CCIT Report #472 March 2004

On Causal and Semicausal Codes for Joint Information Embedding and Source Coding

Neri Merhav*
Department of Electrical Engineering
Technion – Israel Institute of Technology
Haifa 32000, Israel
merhav@ee.technion.ac.il

Erik Ordentlich
Hewlett-Packard Laboratories
1501 Page Mill Road
Palo Alto, CA 94304, USA
eord@hpl.hp.com

March 1, 2004

Abstract

A source of random message bits is to be embedded into a covertext modeled as a discrete memoryless source (DMS), resulting in a stegotext from which the embedded bits should be recoverable. A causal code for such a scenario consists of an encoder that generates the stegotext as a causal function of the message bits and the covertext, and a decoder that reproduces the message bits as a causal function of the stegotext. A semicausal code, on the other hand, has an encoder that is causal only with respect to the covertext, and not necessarily with respect to the message, and has a possibly noncausal decoder. We analyze the possible tradeoffs among: (a) the distortion between the stegotext and the covertext, (b) the compressibility of the stegotext, and (c) the rate at which random bits are embedded, that are achievable with causal and semicausal codes, with and without attacks on the stegotext. We also study causal and semicausal codes for the private version of the above scenario in which the decoder has access to the covertext. Connections are made with the causal rate–distortion function of Neuhoff and Gilbert [10], as well as the problem of channel coding with causal side information at the transmitter analyzed by Shannon [11]. For example, the optimal tradeoffs among the three quantities above for causal codes are shown to be achievable by time sharing a small number of scalar or symbol–by–symbol encoders and decoders, paralleling the main result of [10].

1 Introduction

We study the problem of joint lossy compression and information embedding under various causality restrictions on the encoder and decoder. Specifically, let $X_1, X_2, \ldots \sim P_X$ be a discrete memoryless covertext, whose elements take on values in a finite alphabet $\mathcal{X}$, and let $U_1, U_2, \ldots$ be an independent stream of purely random message bits. A scheme for joint compression and embedding with embedding rate R_e, in full generality, consists of an encoder that maps $U^{\lceil nR_e \rceil} \stackrel{\triangle}{=} U_1, \ldots, U_{\lceil nR_e \rceil}$ and $X^n \stackrel{\triangle}{=} X_1, \ldots, X_n$ into a stegotext $\hat{X}^n \stackrel{\triangle}{=} \hat{X}_1, \ldots, \hat{X}_n$, taking values in another finite alphabet $\hat{\mathcal{X}}$, and a

*Work done while visiting Hewlett-Packard Laboratories, 1501 Page Mill Road, Palo Alto, CA 94304, USA.