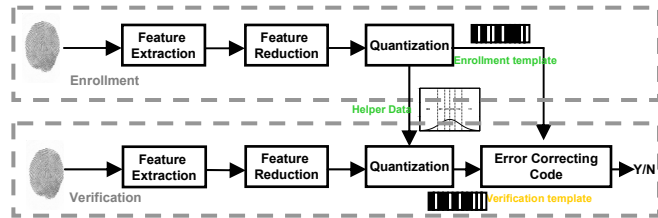
Privacy Protection of Minutia-Based Fingerprint Templates

Haiyun Xu¹, Chun Chen¹
Raymond Veldhuis¹, Ton Akkermans², Tom Kevenaar²
¹University of Twente, ²Philips Research

Introduction

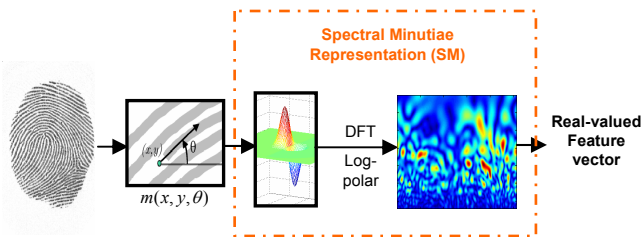
Storing biometric templates in a large number of applications introduces the following *privacy problems*

- Identity theft
- Biometric templates cannot be re-issued
- Cross-matching between databases
- Medical information leakage from template
- Legislation prevents central databases



Feature Extraction for Template Protection

- Fixed-length feature vectors
- Translation, rotation, scaling invariant
- Robust and discriminating feature vectors

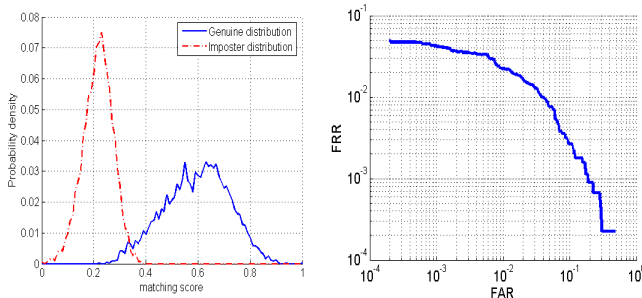


$$m(x, y, \theta) \rightarrow j(w_x \cos \theta + w_y \sin \theta) \cdot \exp(-j(w_x x + w_y y))$$

Results

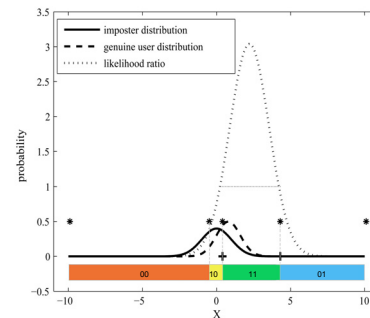
- Database: MCYT
- 100 identities x 10 samples

Minutiae sets	EER	FAR & FRR
Manual minutiae	0.20%	FAR = 0 at FRR = 1.37%
Automatic minutiae	1.84%	FAR = 10 ⁻³ at FRR = 4.31%



Results from MCYT (minutiae extractor: Sagem)

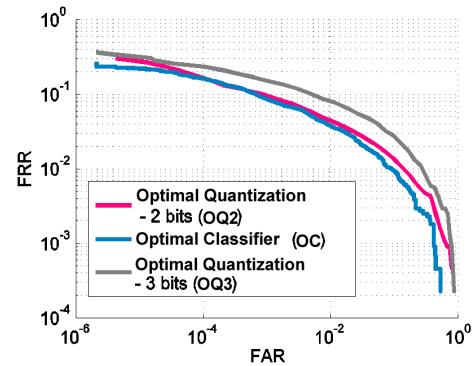
Optimal Quantization



Properties:

- PCA/LDA process enables independent features
- Multi-bits quantization per feature
- ECC functions as Hamming distance classifier
- Equal probability per bit enables independent bits

Classification Results



	FAR=10 ⁻²		FAR=10 ⁻³		FAR=10 ⁻⁴	
	FRR	D	FRR	D	FRR	D
OC	3.8%	N/A	8.7%	N/A	16.2%	N/A
OQ2	4.3%	37	8.7%	33	16.7%	29