INTERNET TRANSACTION SECURITY WITH FINGERPRINT RECOGNITION

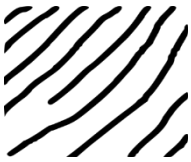
Sagar Nilesh Shah, Kannan Chandrasegaran,
Saurabh Swarup & Shrikant Patnaik

Supervised By - Prof. Cunsheng Ding (CSE) & Prof. Bing Zeng (ECE)

Project Overview

Unlike images from a traditional fingerprint scanner, *fingertip* photos obtained from a **webcam** suffer from low contrast, high noise, and blurring. We present a system that performs matching using such images.
Fingerprint registration and authentication is performed via a web interface. The images are sent to a server where an image enhancement module extracts the fingerprint. A matching module then computes a similarity score for each pair.

Fingerprint matching relies on features known as minutiae



Ridge Ending

Ridge Bifurcation

We have separated our system into two halves: *client-side* and *server-side.*

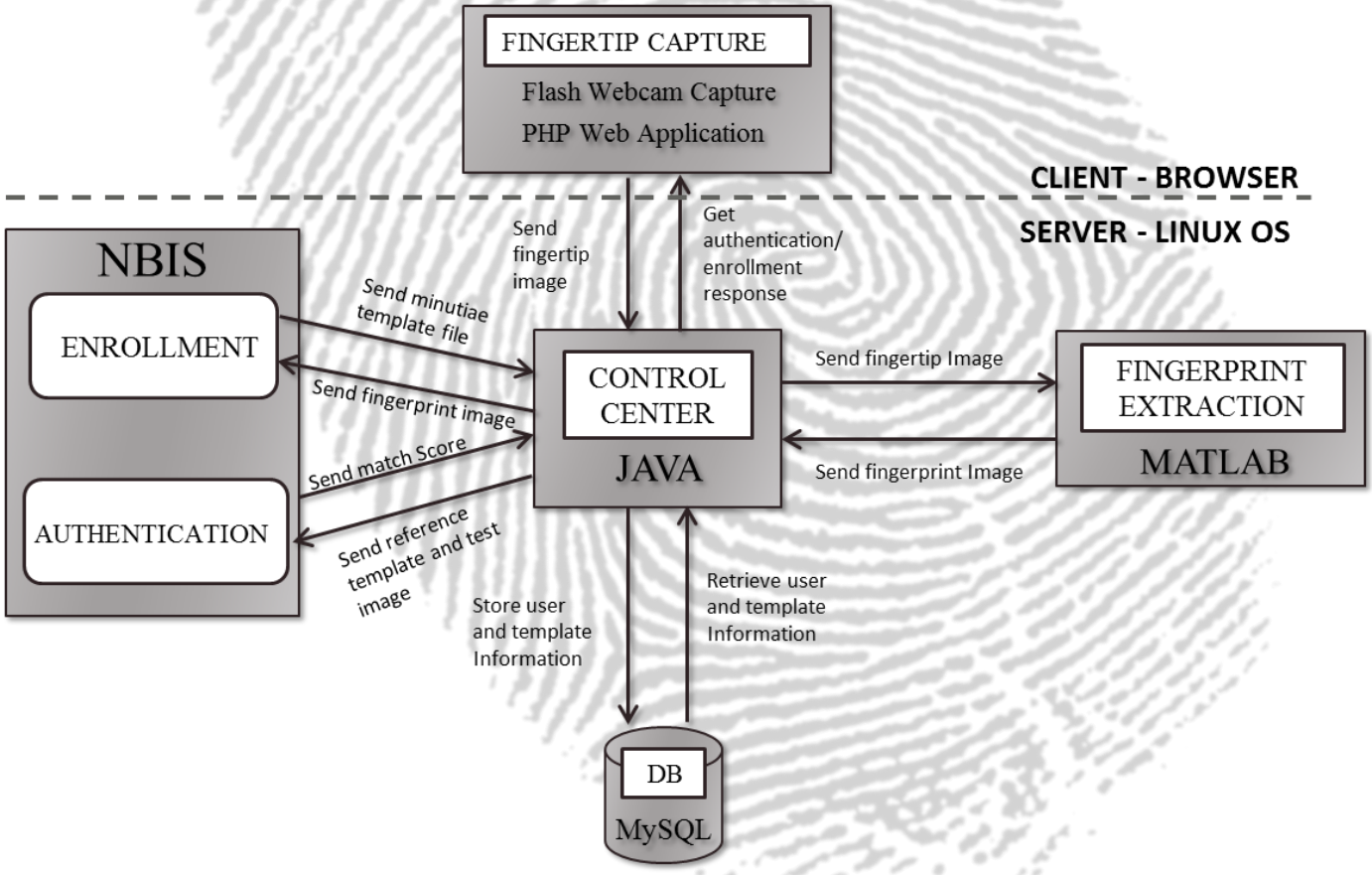
Client side:

- Acquire the low resolution fingertip image from the user, perform basic cropping, and send it to the server securely.

Server application:

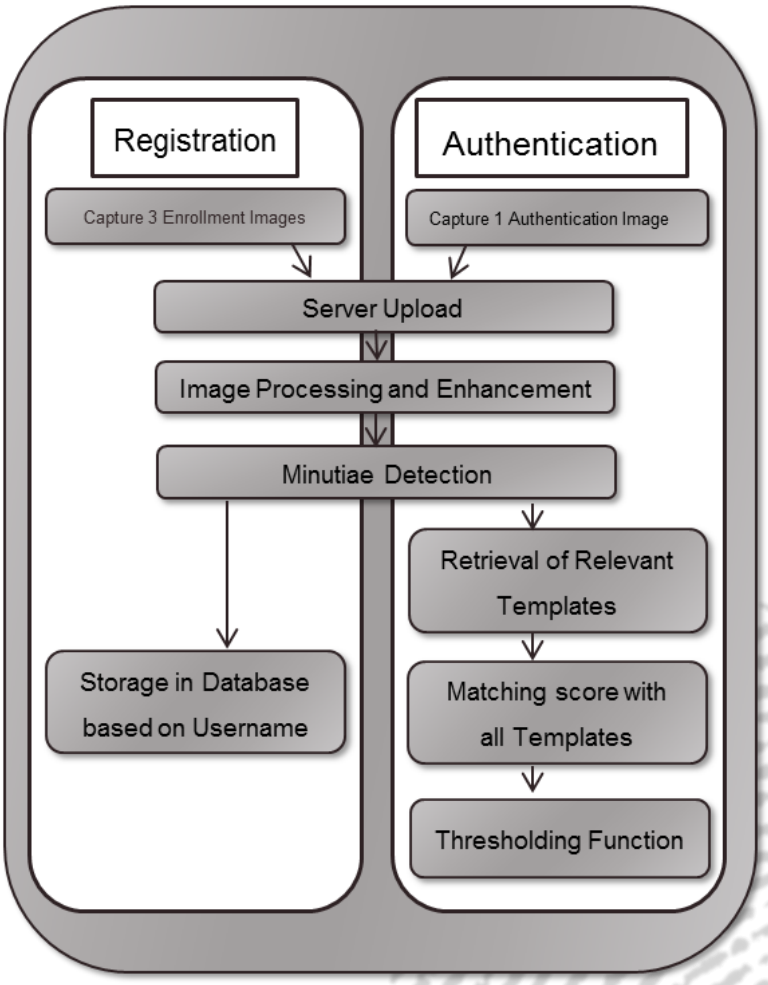
- Perform Image processing, converting a *fingertip* image to a *fingerprint* image
- Perform Authentication using a fingerprint matching module.

System Design

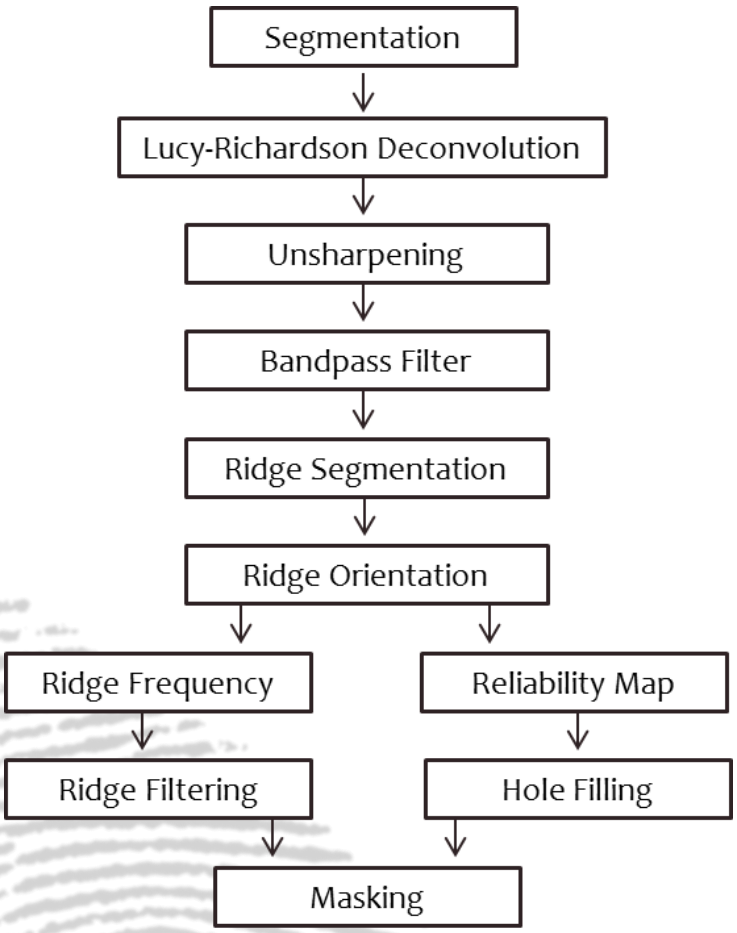


Methodology

Flow Diagram



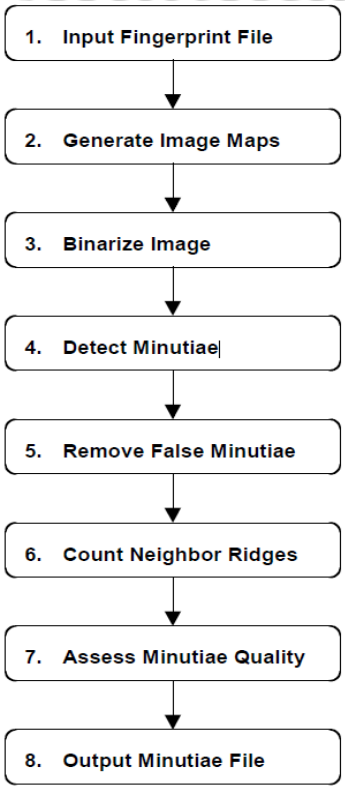
Fingerprint Extraction

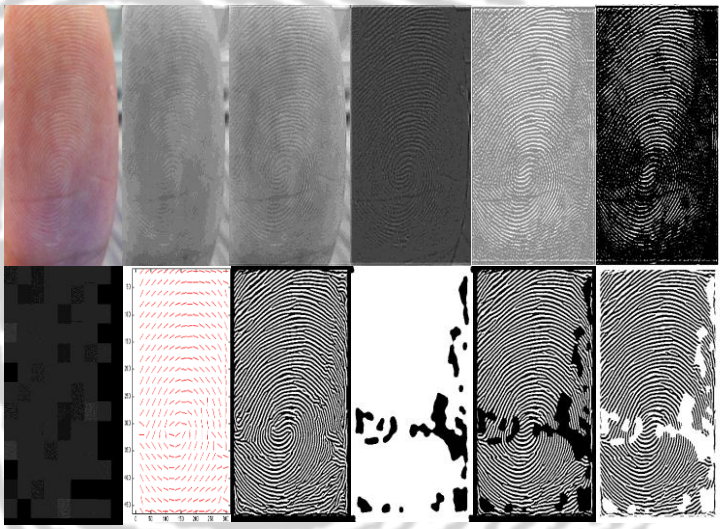


Fingerprint Matching

We use four main NBIS binaries for Matching.

- DJPEG and CJPEG, which convert a MATLAB processed image to a NBIS compatible grey scale image.
- MINDTCT for minutiae detection.
- BOZORTH3 for fingerprint matching.



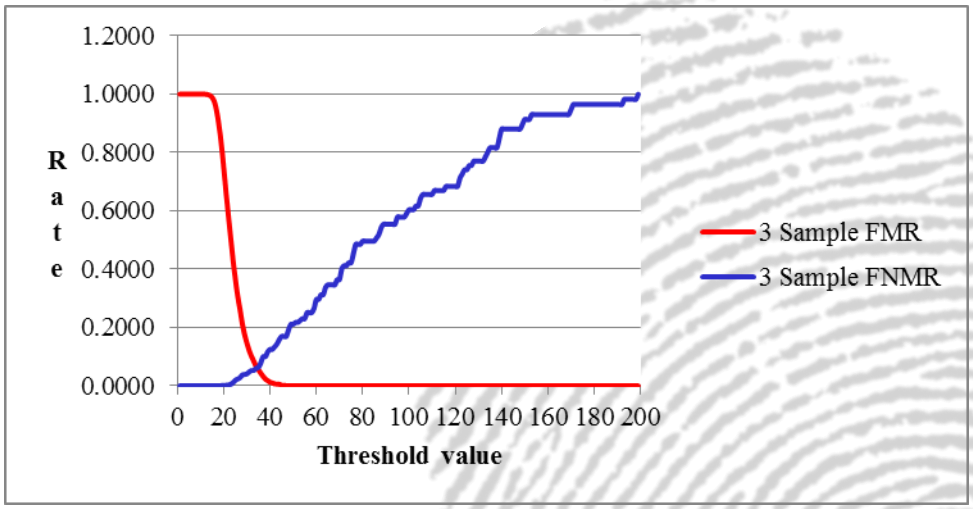


Results after each step of Image Enhancement (from top left):-
1. Original fingertip image 2. Grayscale Image
3. Lucy-Richardson deconvolution
4. Unsharpening 5. Bandpass filtering
6. Normalization 7. Ridge frequency
8. Orientation image 9. Ridge filter
10. Mask after hole filling 11. Masked image
12. Final image

Results

In testing the performance of any fingerprint matching system, two types of errors need to be considered - False Non-Match Rate (FNMR) is the rate at which a genuine user is rejected by the system and False Match Rate (FMR) is the rate at which an impostor is accepted by the system.
There is a natural tradeoff between these two values in any system, as having a more liberal acceptance policy will inevitably accept more impostors, and vice versa. To evaluate a system in general, the Equal Error Rate (EER), defined as the point at which FMR = FNMR, may be used.

We found that 3 Enrollment Samples were ideal as it gave the lowest EER of **6.17%**.



When False Match Rate is set at **1%** (which means there is a 1% chance of an impostor breaching the system) the False Non Match Rate (the chance of a genuine user being rejected) is only **12.5%**.

Conclusion

Our system has a number of merits that give it a significant edge over other authentication systems :

- The system adds an additional layer of security by implementing the webcam based fingerprint authentication system.
- As the registration and authentication system is accessible from a browser, it can be instantly deployed to any user who has access to a computer, a webcam, and a browser.
- As the only required hardware component is a low resolution camera (640 x 480), the deployment cost is very low.
- As the bulk of the processing happens on the server, clients can be built for any platform with great speed.