

Secure Matching of Fingerprint Representations Using Smart Chip Devices

James G. Reisman

Siemens Corporate Research, Inc

Princeton, NJ

james.reisman@scr.siemens.com

INVESTIGATION

Can biometric template information be secured from identity theft without sacrificing matching performance?

Why?

- Biometric templates need to be safeguarded against identity theft, and against invasions of privacy.
- Compromised biometric templates can be used in spoofing attacks to access private information.

How?

- A secure method of storing and matching biometric information stored on a smart chip device is used.

SECURE MATCHING METHOD

Scanning Unit

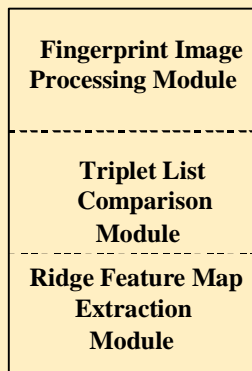


Smart Card

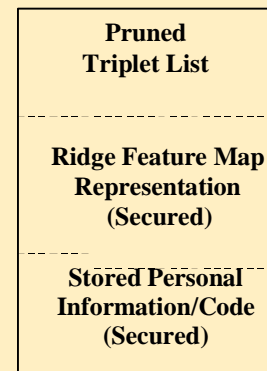


1. Pruned Triplet list (w/o $\langle x,y \rangle$ info)
2. List of matching triplets hits
3. Image Translation Value
4. Aligned Template
5. Released Info/Code

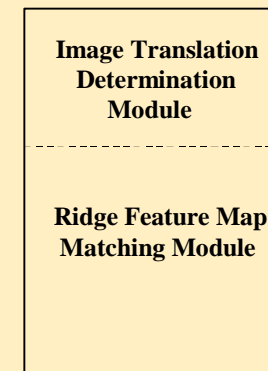
Embedded System
Modules



On-Card Data

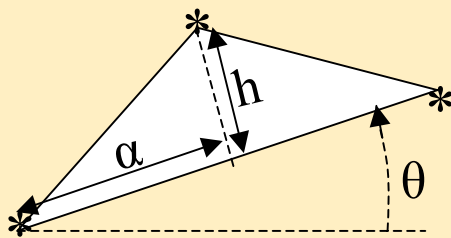


On-Card Modules



FEATURE REPRESENTATIONS

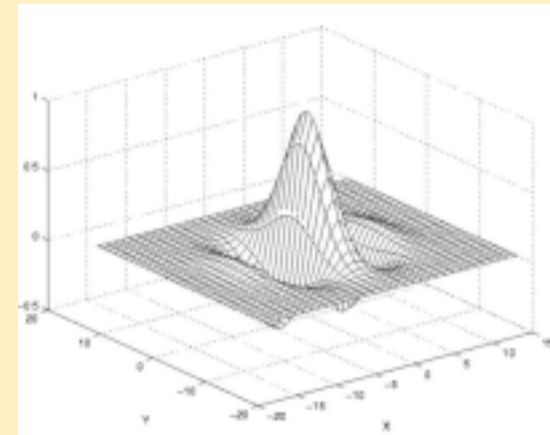
Minutiae Triplet List (Alignment Feature)



Legend

- *: minutia location
- h: height of perpendicular
- θ : angle deflection
- α : bisected fraction

Ridge Feature Map (Secured Matching Feature)



RESULTS

- Performance is similar to more computationally demanding unsecured fingerprint matchers.
- Computational requirements are within the boundaries of a smart card chip specifications.

CONCLUSION

- **It is possible to perform accurate fingerprint matching without sacrificing performance, and without risking the compromise of biometric information.**