Equal Error Rate (EER)

EER is the value where FMR(i) and FNMR(i) are equal, i.e., where FMR(i) = FMNR(i). Figure 4 shows an EER value of 0.01 for both FMR and FNMR related to score value 0.3638. Note that EER is the value that, when selected as DT, guarantees the same FMR and FNMR error rates for the algorithm.

The EER is the best single description of the Error Rate of an algorithm and as lower be the EER the lower error rate of the algorithm.

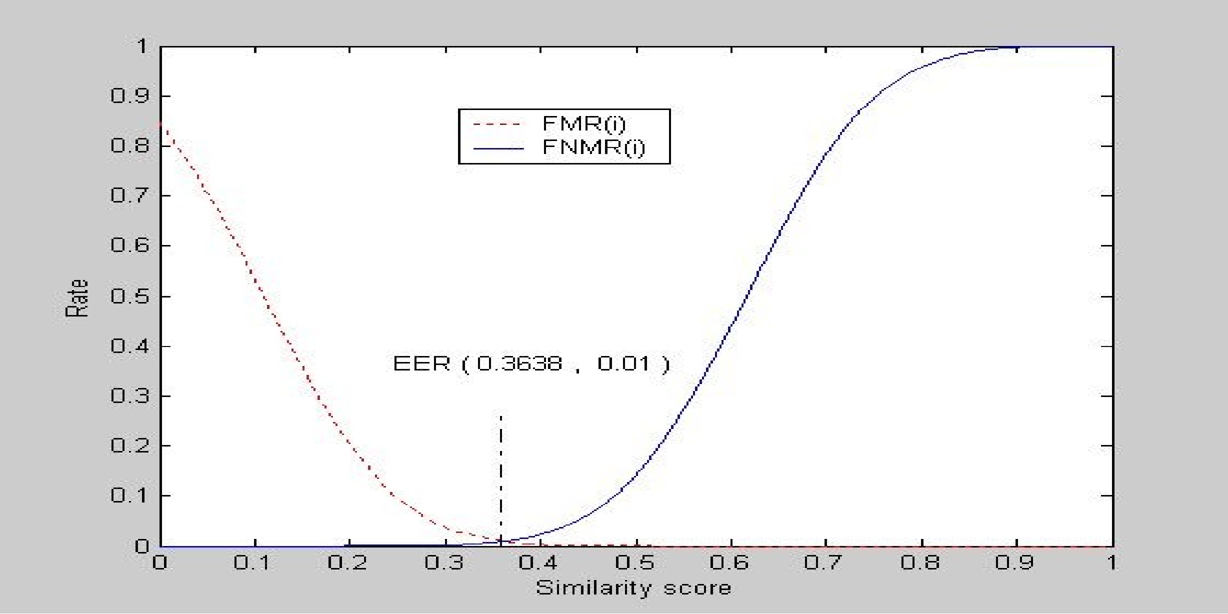

Figure 7. Most commonly used metrics for a verification algorithm. Each metric shows the score value, FMR and FNMR values.

Figure 4. The EER point (0.36328 , 0.01) for the FMR e FNMR functions of the example. For the score value 0.3638, the FMR e FNMR functions have the same value (0.01).<?xml:namespace prefix = o ns = "urn:schemas-microsoft-com:office:office" />

An important issue to use a matching algorithm is to decide the decision threshold. Select the EER score value as DT is frequently a good decision for a regular biometric application because it guarantees the same FMR and FNMR. For example, for the algorithm described on figure 4 if EER is selected as DT the rate for both types of error is 1%. Nevertheless, there is a kind of applications that needs more tuned DT. Let's analyze two different scenarios:

Scenario 1: High security scenario (Bank account access, Ultra secret location access): For a high security scenario FMR of 1% is not acceptable because it means that for one hundred attempts to access the system by impostors one of them will be succeeded. It is an extremely high rate for this kind of application. For decreasing the FMR rate the DT must be increased and as consequence the FNMR will simultaneously increase. In our example, suppose the DT is fixed on 0.507 as showed in figure 5. In that case, the FMR(0.507) is 0,0001 (0,01%) guaranteeing that for ten thousand attempts to access by impostors only one of them would be succeeded which is an acceptable rate for the application. Nevertheless, it must be admitted simultaneously a FNMR rate of 0,1568 (15%) meaning that fifty percents of the genuine attempts to access will be denied. In that case, the system is more save but also more rejected by users, because the high number of unsuccessful attempts of genuine access.

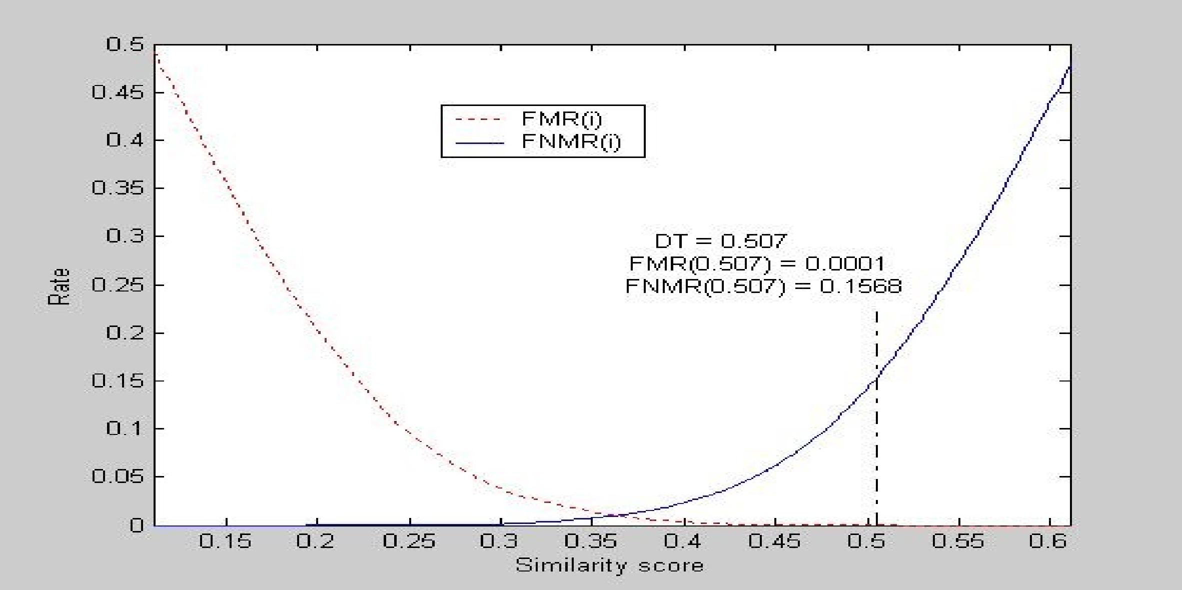

Figure 5. Decision threshold (0.507) fixed for a high security scenario. The FMR value is 0.0001 (0,01%) and the FNMR is 0.1568 (15,6%).

Scenario 2: Low security scenario (Massive access organization, Classroom access, etc) For a low security scenario it is desirable a stable and quickly access for genuine persons and security is desired but it is not a critical issue. In that scenario 1% of FNMR could be very high because it means that for one hundred genuine attempts to access one of them will be rejected. If the DT is fixed in 0.223 as showed in figure 6, the FNMR(0.223) is 0.0001 (0.01%) guaranteeing that for ten thousand genuine attempts to access only one will be rejected.. In that case, the FMR (0.223) is 0.1493 (14,9 %) and it means that almost fifteen percent of impostor attempts to access will be erroneously accepted. In that case, the system will be more accepted by users because the very low probability for genuine rejection, but at the same time its security decreases.

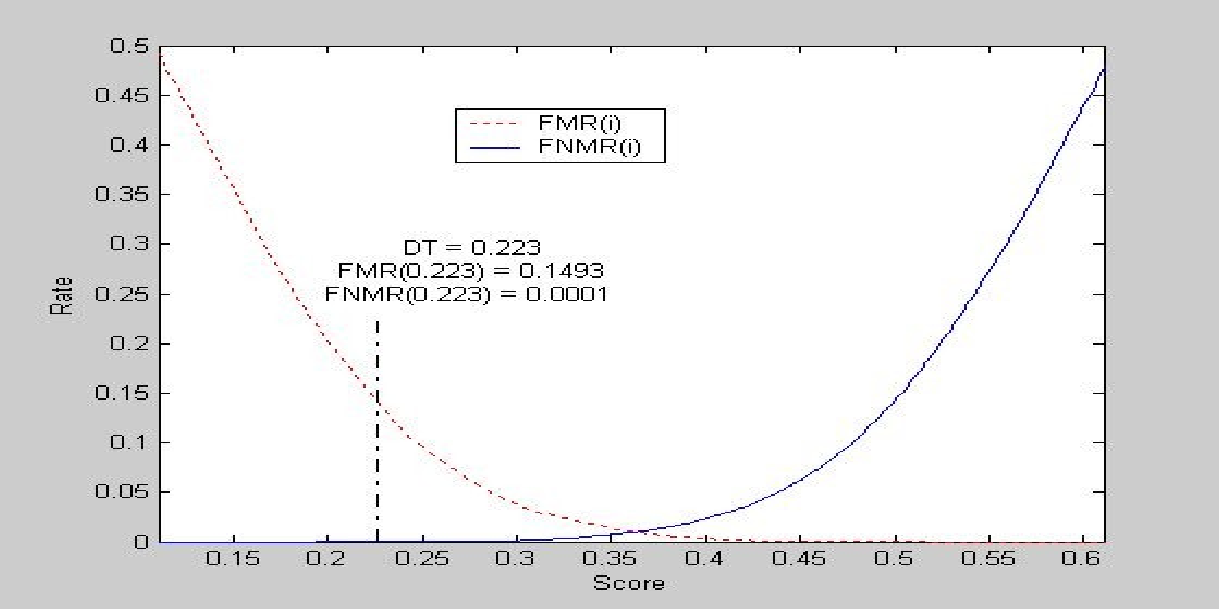

Figure 6. Decision threshold (0.223) fixed for a low security scenario. The FMR value is 0.1493 (14,9%) and the FNMR is 0.0001 (0,01%).