

Biometric Crossovers

Biometric devices use entirely different means to identify a person. Some of the more familiar techniques involve fingerprinting, iris and retina scans, facial mapping, and voice recognition.

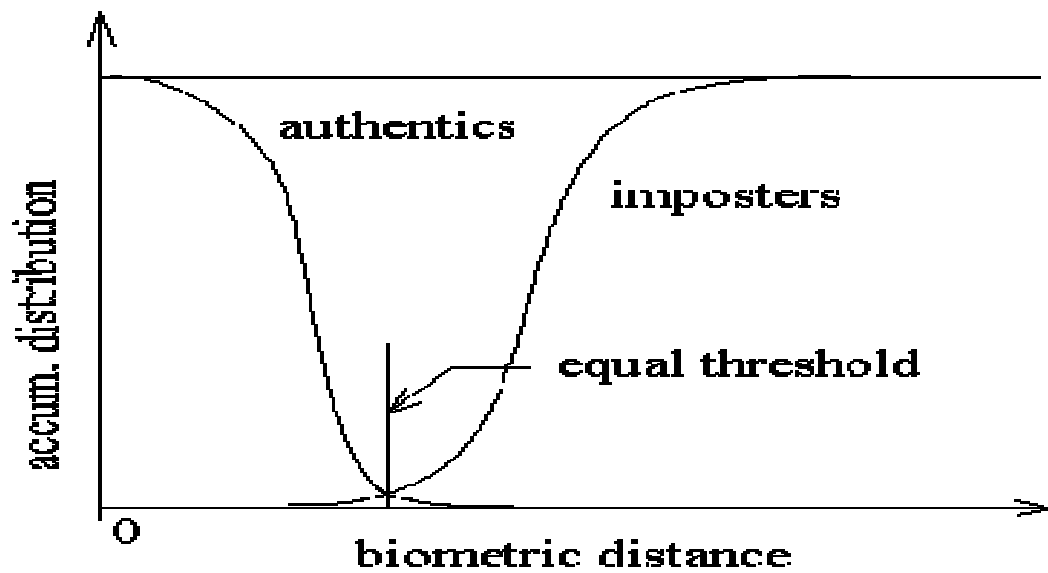
Let's assume that both Alice and Bob both use a laptop and want to use its fingerprint scan biometric authentication device. Alice scans one or more fingers into the reader, which calculates a digital image of her fingerprints for each finger enrolled and stores these images for comparison later. If later, Alice slides her finger in the reader for authentication, the system gets a dynamic image and compares it to the saved image. If they agree, Alice is authenticated. Similarly, Bob has enrolled one or more of his fingers and can use the same system to authenticate to the laptop.

Bob likes reading the sports scores and likes the outdoors. One day, Bob was outside cutting the grass and came in, slid his finger of the scanner and it rejected him. He was really Bob, but the system rejected him. We call that a false rejection. Similarly, one day Alice as busy putting on facial lotion and did not get all the lotion off her fingers, and was similarly rejected by the fingerprint scan. We also say that this was a false rejection.

On the other hand, what if someone other than Alice slid her finger over the reader and it accepted her as Alice? We call that a false acceptance. Of course, theoretically, this could happen to Bob.

For a given type of biometric device, the "the Biometric Crossover Rate" occurs when the false acceptance ratio equals the false rejection ratio. In some available literature, this is called the Biometric Crossover Point. Since biometric systems in general do not have the same threshold settings for acceptance and rejection, it is difficult to compare their goodness using simple threshold values. The Biometric Crossover Rate is actually listed as a normalized statistic so that comparisons can be made with different devices which have different thresholds. In the graph below, we see the Biometric Crossover Rate occurs where the thresholds are the same.

Biometric Crossovers



The table below gives approximate Biometric Crossover Points for some known devices

Biometric Solution	BCP	Biometric Solution	BCP
Digital Fingerprints	< 0.00001 or $< 1 * 10^{-5}$	Forensic Fingerprints	0.0000001 or $< 1*10^{-7}$
Face Recognition	Best is <0.01 or $1*10^{-2}$	Iris Scan	< 0.0000001 or $< 1*10^{-7}$
Speaker Recognition	Best is <0.01 or $1*10^{-2}$	Retina Scan	<0.0001 or $1*10^{-4}$
Signature Analysis	<0.02 or $2*10^{-2}$		

After reading some of the biometric literature on the web, I found one interesting conclusion, which was backed up with some heavy probabilistic mathematics.

The conclusion was "**One strong biometric is better alone than in combination with a weaker one.**"