

Likelihood-ratio classifiers in biometrics

Prof.Dr.Ir. R.N.J. Veldhuis (Raymond)
University of Twente
The Netherlands

October 16, 2018, 10.00 – 11.00

Sala Multimediale

**Section of Applied Electronics, Engineering Department, Roma Tre University,
Via Vito Volterra 62, B, 00146, Roma, Italy**

Abstract

The likelihood-ratio is a valuable concept in pattern recognition in general as well as in biometrics. One reason for this is that it is optimal in Neyman-Pearson sense, guaranteeing the best receiver operating characteristic. In this presentation, 2 examples of how the use of likelihood-ratio can improve biometric recognition performance.

Example 1: A likelihood-ratio classifier for histogram features

In a number of classification problems, the features are represented by histograms. Traditionally, histograms are compared by simple distance measures such as the chi-square, the Kullback-Leibler, or the Euclidian distance. This paper proposes a likelihood ratio classifier for histogram features. It assumes that the bin probabilities of the histograms can be modeled by a Dirichlet distribution. A simple method to estimate the Dirichlet parameters is included. Feature selection prior to classification improves the classification performance. It will be demonstrated that the proposed classifier outperforms the chi-square distance measure.

Example 2: Integration of homomorphic encryption and optimal likelihood ratio classifiers

Homomorphic encryption can be used to perform biometric verification, in particular the comparison of biometric features, in an encrypted domain. Because of its complexity in terms of numbers of required operations and the communication protocols involved, proposed implementations involve simple classifiers, such as Euclidian or cosine distances. This may lead to a lower recognition performance than could be achieved with a better classifier. We propose a two-party verification protocol that integrates the likelihood-ratio classifier with El-Gamal homomorphic encryption in such a way that the biometric recognition performance does not decrease with low computational complexity.