CCIT Report #482 May 2004

On Joint Coding for Watermarking and Encryption

Neri Merhav

Department of Electrical Engineering
Technion - Israel Institute of Technology
Haifa 32000, ISRAEL
merhav@ee.technion.ac.il

Abstract

In continuation to earlier works where the problem of joint information embedding and lossless compression (of the composite signal) was studied in the absence [8] and in the presence [9] of attacks, here we consider the additional ingredient of protecting the secrecy of the watermark against an unauthorized party, which has no access to a secret key shared by the legitimate parties. In other words, we study the problem of joint coding for three objectives: information embedding, compression, and encryption. Our main result is a coding theorem that provides a single–letter characterization of the best achievable tradeoffs among the following parameters: the distortion between the composite signal and the covertext, the distortion in reconstructing the watermark by the legitimate receiver, the compressibility of the composite signal (with and without the key), and the equivocation of the watermark, as well as its reconstructed version, given the composite signal. In the attack–free case, if the key is independent of the covertext, this coding theorem gives rise to a threefold *separation principle* that tells that asymptotically, for long block codes, no optimality is lost by first applying a rate–distortion code to the watermark source, then encrypting the compressed codeword, and finally, embedding it into the covertext using the embedding scheme of [8]. In the more general case, however, this separation principle is no longer valid, as the key plays an additional role of side information used by the embedding unit.

Index Terms: Information hiding, watermarking, encryption, data compression, separation principle, side information, equivocation, rate–distortion.