CCIT Report No. 304

Identification in the Presence of Side Information with Application to Watermarking

Yossef Steinberg and Neri Merhav

ABSTRACT

Watermarking codes are analyzed from an information-theoretic viewpoint as identification codes with side information that is available at the transmitter only or at both ends. While the information hider embeds a secret message (watermark) in a covertext message (typically, text, image, sound, or video stream) within a certain distortion level, the attacker, modeled here as a memoryless channel, processes the resulting watermarked message (within limited additional distortion) in attempt to invalidate the watermark. In most applications of watermarking codes the decoder need not carry out full decoding, as in ordinary coded communication systems, but only to test whether a watermark at all exists and if so, whether it matches a particular hypothesized pattern. This fact motivates us to view the watermarking problem as an identification problem, where the original covertext source serves as side information. In most applications, this side information is available to the encoder only, but sometimes it can be available to the decoder as well. For the case where the side information is available at both encoder and decoder, we derive a formula for the identification capacity and also provide a characterization of achievable error exponents. For the case where side information is available at the encoder only, we derive upper and lower bounds on the identification capacity. All characterizations are obtained as single-letter expressions.