Comparative Study on Securing Biometrics Data

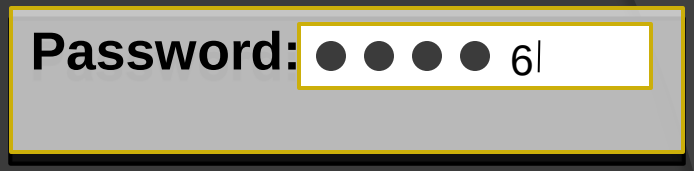
By: Brigitte Liu and Melonie Hardy
MERIT BIEN SUMMER 2011
University of Maryland, College Park

MAST
Media & Security Team at UMD

Motivation & Contribution

- 

vs.

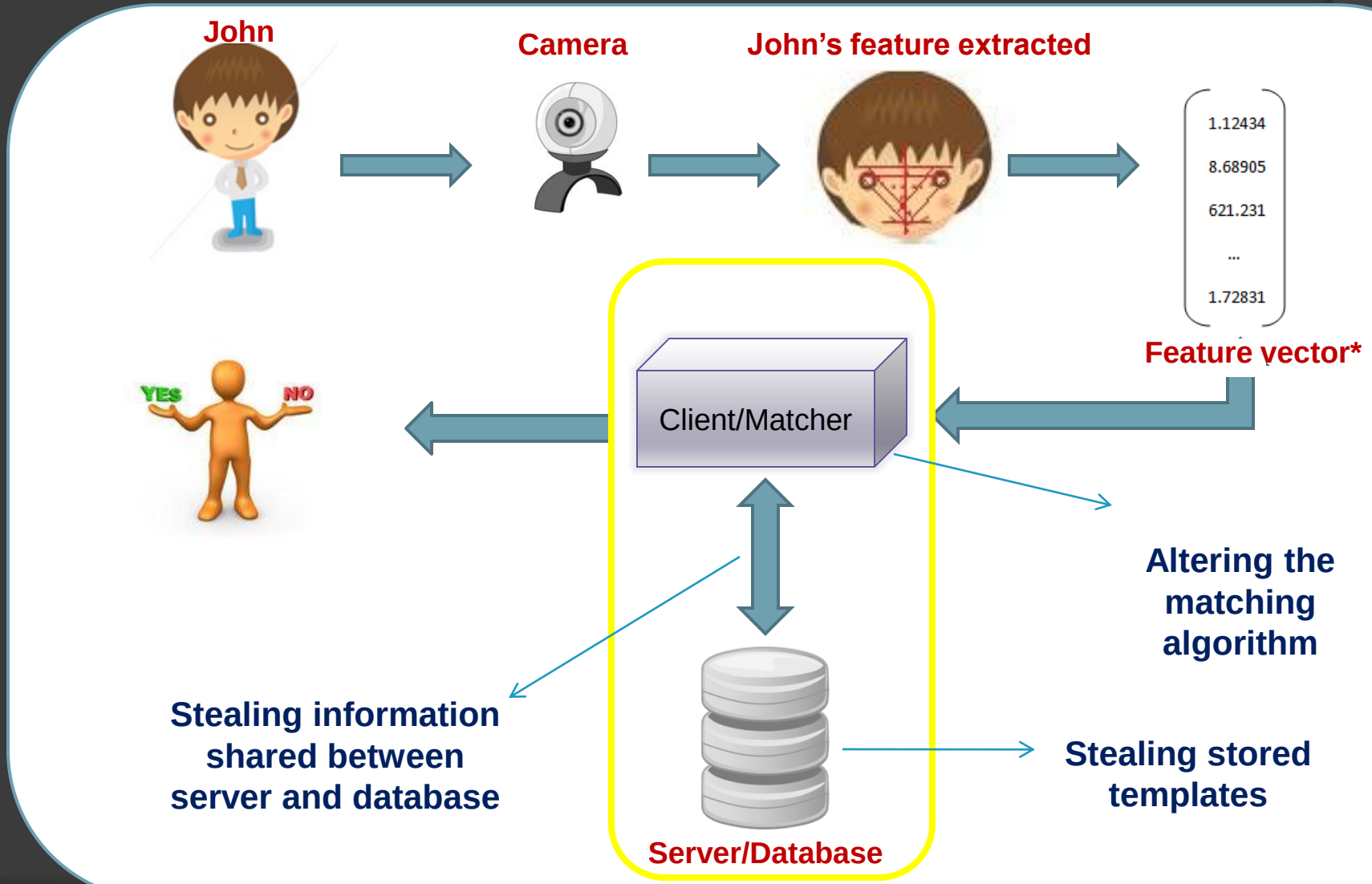


Useful but difficult to replace when compromised

Easy to crack, easy to steal, easy to replace

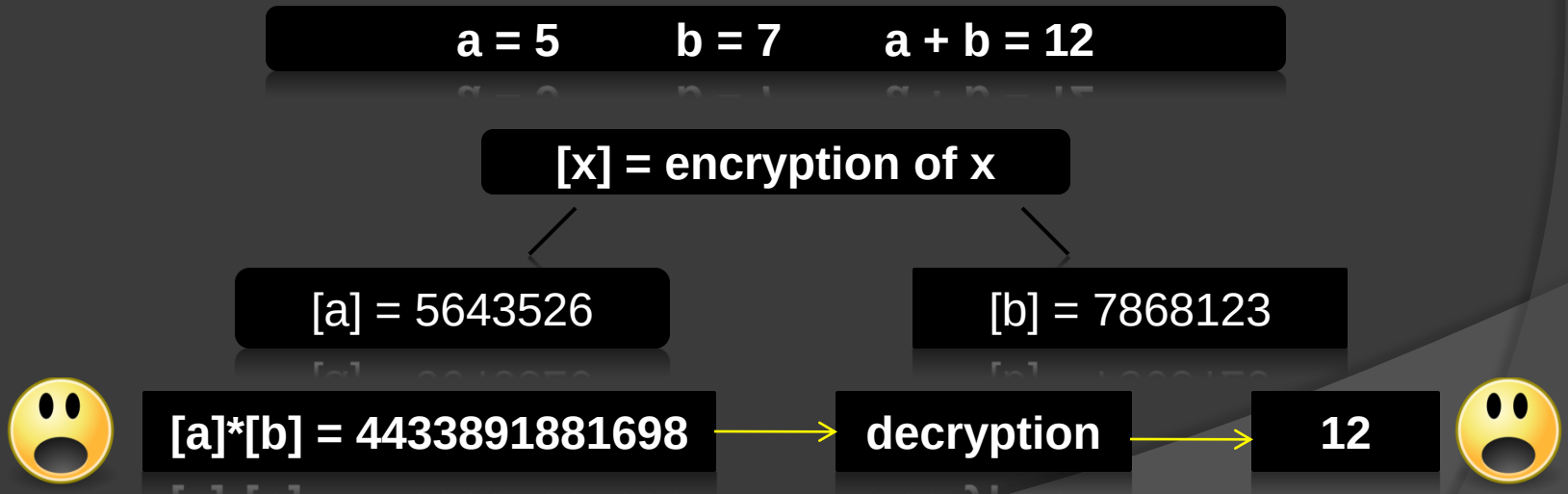
- Implementation of methods:
  1. Homomorphic Encryption & cryptographic protocol
  2. Random Projections
- Contribution: comparison and trade-off of methods
  1. Communication bandwidth
  2. Runtime
  3. Security strength & Matching accuracy
- Applications: Forensics, Identification, etc.

Points of Attacks



Homomorphic Encryption

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



HE- High Level Overview

Alice (Client)

Gives Bob [feature vector]

Euclidean Distance protocol

Minimum/Match Finding protocol

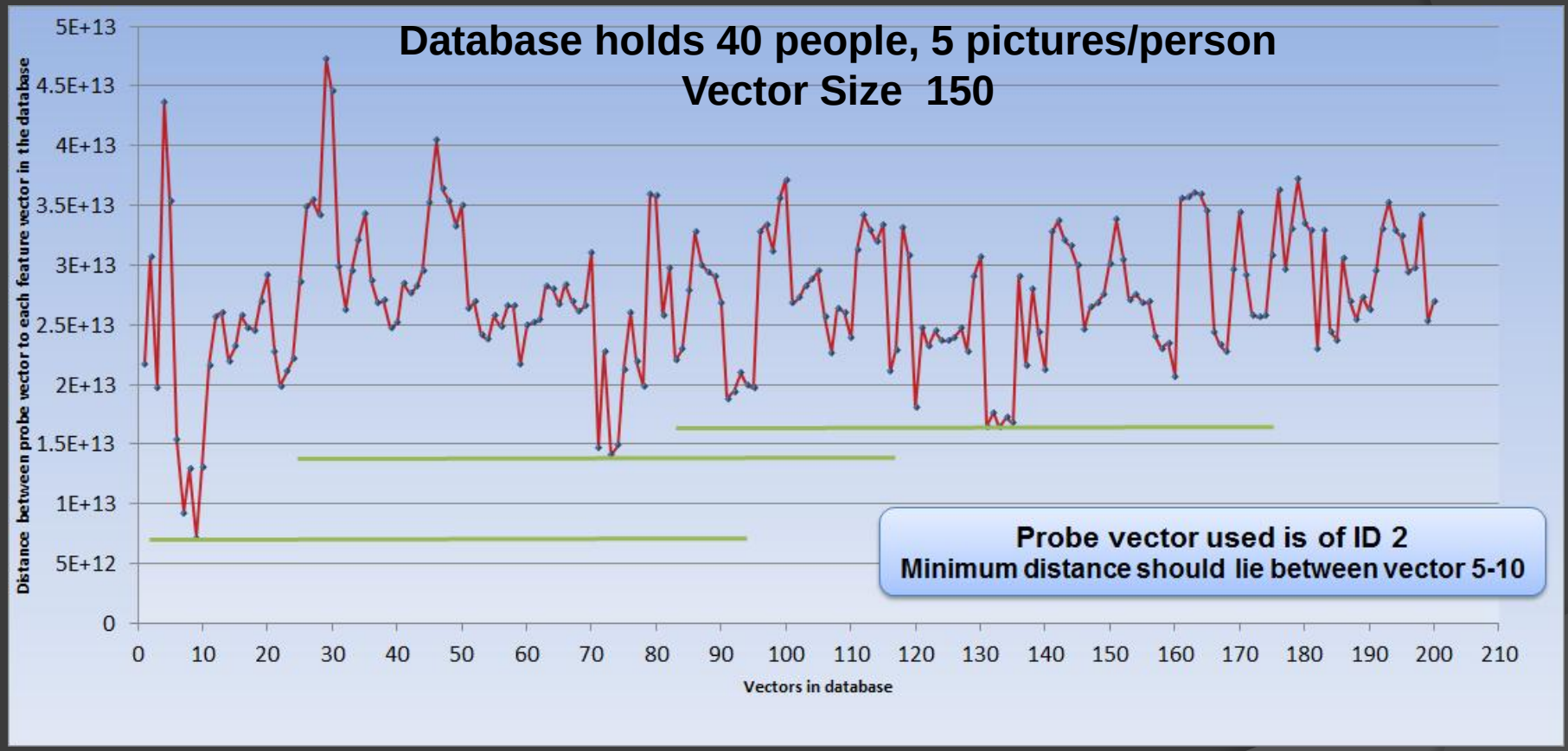
Bob (Server)

Area of Secure communication over an encrypted domain

Alice decrypts the ID

Give [Id] to Alice or 0

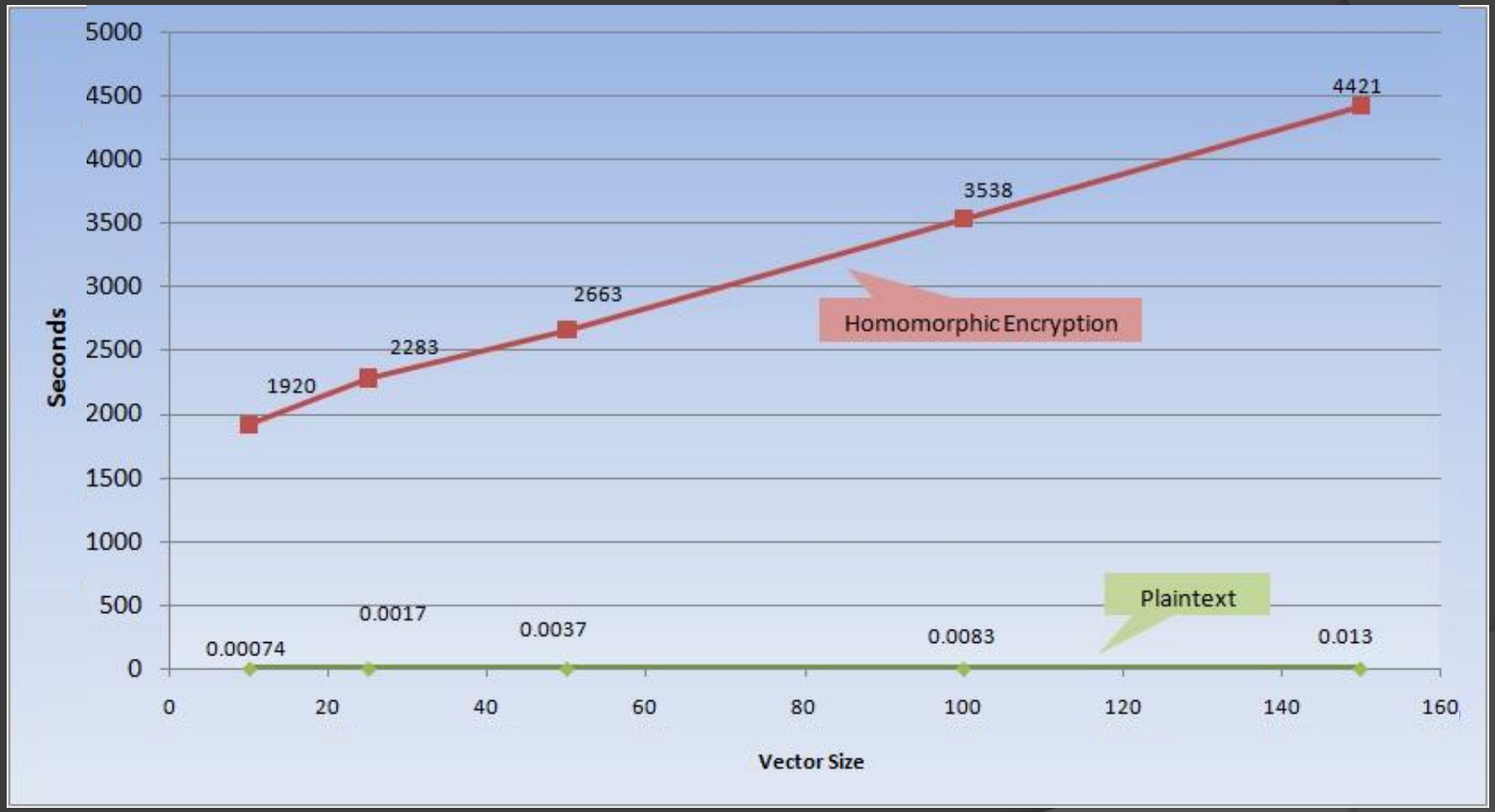
Distance Verification



Example of face variations/person:

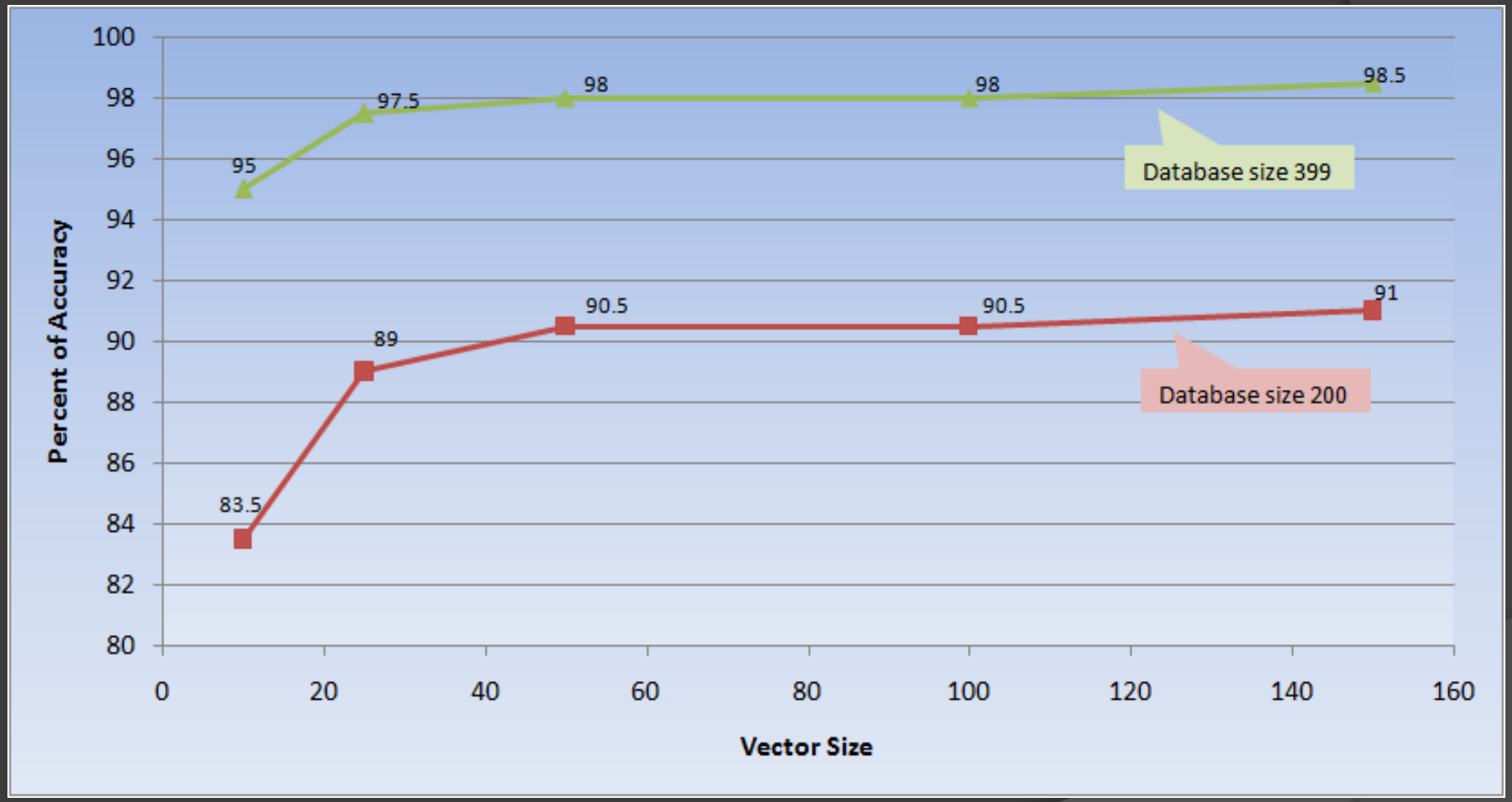
…

HE: Vector Size v. Time



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

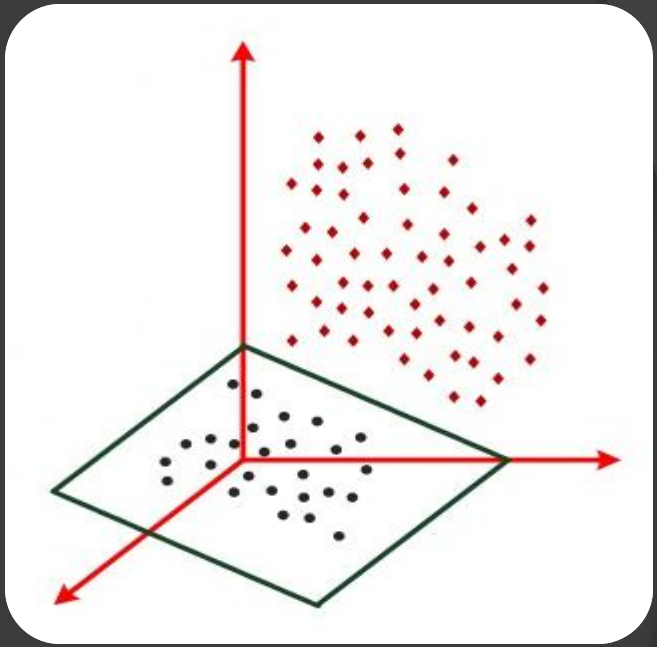
HE: Vector Size v. Accuracy



Database 200: 40 people, 5 representative variation pictures/person
Database 399: 40 people, 10 representative variation pictures/person

Random Projections

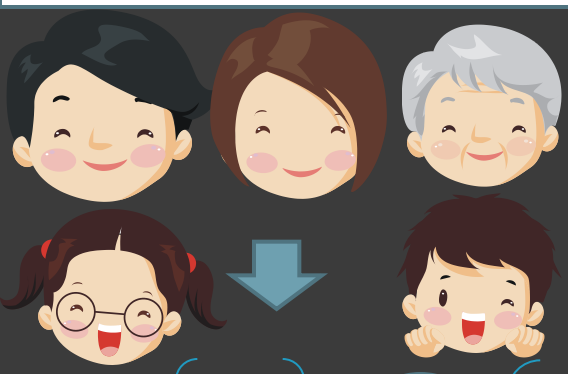
- The core computational method involved in Random Projection is matrix multiplication
- Gaussian, Bernoulli, or other random distribution matrix



$$y = \Phi g$$

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

RP: High Level Overview



Enrollment

$$\begin{bmatrix} 5 \\ \dots \\ 23 \end{bmatrix} \otimes \begin{bmatrix} 12 & 5 \\ \dots & \\ 7 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 24 \\ \dots \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} 4 \\ \dots \\ 22 \end{bmatrix} \otimes \begin{bmatrix} 12 & 5 \\ \dots & \\ 7 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 23 \\ \dots \\ 12 \end{bmatrix}$$

Store TFV

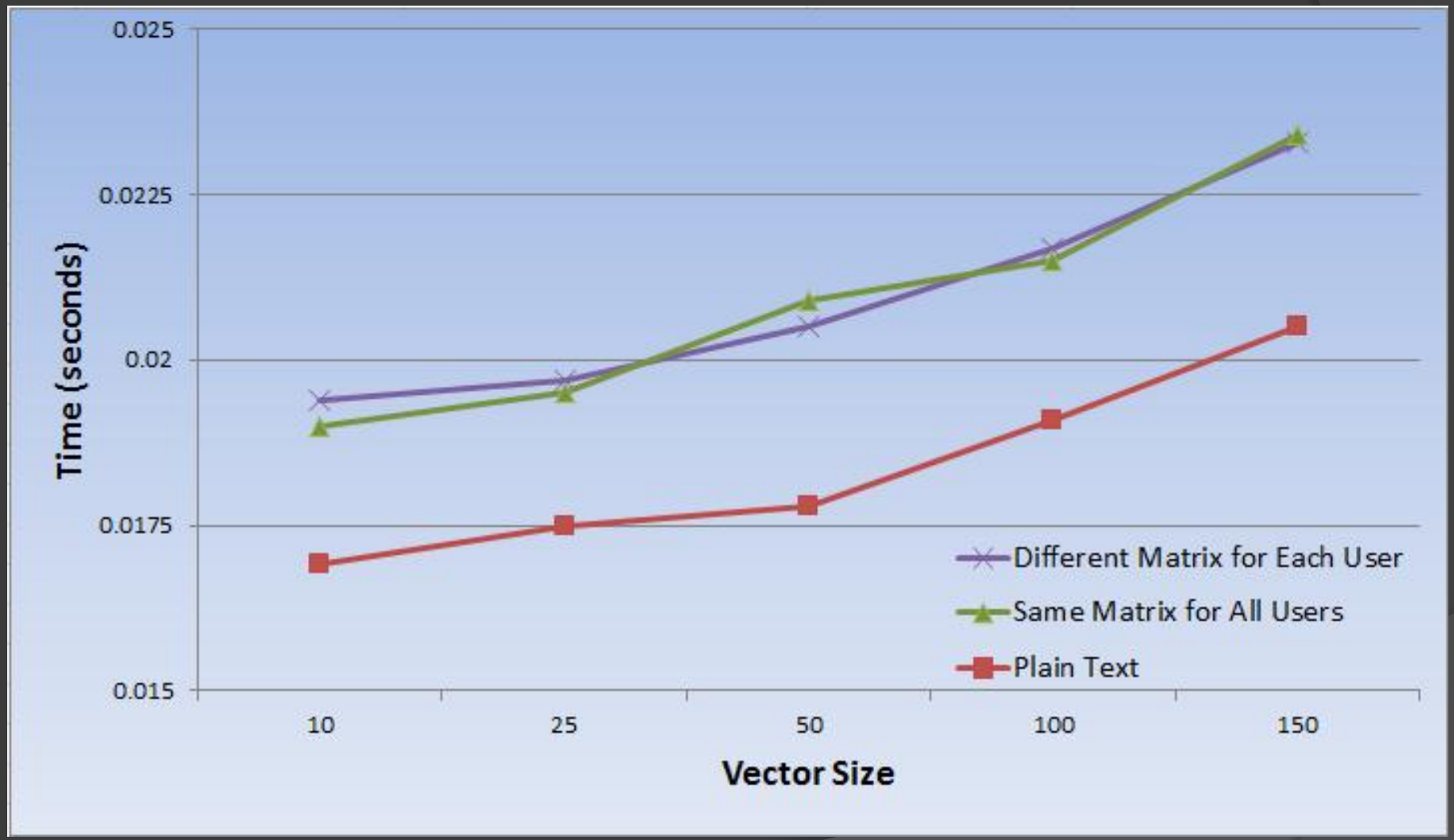
Database

Compare TFV

Yes (ID) or No

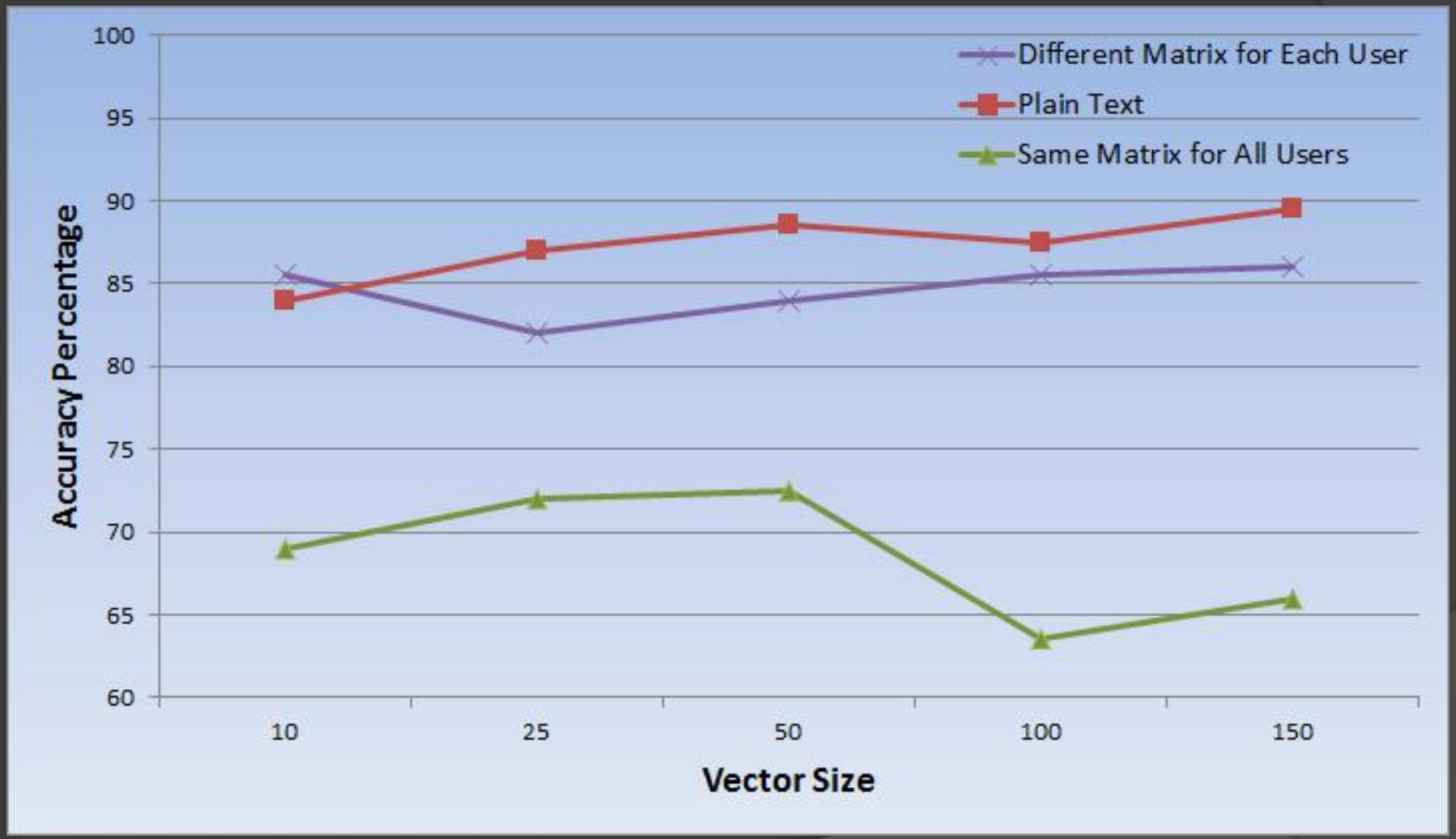
Verification

RP Verification: Vector Size v. Time



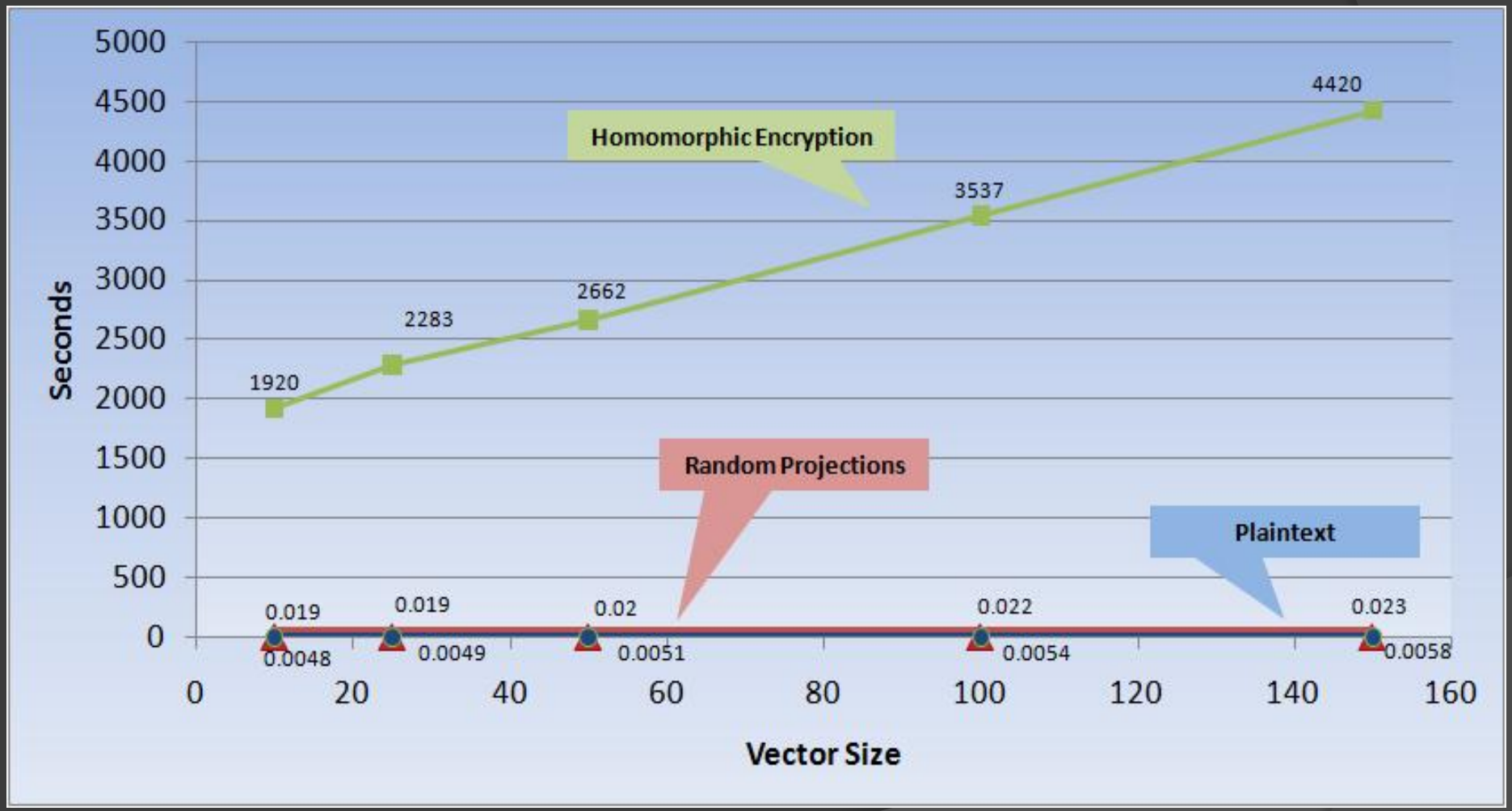
Database 200: 40 people, 5 representative variation pictures/person

RP Verification: Vector Size v. Accuracy

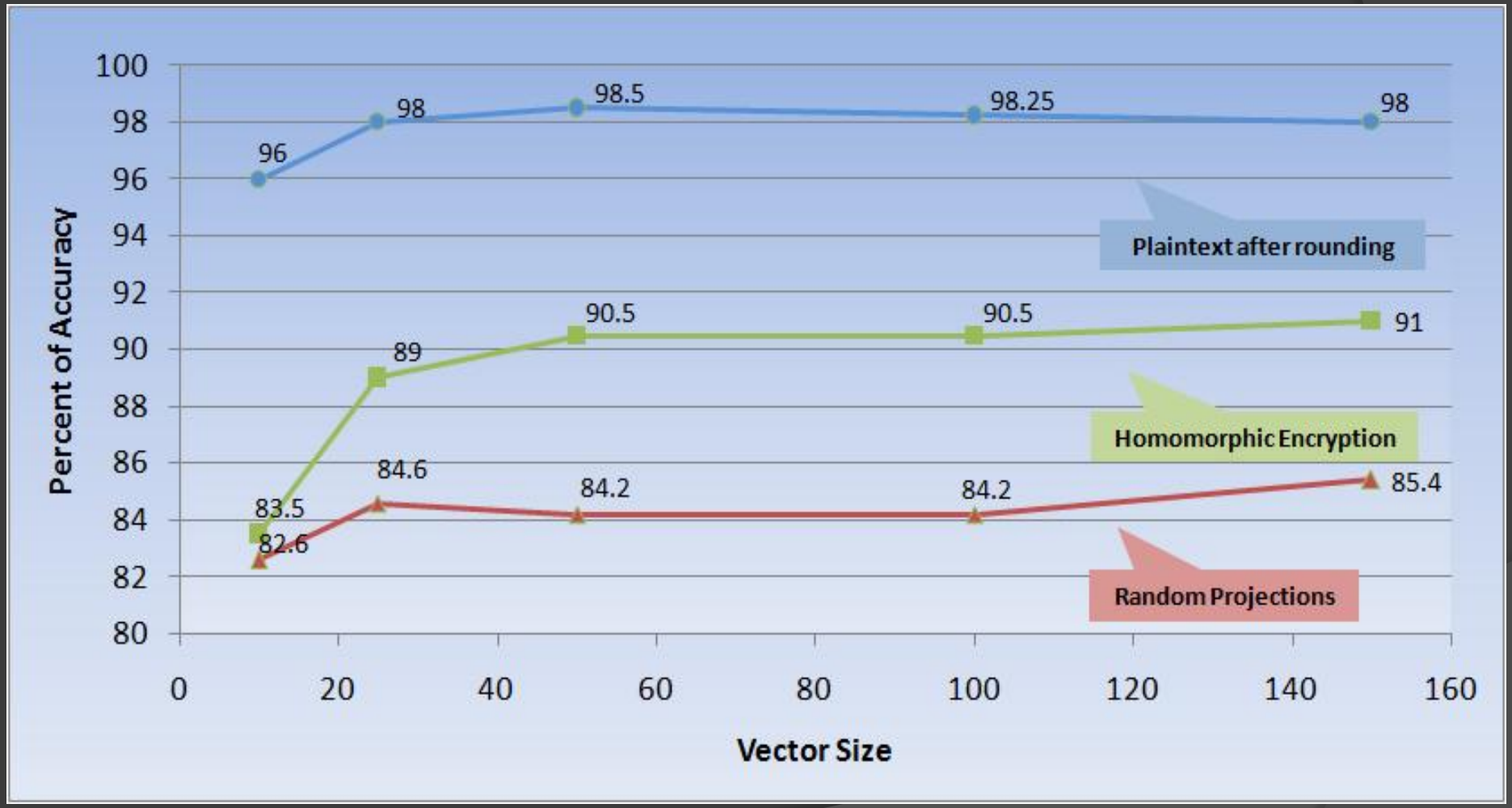


Database 200: 40 people, 5 representative variation pictures/person

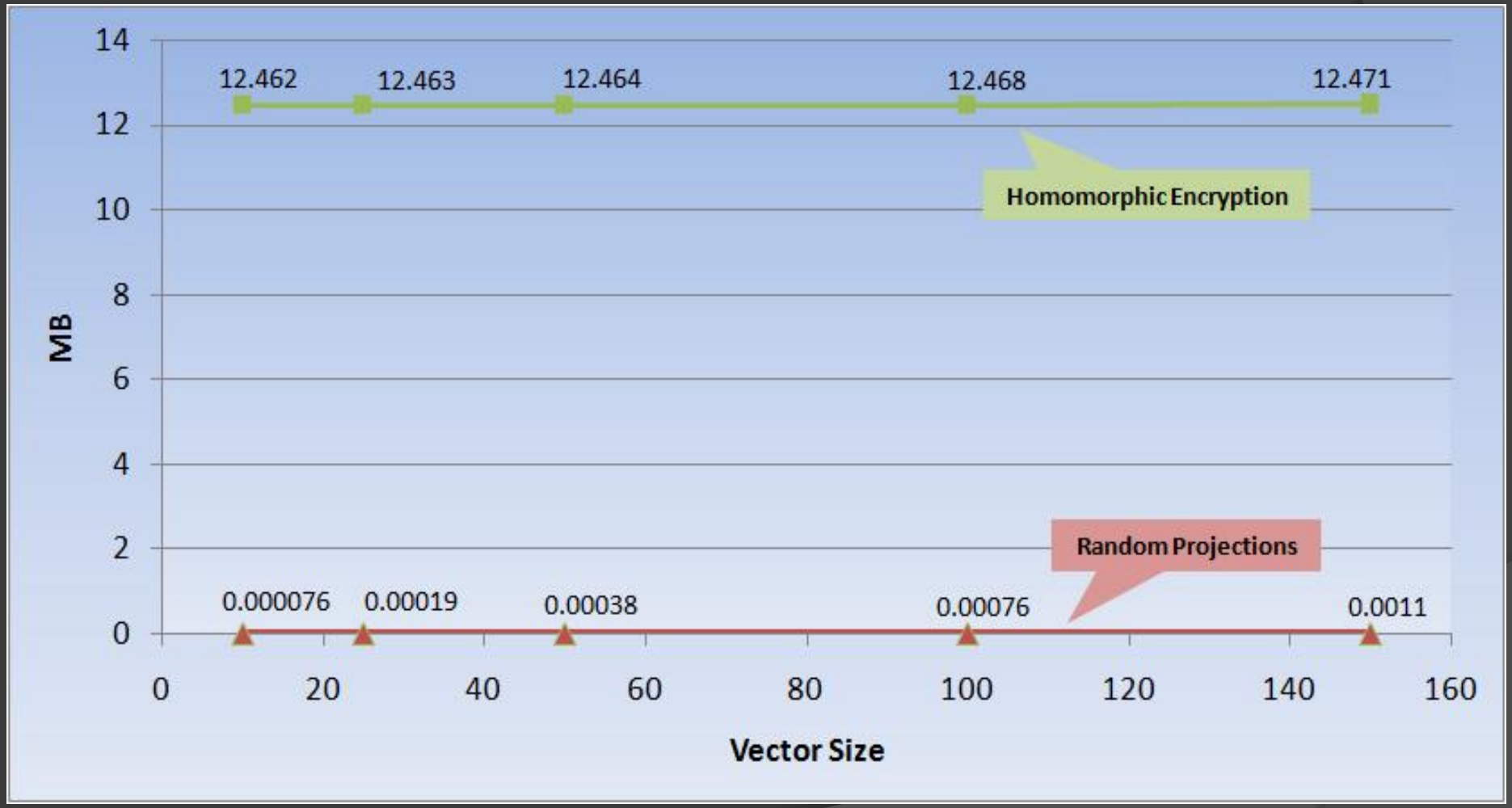
Vector Size v. Runtime



Vector Size v. Matching Accuracy



Vector Size v. Bandwidth



Conclusion & Future Work

- 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

- Pillai, J.K.; Patel, V.M.; Chellappa, R.; Ratha, N.K.; , "Sectored Random Projections for Cancelable Iris Biometrics," *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on* , vol., no., pp.1838-1841, 14-19 March 2010
- Teoh, A.B.J.; Goh, A.; Ngo, D.C.L.; , "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs," *Pattern Analysis and Machine Intelligence, IEEE Transactions on* , vol.28, no.12, pp.1892-1901, Dec. 2006
- Beng Jin Teoh, A.; Chong Tze Yuang; , "Cancelable Biometrics Realization With Multispace Random Projections," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on* , vol.37, no.5, pp.1096-1106, Oct. 2007
- Pillai, J.; Patel, V.; Chellappa, R.; Ratha, N.; , "Secure and Robust Iris Recognition using Random Projections and Sparse Representations," *Pattern Analysis and Machine Intelligence, IEEE Transactions on* , vol.PP, no.99, pp.1, 0

Citations

- Ratha, Connell, & Bolle, 2001, p. 618
- Erkin, Z.; Franz, M.; Guajardo, J.; Katsenbeisser, S.; Lagendijk, I.; Tomas, T.; , “Privacy-Preserving Face Recognition*," PETS '09 Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*, 2009.
- Vladimir Kolesnikov and Thomas Schneider. Improved Garbled Circuit: Free XOR Gates and Applications. In *International Colloquium on Automata, Languages and Programming*, 2008.
- Y. Huang, L. Malka, D.Evans, J.Katz. In *Proc. of the 17th Annual Network and Distributed System Security Symposium (NDSS),* 2011
- A. Sadeghi, T. Schneider, and I. Wehrenberg. Efficient Privacy-Preserving Face Recognition. In International Conference on Information Security and Cryptology,2009
- Some slides are adapted from: http://www.mightbeevil.org/secure-biometrics/ndss-talk.pdf, Huang, Yan. Feb 2011.
- 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