# Trustable And Generalize Biometric Recognition

## Digital Signal Processing

Ashutosh Kakadiya -1401075
Hardil Mehta -1401018
Harsh Mehta -1401086
Kishan Raval -1401117

School of Engineering and Applied Science,
Ahmedabad University

$11^{th}$ May, 2017

# How Algorithm Works?

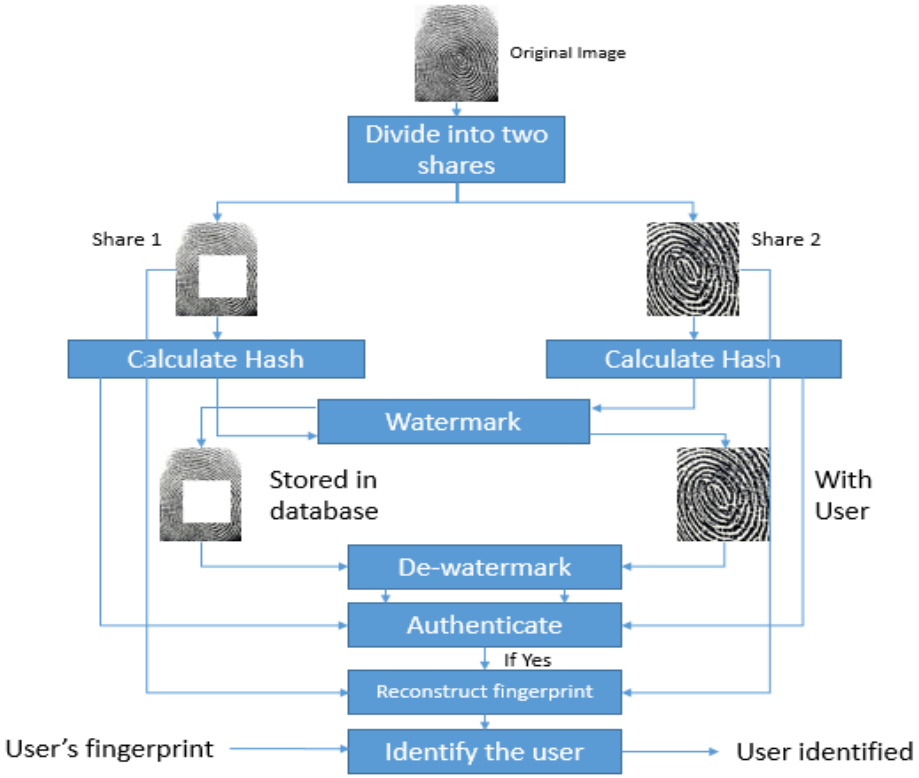


Fig. 1: Flow diagram of an algorithm

# Results

Fig. 2: Original Fingerprint and Share 1 and Share 2

Fig. 3: Watermarked Share 1 and Share 2 with hash values of each other

# Results

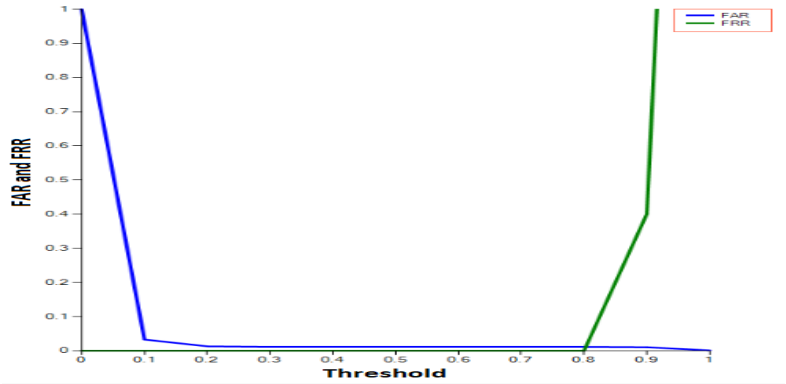


Fig. 4: Threshold vs FAR and FRR for the original images

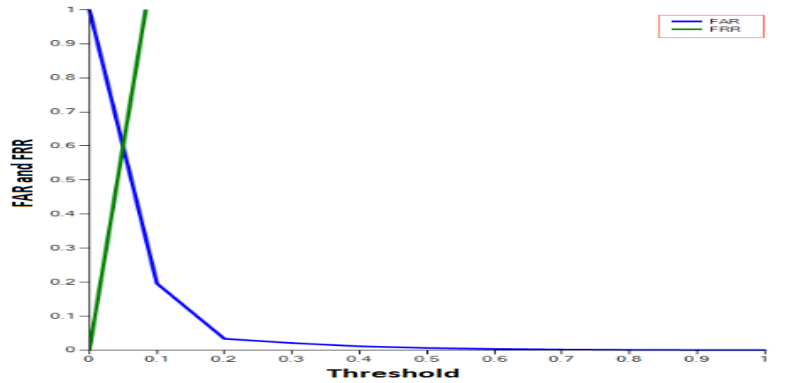


Fig. 5: Threshold vs FAR and FRR for share1

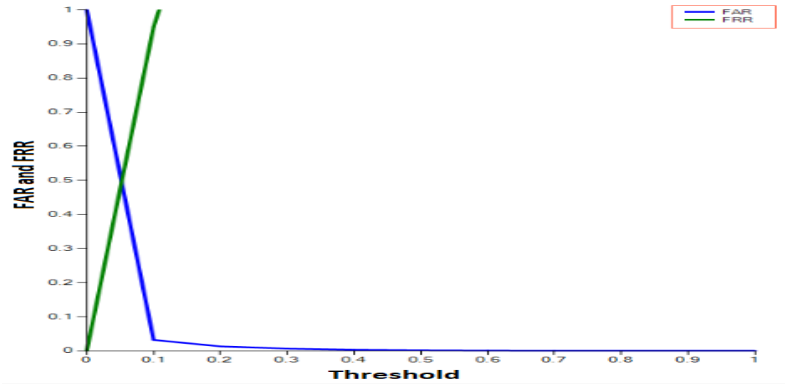


Fig. 6: Threshold vs FAR and FRR for share2

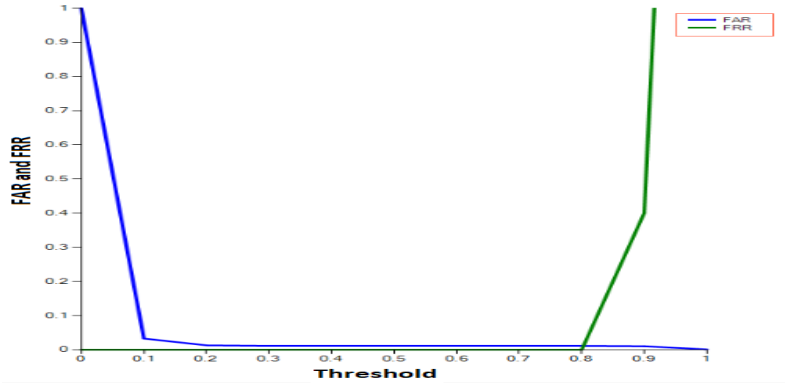


Fig. 7: Threshold vs FAR and FRR for the reconstructed images

# Results

| Comparison of fingerprint of person with fingerprint | Bit Error Rate |
|---|---|
| 1 | 0 |
| 2 | 0.51 |
| 3 | 0.4 |
| 4 | 0.44 |
| 5 | 0.5 |
| 6 | 0.47 |
| 7 | 0.48 |
| 8 | 0.43 |
| 9 | 0.49 |
| 10 | 0.46 |

Table 1: Bit Error Rate of hash values of fingerprint shares of person 1

# Analysis

- FAR and FRR for share1 and share2 says that with the help of only single share we can't identify the user because EER is very high.
- As from the result of FAR and FRR for Original fingerprint and reconstructed fingerprint are same which says that there is no error in reconstructed fingerprint.
- Hash of the one fingerprint share is significantly different then the hash of the other fingerprint and hence system is correctly identifying the person.
- By using hashing and watermarking technique we achieved security of biometric feature.

# References


- [1]M. ABDULLAH, S. DLAY and J. CHAMBERS, "A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography", IEEE, 2016.
- [2]P. Biometrics, "UNDERSTANDING BIOMETRIC PERFORMANCE EVALUATION", 2017.
- [3]Abdullah, M. A., Dlay, S. S., Woo, W. L., & Chambers, J. A. (2016). A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography. IEEE Access, 4, 10180-10193. doi:10.1109/access.2016.2623905