Secure Iris Recognition

Christine Lu, Pennsylvania State University
Avinash Varna, University of Maryland
Dr. Min Wu, University of Maryland
Why Iris Recognition?

- Convenient
- Permanent, intricate
- Responsive to light
- Impossible to surgically modify without unacceptable risk to vision
• Tolerate small changes
• Cannot directly hash iris code
• Goal: authenticate users based on hashed code
XOR-ECC Method

\[ \text{ecc}(\text{key}) \oplus \text{iris1} \oplus \text{iris2} \]

- Tested with various methods of error correction
Results

• 3 irises stored in the database for one person: $1-0.4^3 = 94\%$ chance of being correctly accepted.

Current key sizes: (bits)
- Repetition: 100
- Hadamard: 200
- Hadamard & Reed Solomon: 200
Random Projections

\[ f \cdot R \]

- Reduce dimensionality, preserve distance.
- Take irisCode1 (dot) R – irisCode2(dot)R, and evaluate the difference. As long as it is below some number, treat it as a match. Otherwise, reject.
- 31 times faster than XOR-ECC
- Less accurate
- Compared different methods of secure hashing when applied to iris recognition

- Tested random projection: faster but less accurate.

- Looked at different methods of error correction for XOR-ECC method
• National Science Foundation CISE award #0755224
• Merit
• Dr. Min Wu
• Avinash Varna