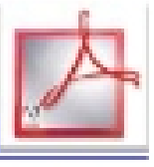
Unseen: An Overview of Steganography and Presentation of Associated Java Application C-Hide

Jessica Codr, jmc5@cec.wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 

ABSTRACT:

People have desired to keep certain sensitive communications secret for thousands of years. In our new age of digital media and internet communications, this need often seems even more pressing. This paper presents general information about steganography, the art of data hiding. The paper provides an overview of steganography, general forms of steganography, specific steganographic methods, and recent developments in the field. The information presented in this paper is also applied to a program developed by the author, and some sample runs of the program are presented.

KEYWORDS:

steganography, steganalysis, data hiding, data security, data embedding, stego-objects, watermarking, secret communications, secret messages, hidden messages, hidden channel, covert channel, LSB alterations

---

TABLE OF CONTENTS:

---

1. Introduction and Overview

Have you ever set up code words for talking with your friends so that you could convey something to them without those nearby knowing you were doing so? Perhaps you established a code word or signal to be used at a party to indicate you were bored and ready to go home or, if you are more devious, established a system to cheat at a card game. If you have done anything like this, you have used steganography. Steganography is the art of hiding a message so that only the intended recipient knows it is there. In the most widely cited description of steganography, two prisoners, Alice and Bob, are trying to plan a jail escape while under the watchful eye of Warden Wendy. Wendy will not tolerate suspicious behavior, such as passing notes that are clearly encrypted. So Alice and Bob communicate such that it seems they are talking about something harmless (such as the weather or their families) when they are actually planning an escape (cited in [Bergmair06] from [Simmons84]). From this simple theoretical example, many steganographic techniques and practices have spawned and have helped improve data security in the real world.

1.1. Steganography Versus Cryptology

In the "real world", steganography, like cryptology, is intended to add a layer of security to communications so that pesky eavesdroppers don't know what Alice is saying to Bob. However, unlike cryptology, steganography is not meant to obscure the message, but to obscure the fact that there is a message at all. Attacks against cryptography take what is known to be an encrypted message and attempt to decrypt the message. Attacks against steganography take what seems to be an ordinary image, text, multimedia file, or other document and determine whether or not there is another message hidden within.

Steganography and cryptography are strongest when combined. A message sent in secret (steganography) in an encrypted form (cryptography) is much more secure than a "plain text" message sent by secret means or a clearly sent encrypted message. There are some cases in which steganography can take the place of cryptography; for instance German bans on encrypting radio communications were recently countered by applying steganography to radio communications [Westfeld06]. Generally, however, steganography "is not intended to replace cryptography but supplement it" [Johnson95].

Steganography, like cryptography, also has its own set of terminology. In steganography, cover refers to the media in which a message is hidden. Covertexts and coverimages are texts and images used as covers, respectively. A stego-object is the cover with the secret message embedded in it.

Steganography also has an additional branch known as watermarking, which is a means of hiding data within a cover in order to mark that cover and prevent duplication or unauthorized use. Whereas pure steganography hides data completely, watermarking is meant to be detectable but unalterable. Watermarks can be applied to text documents containing intellectual property, art work, music files, movies, or anything that an author or owner does not want others to use or copy without proper authorization. The watermark verifies a media file

owner's right to use it. If the watermark can be removed, systems that check watermarks to see if the user is authorized to have the media just see an ordinary file with no protection and allow the owner to use it. Thus, watermarks must be "hidden" so as not to damage the media and must be detectable by an outside system, but not removable [Lu05][Katzenbeisser00]. This discussion of the purpose of watermarking leads into a more general discussion of the goals of strong steganography, presented in the next subsection.

1.2. Characteristics of Strong Steganography

Though steganography's most obvious goal is to hide data, there are several other related goals used to judge a method's steganographic strength. These include capacity (how much data can be hidden), invisibility (inability for humans to detect a distortion in the stego-object), undetectability (inability for a computer to use statistics or other computational methods to differentiate between covers and stego-objects), robustness (message's ability to persist despite compression or other common modifications), tamper resistance (message's ability to persist despite active measures to destroy it), and signal to noise ratio (how much data is encoded versus how much unrelated data is encoded). The three main components, which work in opposition to one another, are capacity, undetectability, and robustness. Increasing one of these causes the others to decrease; thus, no steganographic technique can be perfectly undetectable and robust and have maximum capacity [Salomon03]. In most cases, capacity is not as important as the other two, and whereas watermarking favors robustness most strongly, general steganography considers undetectability the most important [Salomon03]. A summary of the properties of good steganography is presented in figure 1 below.

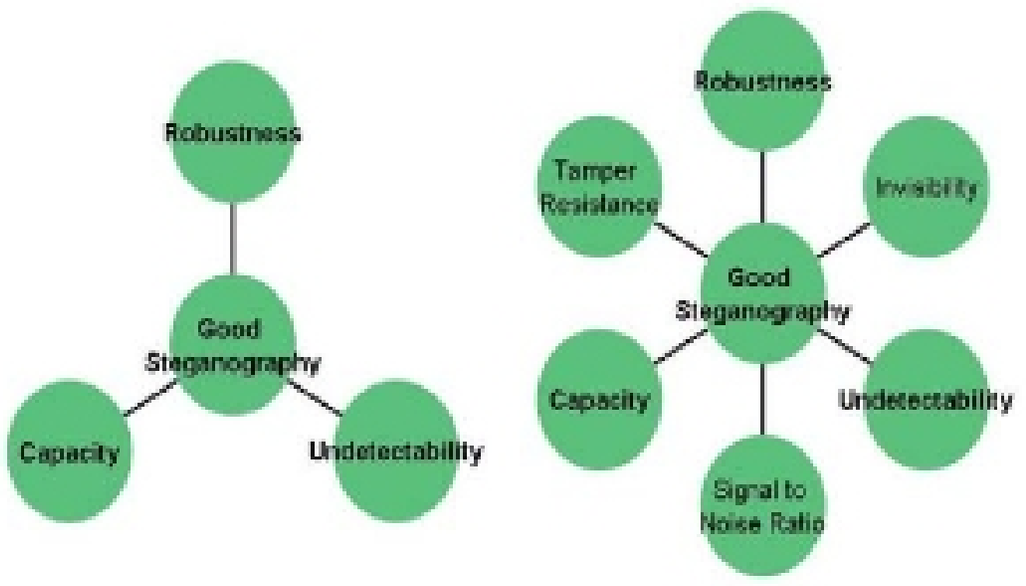


Figure 1 Properties of Good Steganography: the three most simple opposed properties (left) and a display of all six key properties (right)

As some of these properties indicate, steganography seeks to be strong against steganalysis, which is the attempt to uncover the hidden message within a stego-ojbect. Figure 2 summarizes the steganalysis process. Steganalysis can combat steganography in ways other than detecting the message, but determining how to uncover the message is the main problem steganalysis seeks to solve.