Databases for Biometric Identification

Frans M.J. Willems
Eindhoven University of Technology
Department of Electrical Engineering
Eindhoven, The Netherlands
Email: f.m.j.willems@tue.nl

ABSTRACT

In this lecture we consider databases that are used in biometric identification settings. We assume that the biometric sequences describing the individuals consist of independent and identically distributed variables. It is our objective to find the fundamental limits that characterize such systems.

First we consider an unprotected database. We determine the so-called identification capacity, i.e., the maximum rate of individuals that makes reliable identification of the individual based on a noisy observation of the corresponding enrolled sequence possible [1],[2].

Next we focus on search complexity. Since the database contains randomly generated enrollment sequences, exhaustive search procedures seem to be required to achieve the identification capacity. To find out whether smaller search complexities can be achieved, we investigate a clustering approach, in which a first decoder determines a clustering index and a second decoder does the identification, based on this index. The first decoder is unaware of the enrolled sequences, the second one has access to these sequences. For this setting we determine the fundamental limits. These limits give us an idea about the trade-off between search and memory complexity. Although the fundamental limits that characterize such systems.

In the second part of the lecture we discuss protected databases, that are used for authentication as well as for identification. Each individual, by enrolling in the database, obtains a secret. Moreover helper data is stored in the database for each individual. During identification in addition to the identity index, this secret has to be reconstructed, from the noisy observation of the enrolled sequence and the helper data [9],[11]. We assume that the database does not leak information about the secrets and consider also the so-called privacy leakage, i.e. the information that the database contains about the biometric enrollment sequences [7],[10]. We investigate the fundamental limits for this setting and discuss the connections to earlier work, e.g. that of Westover and O’Sullivan [4] and Tuncel [5].

Collaborators: Tanya Ignatenko, Eindhoven University of Technology, and Farzad Farhadzadeh, University Geneva.

REFERENCES