Chapter XII
Steganalysis: Trends and Challenges

Hafiz Malik
University of Michigan–Dearborn, USA

Rajarathnam Chandramouli
Stevens Institute of Technology, USA

K. P. Subbalakshmi
Stevens Institute of Technology, USA

ABSTRACT

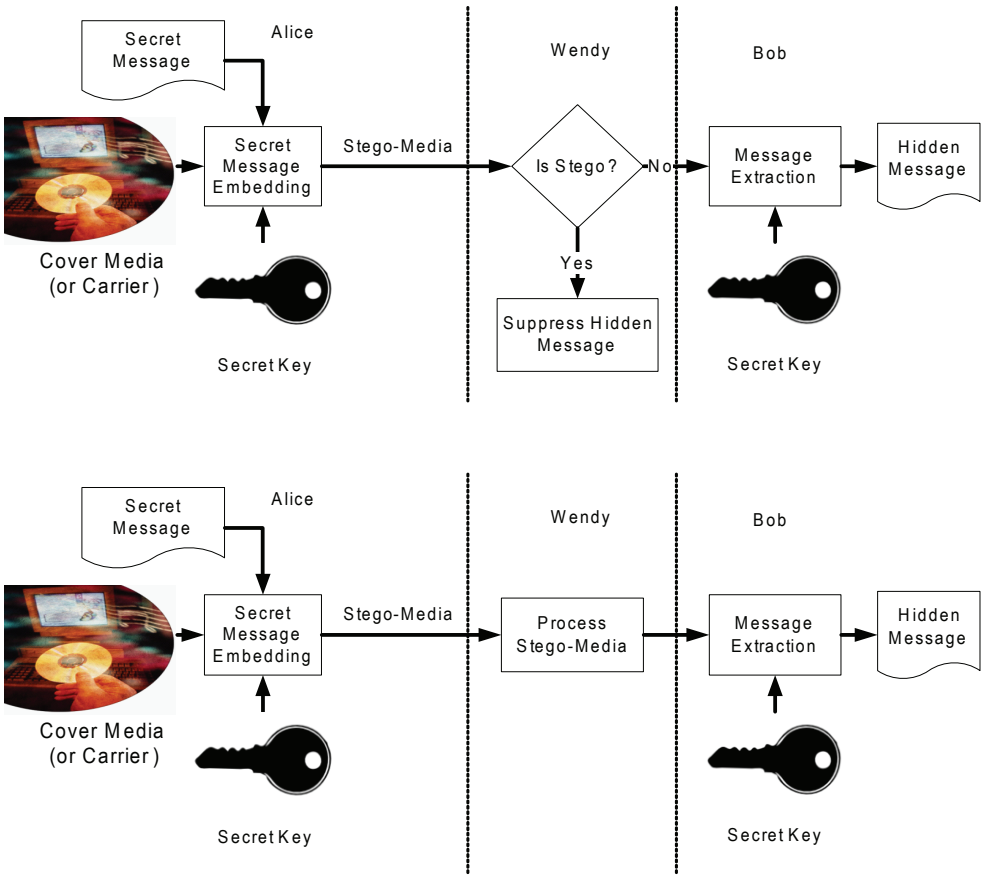
In this chapter we provide a detailed overview of the state of the art in steganalysis. Performance of some steganalysis techniques are compared based on critical parameters such as the hidden message detection probability, accuracy of the estimated hidden message length and secret key, and so forth. We also provide an overview of some shareware/freeware steganographic tools. Some open problems in steganalysis are described.

INTRODUCTION

Steganography deals with hiding information into a cover (host or original) signal such that no one other than the intended recipient can detect or extract the hidden message. The steganographic encoder embeds a message into the cover signal using a secret key such that perceptual and other distortion constraints are satisfied. A statistical dissimilarity measure between the cover and the stego-signal is generally used to measure the security of a given steganographic method (Cachin, 1998; Chandramouli & Memon, 2003; Zollner et al., 1998).

Steganography can be modeled as a prisoner's problem (Simmons, 1984). For example, consider two prisoners, Alice and Bob, who want to secretly exchange information regarding their escape

Figure 1. Secret key steganography in the presence of a passive warden (top) and an active warden (bottom)



plan. However, the warden, Wendy, examines every communication between Alice and Bob and punishes them if steganographic covert communication is detected. In a standard steganographic framework, Alice sends a secrete message, ***M***, to Bob by embedding her secret message into the cover signal, **S**, to obtain the stego-signal **X**. Alice then sends **X** to Bob using a public channel. The warden, who examines the communication channel between Alice and Bob, can be passive or active. A passive warden attempts only to detect a steganographic covert channel. An active warden, on the other hand, deliberately alters every signal exchanged between Alice and Bob, to foil any covert communication between them. The allowable distortion the warden can introduce in the stego-signal depends on the underlying model and the cover signal used. Figure 1 illustrates secret key steganography for active and passive warden scenarios.

Clearly, Alice and Bob attempt to design the steganographic channel (encoder, secret key, and decoder) such that the warden is unable to distinguish in any sense (statistically as well as perceptually) between the cover signal and the stego-signal. On the other hand, Wendy tries to