Comparative Study on Securing Biometrics Data

By: Brigitte Liu and Melonie Hardy
MERIT BIEN SUMMER 2011
University of Maryland, College Park
Motivation & Contribution

Implementation of methods:
1. Homomorphic Encryption & cryptographic protocol
2. Random Projections

Contribution: comparison and trade-off of methods
1. Communication bandwidth
2. Runtime
3. Security strength & Matching accuracy

Applications: Forensics, Identification, etc.

Password: 6

Useful but difficult to replace when compromised

Easy to crack, easy to steal, easy to replace
Points of Attacks

John → Camera → John’s feature extracted

Stealing information shared between server and database

Client/Matcher

Feature vector*

1.12434
8.68905
621.231
...
1.72831

Altering the matching algorithm

Stealing stored templates

Server/Database
Homomorphic Encryption

- Traditional Encryptions: scramble to hide plaintext
- What is special about Homomorphic encryption?
  Enables certain processing/operations of encrypted data

\[ a = 5 \quad b = 7 \quad a + b = 12 \]
\[ [x] = \text{encryption of } x \]
\[ [a] = 5643526 \]
\[ [b] = 7868123 \]
\[ [a][b] = 4433891881698 \]

\[ \text{decryption} \quad 12 \]
Area of Secure communication over an encrypted domain

Alice (Client)

- Alice decrypts the ID

Bob (Server)

- Gives Bob [feature vector]
- Euclidean Distance protocol
- Minimum/Match Finding protocol
- Give [Id] to Alice or 0
Database holds 40 people, 5 pictures/person
Vector Size 150

Example of face variations/person:

Probe vector used is of ID 2
Minimum distance should lie between vector 5-10
HE: Vector Size v. Time

Database Size = 200 (40 people, 5 vectors per ID)
Average time for one query out of 200 queries (runs)

Homomorphic Encryption
Plaintext
Database 200: 40 people, 5 representative variation pictures/person
Database 399: 40 people, 10 representative variation pictures/person
Random Projections

- The core computational method involved in Random Projection is matrix multiplication.

- Gaussian, Bernoulli, or other random distribution matrix

\[ y = \Phi g \]

Picture adapted from: http://www.ait.gr/ait_web_site/faculty/apne/Images/nonLinearilySeparable.jpg
Database 200: 40 people, 5 representative variation pictures/person
Database 200: 40 people, 5 representative variation pictures/person
Vector Size v. Runtime

- **Homomorphic Encryption**
  - Vector Size: 1920
  - Time: 0.019 seconds
  - Time: 0.0048 seconds

- **Random Projections**
  - Vector Size: 2283
  - Time: 0.019 seconds
  - Time: 0.0049 seconds

- **Plaintext**
  - Vector Size: 2662
  - Time: 0.02 seconds
  - Time: 0.0051 seconds

  - Vector Size: 3537
  - Time: 0.022 seconds
  - Time: 0.0054 seconds

  - Vector Size: 4420
  - Time: 0.023 seconds
  - Time: 0.0058 seconds
Vector Size v. Bandwidth

- Homomorphic Encryption
- Random Projections
Homomorphic Encryption: security and accuracy most secure communication method, database in plaintext

Random Projections: easy to use and fast communication is not as secure, database doesn’t store plaintext

Current and Future Work:
1. Implementation & testing of Error Correction Code
2. Implementation of Garbled Circuit – ~40% faster
Acknowledgements

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

Ratha, Connell, & Bolle, 2001, p. 618


Picture from: http://www.shutterstock.com/cat.mhtml?lang=en&search_source=search_form&version=llv1&anyorall=all&safesearch=1&searchterm=boy+and+girl+cartoon+faces&search_group=&orient=&search_cat=&searchtermx=&photographer_name=&people_gender=&people_age=&people_ethnicity=&people_number=&commercial_ok=&color=&show_color_wheel=1#id=64025365