CCIT Report #464
January 2004

On Joint Information Embedding and Lossy Compression in the Presence of a Stationary Memoryless Attack Channel

Alina Maor* and Neri Merhav

January 13, 2004

Department of Electrical Engineering
Technion – Israel Institute of Technology
Technion City, Haifa 32000, ISRAEL
{alinam@tx, merhav@ee}.technion.ac.il

Abstract

We consider the problem of optimum joint information embedding and lossy compression with respect to a fidelity criterion. The decompressed composite sequence (stegotext) is distorted by a stationary memoryless attack, resulting in a forgery which in turn is fed into the decoder, whose task is to retrieve the embedded information. The goal of this paper is to characterize the maximum achievable embedding rate R_e (the embedding capacity C_e) as a function of the compression (composite) rate R_c and the allowed average distortion level Δ, such that the average probability of error in decoding of the embedded message can be made arbitrarily small for sufficiently large block length. We characterize the embedding capacity and demonstrate how it can be approached in principle. We also provide a single-letter expression of the minimum achievable composite rate as a function of R_e and Δ, below which there exists no reliable embedding scheme.

1 Introduction

The subject of watermarking and information embedding has been attracting a vast amount of attention of both the academic world and the industry, due to an increasing awareness for the need of data protection in its various forms: ownership identification, data forgery exposure, etc., as is extensively surveyed in e.g., [1]-[4] as well as in many other publications. Generally speaking, a good watermarking code should satisfy several conflicting requirements: One the one hand, the watermark should be *perceptually transparent*, that is,

*This work is part of A. Maor's M.Sc. dissertation.