Chapter X
Computational Aspects of Digital Steganography*

Maciej Liśkiewicz
Institute of Theoretical Computer Science, University of Lübeck, Germany

Ulrich Wölfel
Federal Office for Information Security (BSI), Germany

ABSTRACT

This chapter provides an overview, based on current research, on theoretical aspects of digital steganography—a relatively new field of computer science that deals with hiding secret data in unsuspicious cover media. We focus on formal analysis of security of steganographic systems from a computational complexity point of view and provide models of secure systems that make realistic assumptions of limited computational resources of involved parties. This allows us to look at steganographic secrecy based on reasonable complexity assumptions similar to ones commonly accepted in modern cryptography. In this chapter we expand the analyses of stego-systems beyond security aspects, which practitioners find difficult to implement (if not impossible to realize), to the question why *such systems are so difficult to implement and what makes these systems different from practically used ones.*

INTRODUCTION

Digital steganography aims at hiding secret data in unsuspicious cover media. The field has been actively investigated since the early 1990s. In most cases, the cover media chosen are multimedia data, such as images, audio, or video. For this reason, many impulses in steganography research come from statistics, signal and image processing with a focus on heuristic algorithms for hiding, and experimental methods for detecting hidden information. In the early years of scientific investigations this focus caused a lack of theoretical analyses on fundamental properties of steganographic systems, namely capacity, security, and tractability.

Starting in the late 1990s, theoretical analyses of steganography began to be conducted, concerned primarily with security and capacity aspects, which unfortunately have mostly been neglected by practitioners in the field. This is in part due to unrealistic assumptions and simplifications that have been made in order to cope with the difficult problem of formal modeling of steganography. In the case of capacity—besides some superficial practical analyses—a good understanding from an information-theoretic point of view has been achieved (see e.g., the seminal paper by Moulin & O'Sullivan, 2003), but there is still a lack of some guiding theory describing any information-hiding system achieving maximum capacity. Moreover, the focus of the mentioned study was on active adversaries, a scenario that better suits digital watermarking more than steganography, where typically passive adversaries are considered. Because of this we view capacity as a topic that will have to receive renewed attention in the future and thus leave it out of our current study. Regarding security, the focus of theoretical investigations so far has been on the maximum achievable security in different attack scenarios, which has led to interesting insights, but not yet to more secure stego-systems, as practical implementations of such systems prove to be difficult, if not unfeasible, in terms of computational complexity. So the situation of steganography seems in some respects similar to that of cryptography some 50 years ago, where the existence of secure systems, such as the one-time pad, was known, but these could not be practically implemented.

When looking at stego-systems that have been practically implemented, however, one finds that the time span from announcement as the latest and greatest system to the first successful detection by steganalysis often lasts only some two or three years. Because this situation does not appear to change in spite of all efforts by the steganography community, the question arises whether bringing reliable security into real-life systems can be achieved at all. Using experience and methods from cryptography and theoretical computer science one can expect to find answers to the important question if the field of steganography can reach levels of security that are available today in cryptography.

This chapter provides an overview of previous work on theoretical analyses of steganography, in which the central question concerns the security of given systems. Several definitions of secure steganography have been proposed in the literature, but most of them make the rather unrealistic assumptions of unlimited computational power for the parties involved and complete knowledge of the cover and stego-text distributions. We focus on formal models of secure systems that make more realistic assumptions of limited computational resources and restricted access to cover-text distributions. This allows us to look at steganographic secrecy from a computational complexity point of view and to obtain provable security based on widely accepted complexity assumptions, as, for example, the existence of one-way functions. Such security evidence is commonly accepted in the field of cryptography.

We will additionally look at the tractability of secure stego-systems—a topic whose examination has only recently started (Hundt, Liśkiewicz, & Wölfel, 2006). For the tractability analysis we consider that not only the adversary, but also both parties that use steganography are restricted to working in polynomial time. This is an important assumption in the context of real-life stego-systems that is, unfortunately, often forgotten in theoretical constructions. In such systems the complexity of sampling typically plays a crucial role. Thus, the analysis of a stego-system's tractability is an important tool that complements theoretical security analyses and will likely be a major subject in future research. It also helps to divide known stego-systems into categories, yielding a more systematic view on the possibilities of different approaches to steganography. So, in this second part we will expand the analyses presented in this chapter beyond security analyses