CCIT Report #912 July 2017

Ensemble Performance of Biometric Authentication Systems Based on Secret Key Generation

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

We study the ensemble performance of biometric authentication systems, based on secret key generation, which 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, s/he 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. Referring to an ensemble of systems based on Slepian–Wolf binning, we provide a detailed analysis of the false–reject and false–accept probabilities, for a wide class of stochastic decoders. We also comment on the security for the typical code in the ensemble.

Index Terms: biometric security, Slepian-Wolf coding, random binning, error exponents, secrete key generation.

I. Introduction

We consider a biometric authentication system that is described in [7, Sections 2.2–2.6], which is based on the notion of secret key generation and sharing due to Maurer [8] and Ahlswede and Csiszár [1], [2]. Specifically, such a system works as follows. In the enrollment stage, an individual which subscribes to the system provides a biometric signal, $\boldsymbol{X} = (X_1, X_2, \ldots, X_n)$. The system receives this signal and generates (using its encoder) two outputs in response. The first output is a secret key, $\boldsymbol{S}$, at rate $R_{\rm s}$ and the second is a helper message, $\boldsymbol{W}$, at rate $R_{\rm w}$. The secret