Biometrics and Privacy Issues

Problems and Promises

Security vs. Privacy

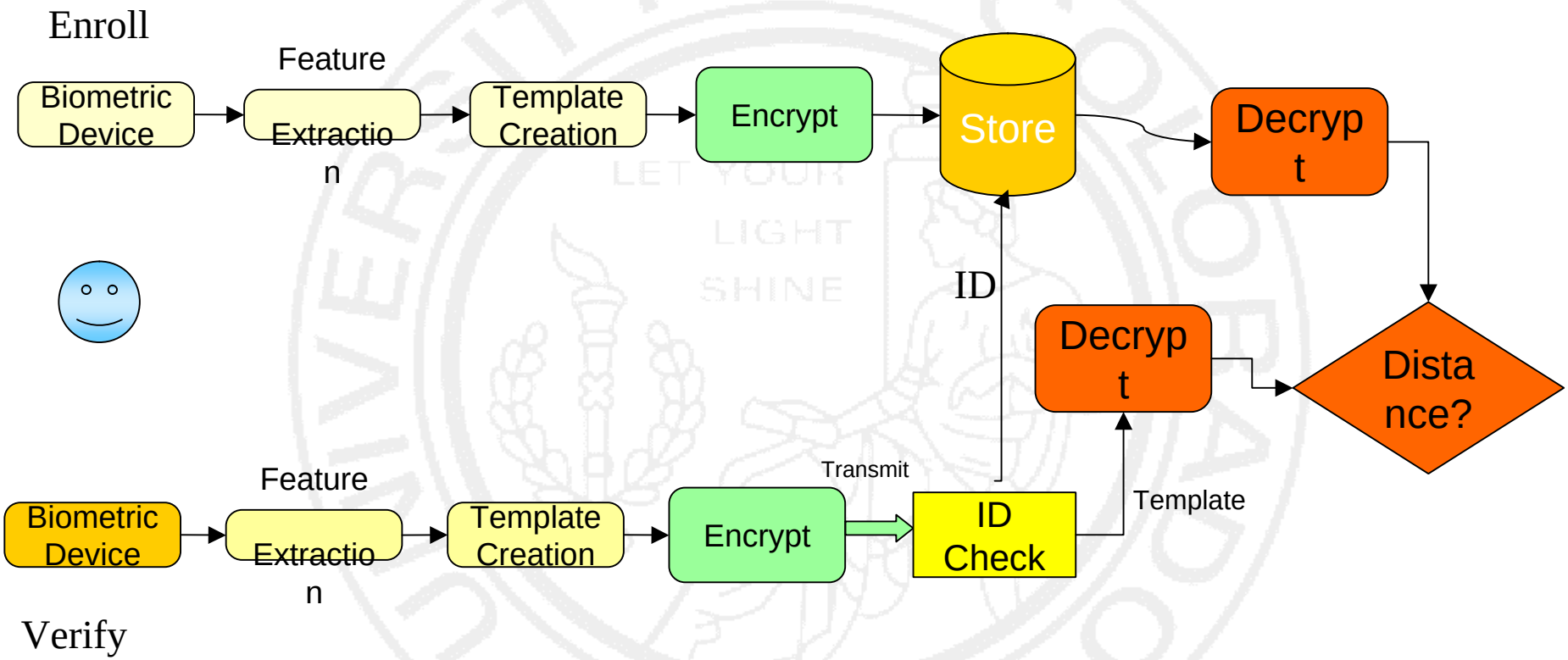
- Accountable to Management
- Risk based assessment. (how likely is it?)
- Access and use controls ***defined by the system owner.***
- Focused on protecting against outsiders.

Encryption Helps
When is it decrypted?

- Accountable to the person.
- Capabilities based assessment. (is it possible?)
- Access and use controls defined by ***use limitation and consent of subject, and legislation.***
- Protecting against outsiders, insiders and system owner.

Who has the keys?
When is it decrypted?

Traditional Encrypted Biometric Privacy Vulnerabilities "Levels"



Revocable Biometrics?

The Key Issue with Biometrics

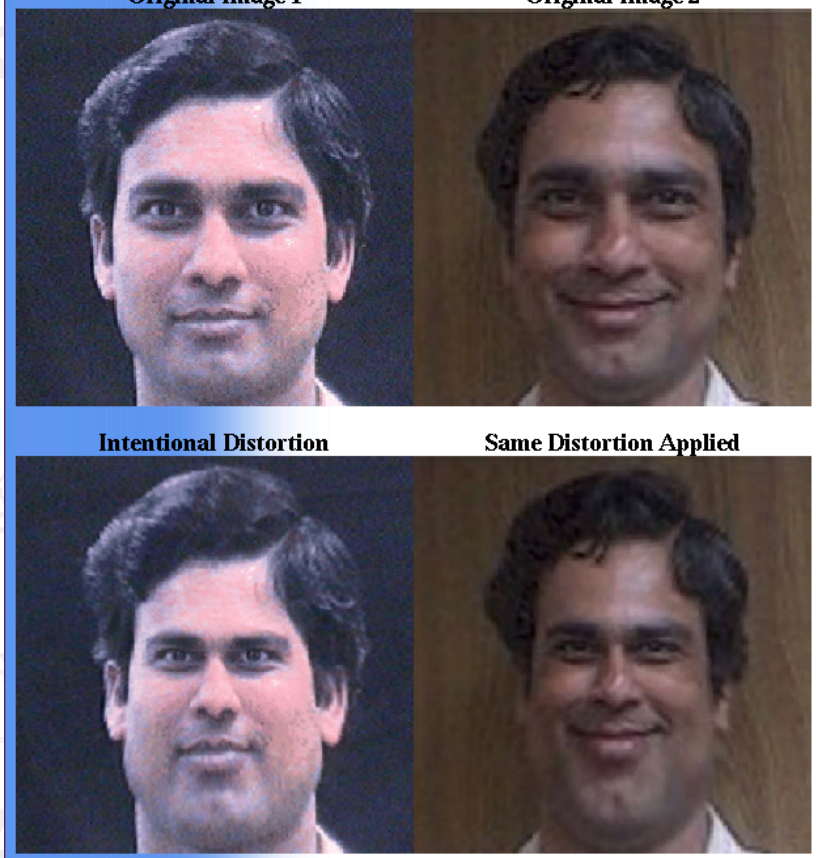
- **The biggest problem with biometrics**
  - If someone steals a token, IT issues a replacement
  - If someone gets your private key, you can revoke the matching certificate and make that key useless
    - A new certificate is created with the new public key
- **What do you do when someone steals your template or spoofs your biometric?**
  - The concept of a revocable credential does not exist in single-factor biometric solutions

RSA SECURITY

From talk by
Chris Miller
RSA security Feb 2002

Early Revocable or Cancelable Biometrics

- IBM's work: Distortion or mixed image:
  - Invertible given transform
  - Distorts "distance"
  - Can be used for "identification"
  + Cancel by changing transform
  + Different transforms for different applications

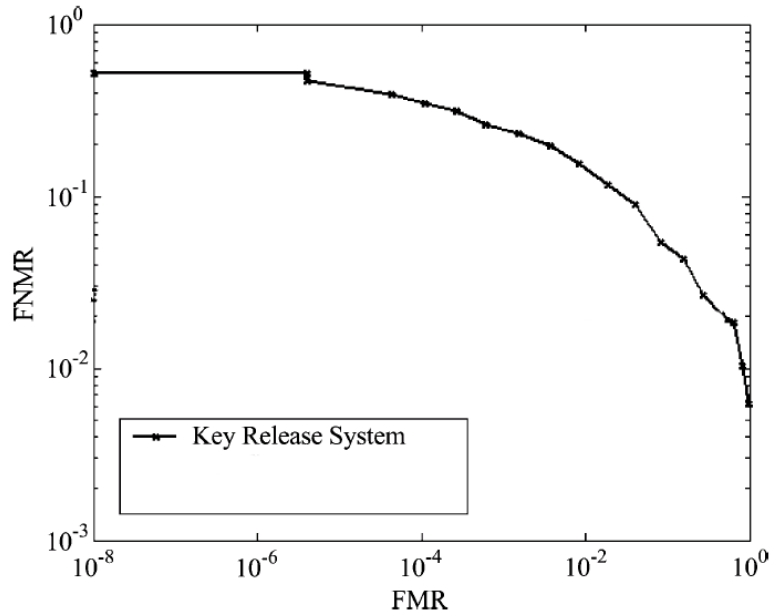


Selected publications:

Enhancing security and privacy in biometrics-based authentication systems
N. Ratha, J. Connell, R. Bolle
IBM Systems Journal, vol. 40, no. 3, 2001, pp. 614-634.

Revocable "hashes" A.k.a. Biometric "keys"

- Hash biometric data to form identity key.
  - Cannot compute "distance" hence need exact match which means it must truncate biometric data to "stable" region
  - Must add forward error correction to address errors/lost features.
  - Truncation increases FMR and FNMR
  - FMR/FNMR tradeoff fixed by hash, cannot vary by application or site



Adapted from Uludag-et-al Proc. of IEEE 2004

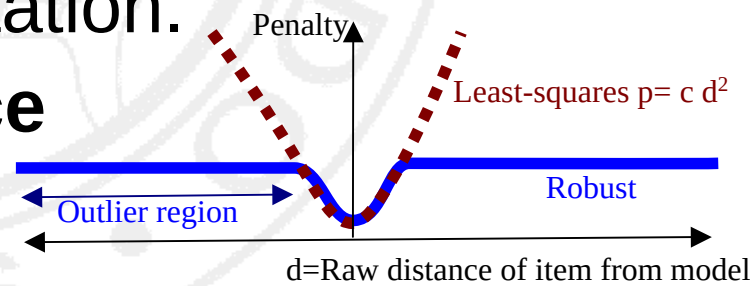
Biometric key "conclusions"

"While researchers have proposed many interesting and clever ideas of generation or binding of biometric keys, we believe many critical problems peculiar to the biometric domain have not been satisfactorily solved."

- Ulugdag, Pankanti, Prabhakar & Jain, Proc. of IEEE, June 2004.

Revocable biometrics with robust distance measure

- Revocable and supports different non-linkable transforms for different applications (i.e. private)
- Not invertible, even given transform parameters
- Variations using incorporating passcode and/or smart-card can be configured to support verification without supporting identification.
- Includes both a “Hash” and other fields that are needed for distance computation.
- **Supports a robust distance measure while encoded!**
- Practical to implement :-)



"Don't be too quick to strike a balance between privacy and security. As Americans, we are entitled to a full measure of both”

- Admiral James Loy, Head, Transportation Security Agency USA, 9th Annual Privacy & American Business Conference, March 2003