CCIT Report #924 May 2018

False–Accept/False–Reject Trade–offs in Biometric Authentication Systems

Neri Merhav

The Andrew & Erna Viterbi Faculty of Electrical Engineering
Technion - Israel Institute of Technology
Technion City, Haifa 32000, ISRAEL
E–mail: merhav@ee.technion.ac.il

Abstract

Biometric authentication systems, based on secret key generation, work as follows. In the enrollment stage, an individual provides a biometric signal that is mapped into a secret key and a helper message, the former being prepared to become available to the system at a later time (for authentication), and the latter is stored in a public database. When an authorized user requests authentication, claiming his/her identity as one of the subscribers, he/she has to provide a biometric signal again, and then the system, which retrieves also the helper message of the claimed subscriber, produces an estimate of the secret key, that is finally compared to the secret key of the claimed user. In case of a match, the authentication request is approved, otherwise, it is rejected.

Evidently, there is an inherent tension between two desired, but conflicting, properties of the helper message encoder: on the one hand, the encoding should be informative enough concerning the identity of the real subscriber, in order to approve him/her in the authentication stage, but on the other hand, it should not be too informative, as otherwise, unauthorized imposters could easily fool the system and gain access. A good encoder should then trade off the two kinds of errors: the false reject (FR) error and the false accept (FA) error.

In this work, we investigate trade–offs between the random coding FR error exponent and the best achievable FA error exponent. We compare two types of ensembles of codes: fixed–rate codes and variable–rate codes, and we show that the latter class of codes offers considerable improvement compared to the former. In doing this, we characterize the optimal rate functions for both types of codes. We also examine the effect of privacy leakage constraints on these trade-offs, for both fixed–rate codes and variable–rate codes.

Index Terms: biometric systems, secret sharing, error exponents, random binning, fixed–length, variable–length, privacy leakage.