Secure Iris Recognition

Christine Lu, Pennsylvania State University. Mentored by: Dr. Min Wu, Avinash Varna

Media and Security Team

MERIT FAIR BIEN 2009

Introduction

-Goal: protect users' private biometrics info and identify them using their ciphertext.

- Biometrics needs to tolerate small changes. It becomes impossible to directly encrypt the representative code.

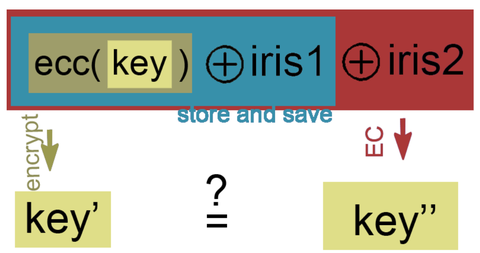
-Using an iris recognition system as our basis, we explored alternative options for secure biometrics methods.

Methods

1. XOR-ECC Method

- Logical operations (XOR) used to hide the iris information with a randomly generated key.
- Error correction code (ECC) used to recalculate the original key, which is used for hashing and identification.

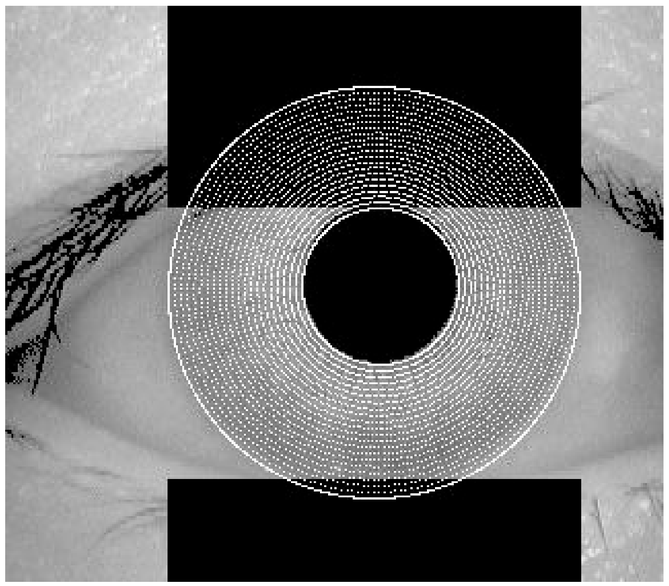
-Based on work by Hao et. Al, University of Cambridge



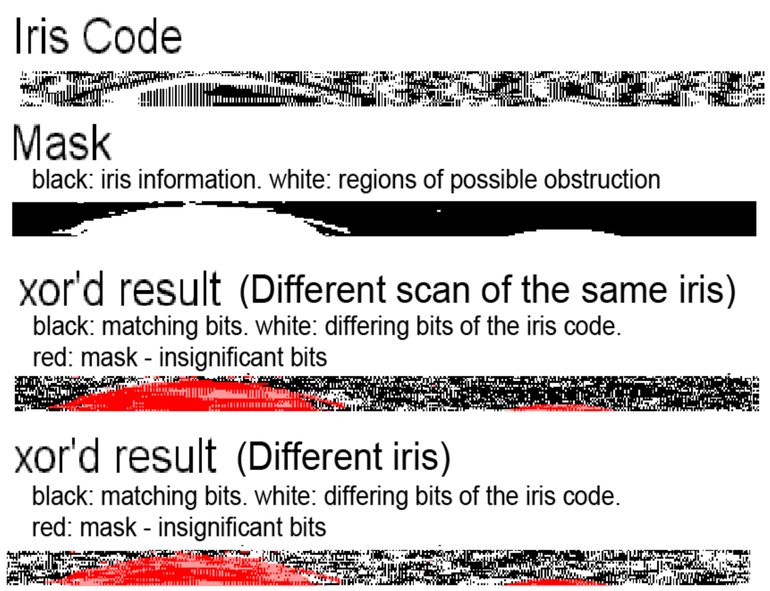
2. Random Projection

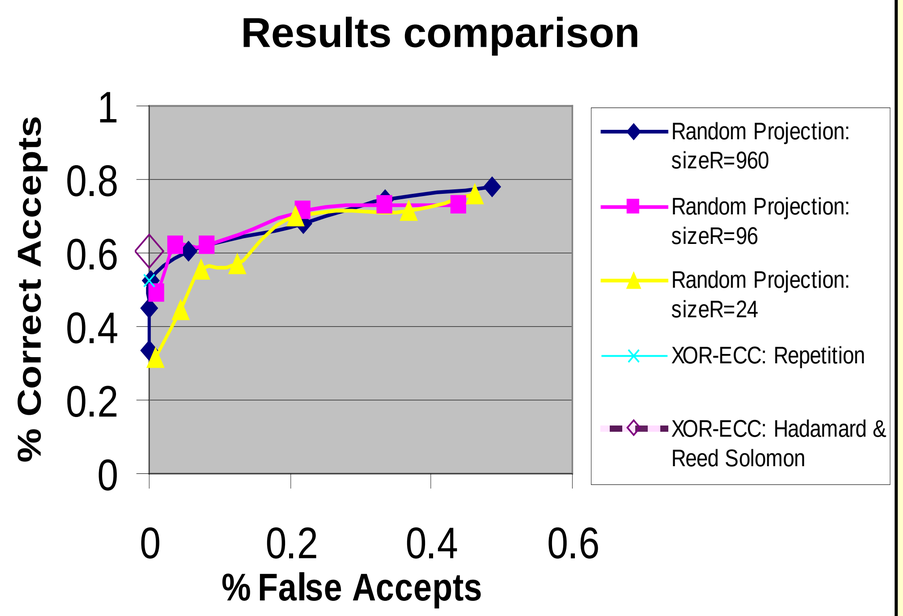
- Random projections used to reduce dimensionality of the iris information, while preserving the distances.
- Vectors are random, so original values are hidden and secure.
- Used the resulting distance to determine possible match.

Results



-Segmented iris scan used to generate iris code.
- Black areas indicate areas of possible iris obstruction





- R: encryption matrix used in random projection.

Conclusions

- Examined the influence of error correction applied to the XOR-ECC method. Hadamard & Reed Solomon has the highest rate of correct accept (60%) and reject (100%).

- Accuracy of random projection increases as the size of the encryption matrix does, but also reveals more information about the original iris.

- Speed of random projection is 31 times that of the XOR-ECC method; there is promise for future research.

- Decreasing the key size leads to less complexity, increased correct acceptance rate, and decreased correct rejection rate.

Acknowledgements: I would like to thank University of Maryland for the opportunity to work here, National Science Foundation for funding this research, and Dr. Min Wu and Avinash Varna for being wonderful mentors and role models.