Comparative Study on Securing Biometrics Data

Brigitte Liu and Melonie Hardy / Advised by: Dr. Min Wu and Wenjun Lu

MERIT FAIR
BIEN 2011

Media & Security Team at UMD
MAST

Motivation

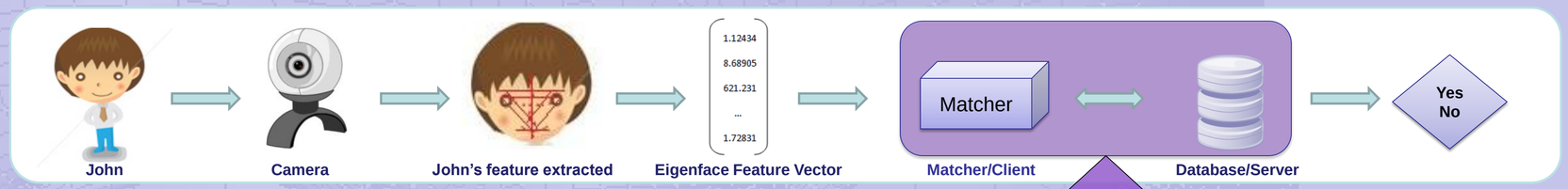
- Biometrics: true measure of identity

vs.

Useful but difficult to replace when compromised

Easy to crack

High Level Overview of System

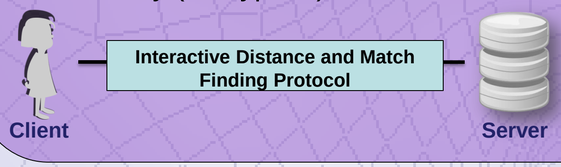


Objectives

- Implement secured biometrics protocols:
  - Homomorphic encryption (HE)
  - Error Correcting Codes (ECC)
  - Random Projections
- Compare methods on:
  - Time complexity & communication bandwidth
  - Matching Accuracy
  - Security-strength offered

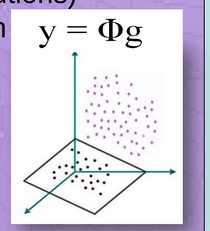
Homomorphic Encryption

- Enables computations on encrypted data
  ex: additive & multiplicative property
- Public key (encryption): Client and Server
  Private key (decryption): Client



Random Projections

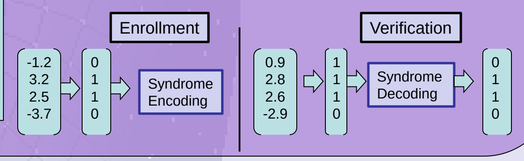
- Φ = random matrix (Gaussian, Bernoulli, or other related distributions)
  g = feature vector of length N
- Use either one Φ for all users or one Φ per user in a system



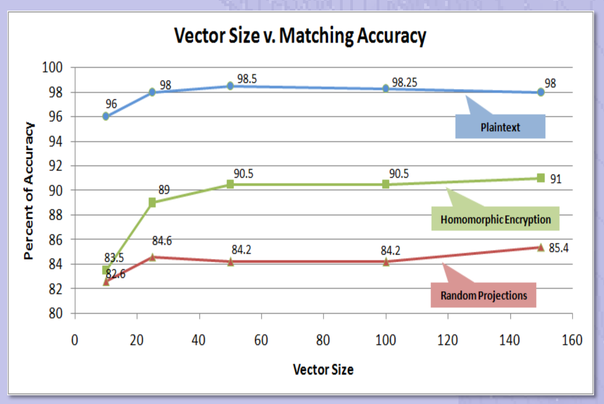
Picture adapted from:
http://www.ait.gr/ait_web_site/faculty/apne/Images/nonLinearlySeparable.jpg

Error Correcting Code

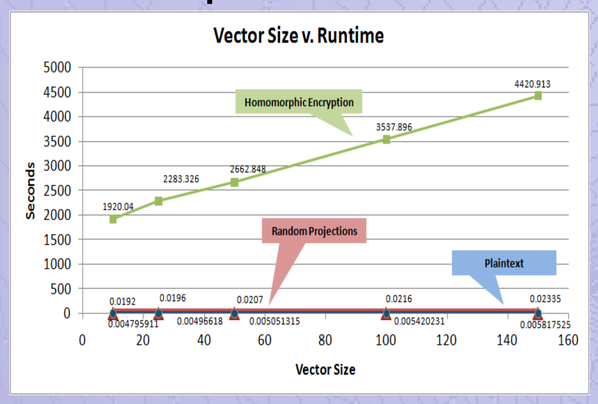
- Correct small inconsistencies between stored &probe vectors (binary)
- Several algorithms such as BCH and LDPC



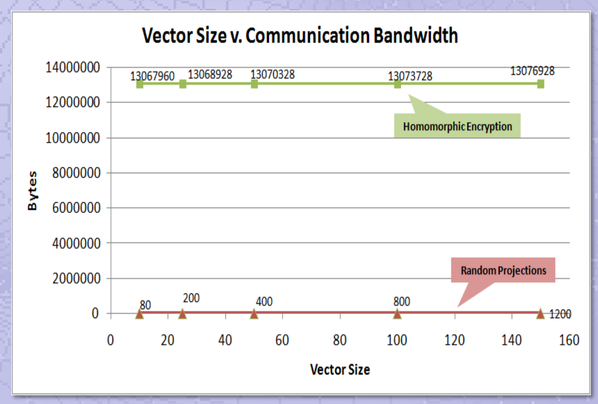
Comparison Results



Homomorphic Encryption is ~5.5% more accurate than Random Projections



Homomorphic Encryption takes ~10^5 seconds longer than Random Projections

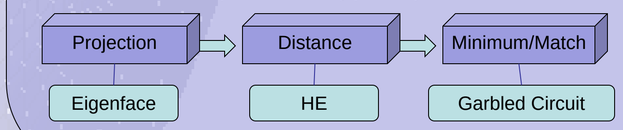


Homomorphic Encryption takes ~10^4 bytes more than Random Projections

What are Protected	Homomorphic Encryption	Random Projections	Error Correcting Code
	(+) Client never sees the data in database Server never sees the ID result & probe vector	(+) Plaintext features not stored in server	(+) Server never sees the plaintext vector and plaintext features
	(-) System compromised when an attacker directly targets the database	(-) Require client/server to hold random projection matrix	(-) System compromised when attacker steals a binary feature vector

Conclusion & Future Work

- HE: high security & accuracy
  Random Projections: ease of use and expediency
- Future Work:
  1. Analyze performance of ECC
  2. Analyze Garbled Circuit (optimization of Homomorphic Encryption)



Acknowledgments

National Science Foundation OCI award #1063035
Advising Mentor : Professor Min Wu
Graduate Student Mentor : Wenjun Lu

Background from: http://blender3d.org.ua/forum/animation/148.html, John's picture from: ID 64025365 (author: notkoo) from shutterstock.com