Iris Recognition for Mobile Devices

Tommy Carpenter, Caleb MacDonald
Central Connecticut State University, New Britain, Connecticut

Why Biometric Security?

As our society evolves further and moves into an age dominated by technology, information security has become a major concern. Unrestricted access to our contacts, credit card and social security numbers has become an increasingly dangerous threat. Our mobile devices now store much of this private information and yet are protected by the weakest forms of security possible, such as a simple password.

Why Iris Recognition?

Iris recognition has been proven to have the lowest Equal Error Rate (EER) among all biometric systems, including fingerprint matching, voice recognition, and facial recognition. It is theorized that iris recognition is the highest form of biometric security available without using DNA.

Mobile Approach

Our iris recognition system was implemented both in Java and in C#, making it readily available for multiple camera-equipped mobile devices and PDAs that run Windows Mobile.

Sacrifices

One of the main constraints we faced during the development process was designing a program that would be able to run quickly and efficiently on a mobile device with limited processing power. To do this, we had to omit certain algorithms that would have improved the EER but also increased the running time. One example of such an algorithm that would have improved the EER is Gabor Filter (which would have added additional time complexity).

Improvements

The goal of future improvements would be to further tweak the system to eliminate discrepancies and increase precision. If we can achieve an EER that matches or is better than systems currently in use, than we would have successfully ported a technology that exists mainly on non-portable computers to mobile devices, which are desperately in need of a higher form of user authentication.

Results

Recognition quality of biometric systems is usually described by the false-accept rate (FAR) and the false- reject rate (FRR). The FAR determines the probability that an impostor can successfully log in to the system, which is closely related the degree of security offered by the system. The FRR determines the probability that a correct user will be rejected by the system, which impacts the degree of user convenience because the user will have to repeat the authentication procedure. Figure 1 shows the FAR and FRR curves of the tested system.

Receiver Operating Curve (ROC) shows the relationship between the ranges of different values of FAR and FRR depending on the level of the decision boundary that is used to discriminate between the authentic user and the impostor. The balance between FAR and FRR depends on this boundary – lowering FAR by increasing the boundary leads to higher FRR and vice versa. An optimal level of the decision boundary can be selected based on the characteristics of the ROC curve to maintain the desired balance between the degree of security and user convenience. Equal Error Rate (EER) is a general measure of a biometric system that indicates the equal values of both FAR and FRR at some level of the decision boundary. As shown in Figure 2, the tested system achieves EER of approximately 3.5%.

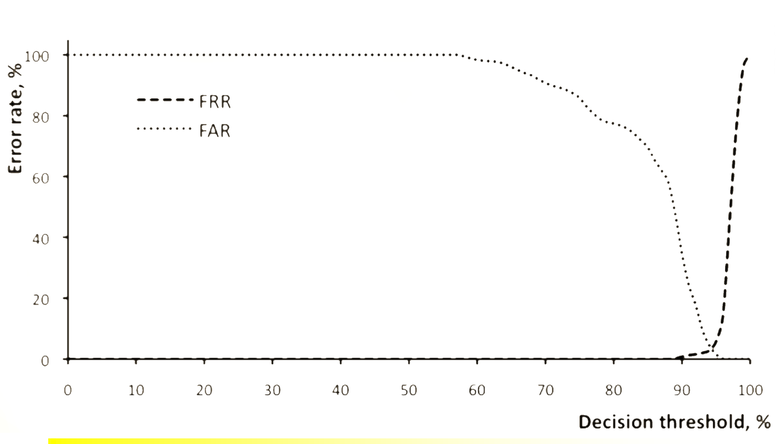

Figure 1. FAR and FRR of the described iris recognition system for a mobile phone.

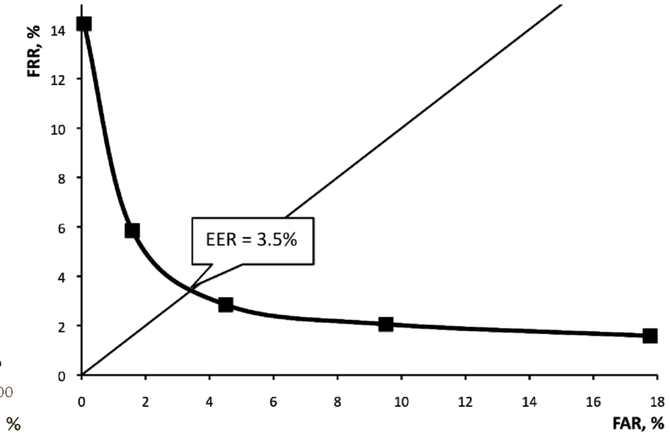

Figure 2. ROC curve showing EER.

EER Comparison

The images used in our testing were obtained from the CASIA database and were 760x480 pixels. Our achieved EER was 3.5% with these images. Equal Error Rates of .05% (near perfect) have been achieved with specially designed mobile hardware and with image resolutions of 2048x1536 pixels. However, the hardware used to achieve these results is not common. Our goal was to describe the results that an average, commercially available phone could achieve. We are planning to port our applications to more powerful devices for future testing. As mobile processing hardware and mobile camera capabilities increase, the EER of iris recognition systems will greatly decrease. We project that commercially available phones will be able to implement iris authentication with a 99+% efficiency rate in the near future.