On Steganographic Embedding Efficiency

Jessica Fridrich[1], Petr Lisoněk[2], and David Soukal[1]

[1] Binghamton University, Binghamton, NY 13902–6000
[2] Simon Fraser University, Burnaby, Britsh Columbia, V5A 1S6, Canada
{fridrich,dsoukal1}@binghamton.edu, plisonek@cecm.sfu.ca

Abstract. In this paper, we study embedding efficiency, which is an important attribute of steganographic schemes directly influencing their security. It is defined as the expected number of embedded random message bits per one embedding change. Constraining ourselves to embedding realized using linear covering codes (so called matrix embedding), we show that the quantity that determines embedding efficiency is not the covering radius but the average distance to code. We demonstrate that for linear codes of fixed block length and dimension, the highest embedding efficiency (the smallest average distance to code) is not necessarily achieved using codes with the smallest covering radius. Nevertheless, we prove that with increasing code length and fixed rate (i.e., fixed relative message length), the relative average distance to code and the relative covering radius coincide. Finally, we describe several specific examples of q-ary linear codes with q matched to the embedding operation and experimentally demonstrate the improvement in steganographic security when incorporating the coding methods to digital image steganography.

1 Introduction

Steganography is the art of undetectable communication. It was originally formalized by Simmons [1] as the prisoners' problem. Alice and Bob are prisoners in separate cells who want to develop an escape plan. Their communication is monitored by a warden. Alice and Bob resort to steganography and hide the details of the escape plot in cover objects, such as digital images, by slightly modifying them. Their goal is to not raise the warden's suspicion. In the simplest case, the warden is passive in that he just observes the traffic without modifying the messages in any way.

The main requirement of any steganographic technique is *undetectability*—the warden should not be able to distinguish between *cover* and *stego objects* (cover embedded with data) with success better than random guessing. A formal definition of steganographic security was given by Cachin [2]. The detectability of data hidden in a stego object is influenced by many factors, such as the choice of the cover object, the selection rule used to identify individual elements of the cover that could be modified during embedding, the type of embedding operation that modifies the cover elements, and the number of embedding changes (directly related to the secret message length). Assuming two embedding methods share the same source of cover objects, the same selection rule and embedding operation,

J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 282–296, 2007.
© Springer-Verlag Berlin Heidelberg 2007

the one that introduces fewer embedding changes will be less detectable as it decreases the chance that any statistics used by the warden will be sufficiently disturbed to mount a successful steganalysis attack. The expected number of random message bits embedded per one embedding change is called *embedding efficiency*. This concept has been introduced by Westfeld [3] and has since been accepted as an important attribute of steganographic schemes [4, 5].

In 1998, Crandall [6] and Bierbrauer [7, page 195–197] showed that embedding efficiency of steganographic schemes can be improved by applying covering codes to the embedding process. This fact has been later independently rediscovered by van Dijk et al. [8] and Galland et al. [9]. In particular, a linear code can be used to construct an embedding scheme[1] whose embedding capacity is the code redundancy, while the covering radius corresponds to the maximal number of embedding changes necessary for embedding any message.

In this paper, we first show that the *expected* number of embedding changes, which is directly related to the concept of embedding efficiency as used in current steganographic literature, corresponds to the *average distance to code* rather than the covering radius. Moreover, we show that in the class of linear codes of fixed length and dimension the highest embedding efficiency may not always be attained for a code with the smallest covering radius. However, with increasing code length and fixed rate (i.e., fixed relative message length), the relative covering radius and the relative distance to code asymptotically coincide.

In Section 2, we review selected known facts about embedding schemes realized using q-ary linear codes and state bounds on embedding efficiency. In Section 3, we study the properties of the average distance to code. Examples of specific coding schemes that can substantially improve the embedding efficiency of steganographic schemes are given in Section 4, where we experimentally demonstrate the benefit of using the proposed coding techniques for steganography. The paper is concluded in Section 5.

2 Covering Codes in Steganography

In this section, we briefly review some known results about steganographic schemes and covering codes including bounds on achievable embedding efficiency. We do so for a rather general definition of an embedding scheme in which message symbols from some finite field (rather than bits) are embedded at each pixel. The reason for this more general approach will become clear in Section 4 when we discuss the importance of ternary codes for steganography. Throughout the text, boldface symbols stand for vectors or matrices and the calligraphic font is used for sets. Italicized text highlights definitions of new concepts.

We will assume that the *cover image* $\mathbf{X}$ is an element of $\mathcal{G}^n$, where $\mathcal{G}$ is the set of all possible pixel values. For example, in steganography using 8-bit grayscale digital images, $\mathcal{G}$ is the set of all integers in the range $[0, 255]$ and n is the number of pixels. Data embedding consists of modifying the values of selected pixels so

[1] In steganographic literature, such embedding schemes realized using linear codes are called *matrix embedding* [6, 3, 10].