Chapter XXIII
Digital Steganography Based on Genetic Algorithm

Frank Y. Shih
New Jersey Institute of Technology, USA

Yi-Ta Wu
Industrial Technology Research Institute, Taiwan

ABSTRACT

Steganography is the art of hiding secret data inside other innocent media file. Steganalysis is the process of detecting hidden data which are crested using steganography. Steganalysis detects stego-images by analyzing various image features between stego-images and cover-images. Therefore, we need to have a system that develops more critical stego-images from which steganalysis cannot detect them. In this chapter, we present a Genetic algorithm-(GA) based method for breaking steganalytic systems. The emphasis is shifted from traditionally avoiding the change of statistic features to artificially counterfeiting the statistic features. Our idea is based on the following: in order to manipulate the statistic features for breaking the inspection of steganalytic systems, the GA-based approach is adopted to counterfeit several stego-images (candidates) until one of them can break the inspection of steganalytic systems.

INTRODUCTION

As digital information and data are transmitted more often than ever over the Internet, the technology of protecting and securing the sensitive messages needs to be discovered and developed. Digital steganography is the art and science of hiding information into covert channels, so as to conceal the information and prevent the detection of the hidden message. Covert channel is a genre of information security research, which generally is not a major player, but has been an extremely active topic in the academia, industry and government domains for the past 30 years.

The data hiding in steganography is intended in such a way that only the receiver knows the existence of the secret data. It is different from cryptography which encodes messages by scram-
bling, so nobody can read it without the specific key. Another technique, digital watermarking, is concerned with issues related to copyright protection and intellectual property (Shih, 2007; Cox, 2001; Wu, 2004); therefore, a watermark usually contains the information pertaining to the carrier and the owner. The well-known steganographic methods include covert channel, invisible ink, microdot, and spread-spectrum communication (Kahn, 1996; Norman, 1973).

There is a classic example to explain steganography illustrated by Simmons in 1983, which is called the prisoners’ problem (Simmons, 1984). There are two prisoners, called Alice and Bob, who are planning to escape from jail. All the communications between them are monitored by a warden, called Wendy. So to escape from the eyes of Wendy, the two prisoners must communicate with each other by a cover on their messages. They create a stego-object, which is sent through the public channel to be observed by Wendy who can freely inspect it. Wendy’s observation is classified into two types, called active and passive. In an active state, Wendy can modify the message by a little thwart any hidden communication, but the hidden message may be survived under Wendy’s modification. In a passive state, Wendy can examine all the messages between Alice and Bob and does not change any message but finds whether they have hidden messages encoded into them. Figure 1 shows an example of steganography, where (a) is a cover-image, (b) is the secret image containing NJIT logo, and (c) is the stego-image after the least-significant-bit (LSB) embedding of the secret image into the cover-image.

Modern techniques in steganography have far-more-powerful tools. Many software tools allow a paranoid sender to embed messages in digitized information, typically audio, video or still image files that were sent to a recipient. Although steganography has attracted great interests from the military and governmental organizations, there is even a big interest shown from commercial companies to safeguard their information from piracy. Today, steganography