CERIAS Tech Report 2007-13

EQUATING BIOMETRIC ENTROPY

by Young, M. R.

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Biometrics in E-Authentic
Equating Biometric Entr

Graduate

Biometric Cons

Se

Biometric Standards, Performance, and Assurance Laboratory

PIN Compared to FAR

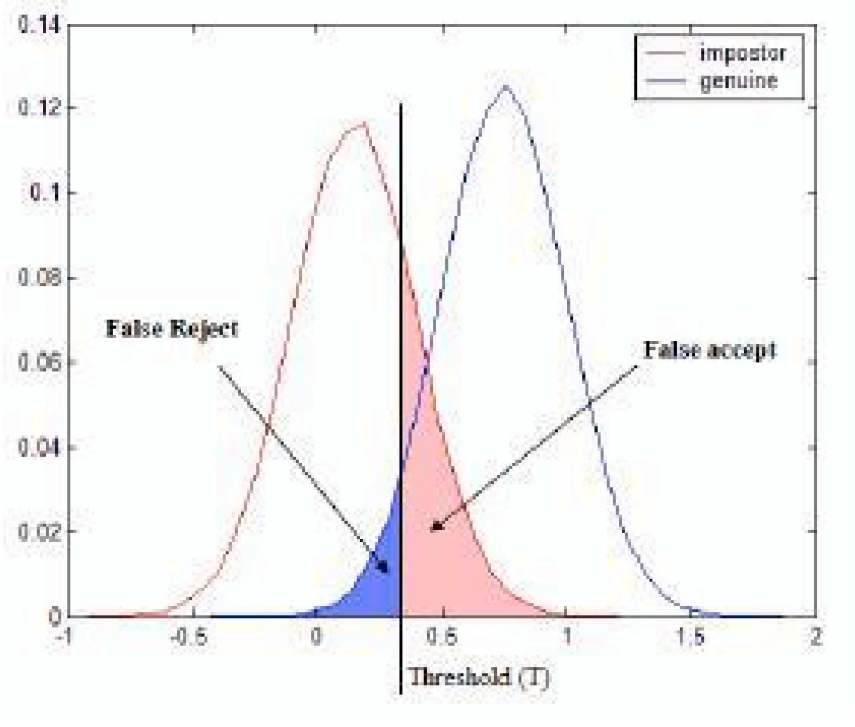
- Common assumption to equate entropy of a
  False Accept Rate (FAR) of a biometric syst
- Biometric FAR: 0.01% = 1 in 10,000 chance
  "guessing" or False Accept.
- PIN: Four digit PIN = (10x10x10x10), 1 in 1
  chance of "guessing" the PIN.
- Are these the same?...not exactly

1. Brute force on PINs focused on a SINGLE P
biometric system includes ALL samples.

- Just as some secrets are harder to guess
so too are biometric templates to be matc
(Doddington, G., et al.).

Doddington, G., et al. *Sheep, Goats, Lambs and Wolves. An Analysis of Individual Differences in*
Performance. in *International Conference on Spoken Language Processing*. 1998. Sydney, Austr

2. FARs are NOT a static value for biometric sy
   - Variable thresholds in biometric matching between FAR and FRR to suit application

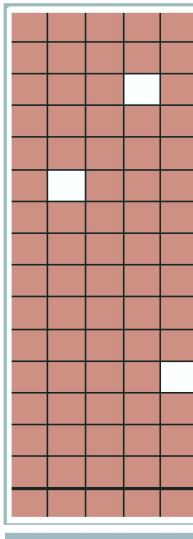


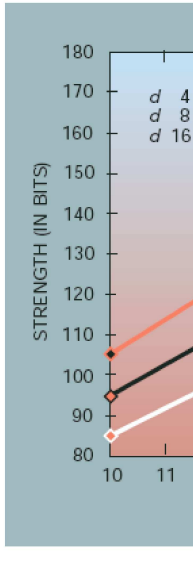
3. Entropy of secrets is directly tied to keyspac

- Assumption does not use keyspace for de entropy of biometrics.
- Entropy of biometrics must be measured u in order to be an equal comparison.
- How many individual representations are biometric systems?

Defining Keyspace of Fingerprint Image

- Ratha, N., et al. considers:
- Dimensions of the image (pixels)
- # of pixels a minutiae point consumes.
- Orientation angles of minutiae.
- # of minutiae required to be matched.
- 25 minutiae matched = 82 bits of information.
- Equal to 16-character nonsense password “m4yus78xpmks3bc9”.



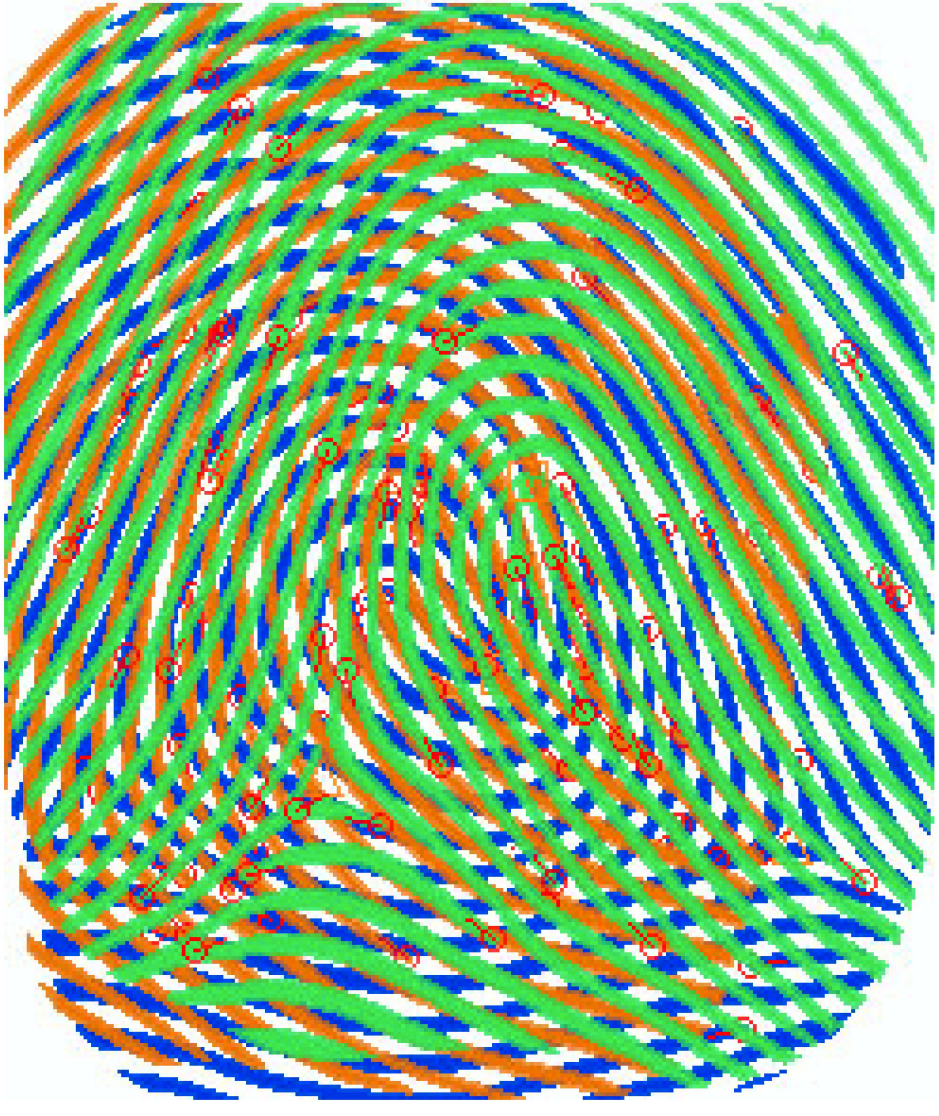


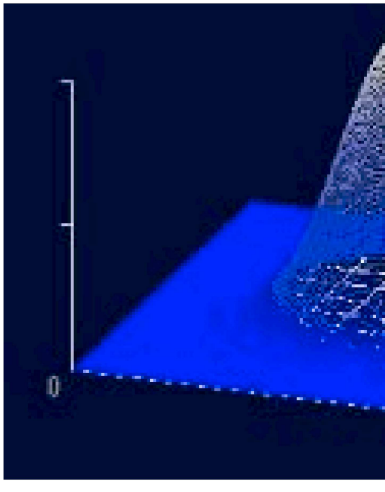
Ratha, N., J. Connell, and R. Bolle, *Enhancing security and privacy in biometrics-based authentication systems.* IBM Systems Journal, 2001. 40(3).

Proposed Methodology

- Build on the work done by Ratha, et al.
- Factor in probabilities of minutiae appearin possible location using 3-D model.
- Incorporate the principles of Shannon's In Theory and determination of entropy.

Proposed Methodology





$$H(X) = \sum_{x}^{n} p(X) \log_2 \left(\frac{1}{p(X)} \right)$$

- Where:
- *n* = total # of possible locations for minutiae in the image.
- *p(X)* = the probability of minutiae occurring at each individual location.
- *H(X)* = Entropy in bits

- Example in regions:

0.00
0.50

$$H(X) = (.50)\log_2(2) + 2((.25)\log_2(4)) = 0$$

Shannon, C.E., *Communication Theory of Secrecy Systems.* Bell Systems Technology, 1949. 28(October): p. 656-715.

Thank You!

Matthew Young
mryoung@purdue.edu
Graduate Research Assistant
Purdue University
Biometric Standards, Performance and Assurance La
www.biotown.purdue.edu
401 N. Grant St.
West Lafayette, IN 47906