Safety in Numbers

R. Dettmer

November, 2004

IEE Review

Consider the problem of issuing ID cards [identity cards]. A primary concern of the authorities will be to prevent the issuing of an ID card under two or more, unconnected, identities (allowing, for example, a card holder to make multiple, fraudulent claims for benefit). When an individual, Mr Brown say, applies for an ID card, his biometric will be collected. If this is a first application, then the biometric should not match the biometric of anyone already enrolled in the identity register, and Mr Brown's details and biometric can be added as a new entry. If Mr Brown is already registered, then the biometric search should reveal details of the previous application, preventing him from establishing a second fraudulent identity.

In this instance, the relevant biometric errors are:

- False negative identification error - the biometric search fails to find the previously enrolled biometric, presenting the risk of a fraudulent application.

- False positive identification error - the individual's biometric erroneously matches that of another person already enrolled, requiring further checks against the possibility of a fraudulent application.

Usability [ease of use] requires a low probability of false positive identification, while security requires a low probability of false negative identification.