

Biometric Consortium 2003 Conference

Natalia A. Schmid and Joseph A. O'Sullivan
West Virginia University

Large Deviations Performance Analysis for Biometrics Systems

In the selection of biometrics for use in a recognition system and in the subsequent design of the system, the predicted performance is a key consideration. Most information available to engineers about biometrics today is in the form of noisy images or signals. A typical challenge here is to select a robust set of deterministic features to guarantee a good recognition performance. An alternative to feature extraction approach is to model the raw data or a set of features as a realization of a stochastic process. While for physical signatures estimation of a stochastic model is more straightforward, for many biometric signatures it remains unapproachable challenge. In this work, we proceed with an analysis assuming the stochastic models are known, providing the analytical tools that will ultimately predict performance when these distributions are better characterized.

Major challenges of biometric system design today include biometric fusion, adjustment of thresholds in decision functions with the goal to achieve an optimal performance, collection of data under conditions of environmental and demographic variations for the purpose of system testing and performance prediction [2,3,5]. In this work, we address two of them. They are performance prediction and capacity for biometrics based identification systems. For our analysis, we model templates stored in the database of an identification system as noisy realizations of independent and identically distributed stationary ergodic random processes. The unknown input data must be identified as a noisy realization of a process that has a known joint distribution with the template realizations. The problem of identification is then a statistical hypothesis testing problem. The average probability of error is asymptotically approximated by an exponential function with explicit dependence on a number of parameters of the system. The minimum probability of error, as we show, is determined by the smallest exponent and is equal to the minimum Chernoff information among all distinct pairs of hypotheses. This result was earlier proved for data with independent and identically distributed components [4]. We extend this result to the case of realizations of stationary and ergodic processes by invoking the theory of large deviations. Capacity and the reliability function [1] of a biometrics-based recognition system are defined. The capacity of an identification system is obtained by viewing identification system as a channel. Finding the capacity provides a guideline for the problem of threshold selection in designing a multimode biometric system.

We provide a number of examples including Gaussian, binary alphabet, and Poisson examples.

This research was supported in part by Office of Naval Research grant MURI N00014-98-1-06-06.

References:

1. R. E. Blahut, *Principles and Practice of Information Theory*, Addison-Wesley, Reading, MA, 1987.
2. "Biometrics: the Future of Identification," *IEEE Computer Magazine*, v. 33, no. 2, pp. 46-81, 2000.
3. A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics. Personal Identification in Networked Society*, (A. Jain, R. Bolle, and S. Pankanti eds.), Kluwer Acad. Publisher, 1999.

4. C. C. Leang, D. H. Johnson, "On the Asymptotic of M-Hypothesis Bayesian Detection," *IEEE Trans. on Info. Theory*, vol. 43, no. 1, pp. 280-282, 1997.

5. A. J. Mansfield and J. L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices," *Version 2.01, NPL Report CMSC 14/02*, Center for Math. and Scientific Computing, National Physical Lab., August 2002.