Hardware Based Steganalysis

Kang Sun, Xuezeng Pan, Jimin Wang, and Lingdi Ping

College of Computer Science and Technology, Zhejiang University, Hangzhou, 310027, China.
swankong@126.com

Summary. Steganalysis is the reverse process of steganography. The goal of ste- ganalysis is to detect, as reliably as possible, the presence of hidden data. Software-based steganalytic systems often fail to keep up with high-speed network through- puts. In this chapter, we present the design of a system that automatically detects ste-ginformation in real-time. In this system, RS steganalytic algorithm is parallel implemented with a three-stage pipeline based on FPGA. Experiment results show that this system can achieve very high throughputs (2.5Gbps) and deal with a far larger amount of traffic than software-based approaches.

Key words: steganalysis, FPGA, RS, steganography, reconfigurable computing

23.1 Introduction

Steganography is the art of secret communication. We can use digital images, videos, audios, and other computer files that contain irrelevant or redundant information as covers or carriers to hide secret messages [1]. Steganography has made positive contributions to the field of information security. Many steganographic software and watermarking algorithms can be downloaded freely from the Internet. People might use these tools to communicate secretly with each other. However, it can also be employed by criminals - terrorists can use steganography to transmit secret messages on internet or launch terrorist at- tacks.

Steganalysis is the reverse process of steganography. The goal of steganal- ysis is to detect, as reliably as possible, the presence of hidden data. On-line real time detection is an effective way to detect hidden data transmitted on internet. But due to huge network traffic, the throughput of existing solutions cannot satisfy the requirements of on-line detection.

In this chapter, we place a strong focus on high throughput implementa- tion of steganalytic algorithm. The architecture of an FPGA based LSB steganography detector is introduced. It uses RS [2] steganalytic algorithm to
detect information hidden in color or gray-scale images. The potential advantages of using FPGA to implement steganalytic algorithm include:

**Algorithm Agility** This term refers to the switching of steganalytic algorithms during operation. In a real network environment, the hidden messages may be embedded in the media by various steganographic programs. It requires the detector can deal with multiple steganographic technologies, and future extensions should be possible. Whereas algorithm agility is costly with traditional hardware, FPGAs can be reprogrammed on-the-fly. And it is perceivable that fielded devices are upgraded with a new steganalytic algorithm which does not exist (or was not standardized) at design time.

**Throughput** Although typically slower than ASIC implementations, FPGA implementations have the potential of running substantially faster than software implementations.

**Cost Efficiency** The time and costs for developing an FPGA implementation of a given algorithm are much lower than for an ASIC implementation. (However, for high-volume applications, ASIC solutions usually become the more cost-efficient choice.)

### 23.1.1 Our Contribution

The primary contribution of our work has been to first implement RS steganalytic algorithm on reconfigurable hardware. In order to achieve high throughput, we propose a completely new reconfigurable steganography detector architecture in which the RS steganalytic algorithm is implemented in full parallel mode. Some critical operations in the algorithm are carried out by lookup table operation to accelerate the processing speed. To the best of our knowledge, there’s no hardware implementation of steganalytic algorithm up to now.

### 23.1.2 Organization of the Chapter

In the rest of this chapter, Section 23.2 provides the background of our work in term of an introduction to the RS steganalytic algorithm and recent previous work on acceleration of LSB steganography detection based on various technologies. Section 23.3 contain the details of the system architecture. Section 23.4 presents the implementation results. At last, in Section 23.5, we conclude the whole chapter.

### 23.2 Background and Related Work

#### 23.2.1 RS Steganalytic Algorithm

RS steganalytic algorithm is proposed by Fridrich, et al [2]-[4]. The stego-detection method starts with dividing the image into disjoint groups of $n$