Chapter 19
A Comparative Review of Various Machine Learning Approaches for Improving the Performance of Stego Anomaly Detection

Hemalatha Jeyaprakash
Thiagarajar College of Engineering, India

KavithaDevi M. K.
Thiagarajar College of Engineering, India

Geetha S.
VIT University, India

ABSTRACT

In recent years, steganalyzers are intelligently detecting the stego images with high detection rate using high dimensional cover representation. And so the steganographers are working towards this issue to protect the cover element dependency and to protect the detection of hiding secret messages. Any steganalysis algorithm may achieve its success in two ways: 1) extracting the most sensitive features to expose the footprints of message hiding; 2) designing or building an effective classifier engine to favorably detect the stego images through learning all the stego sensitive features. In this chapter, the authors improve the stego anomaly detection using the second approach. This chapter presents a comparative review of application of the machine learning tools for steganalysis problem and recommends the best classifier that produces a superior detection rate.

DOI: 10.4018/978-1-5225-4100-4.ch019

INTRODUCTION

Steganographers aim is to conceal some undisclosed message inside an innocuous cover file known as digital images, and later it could be send via an unconfident channel as a stego file. In contrary, the anomaly detection called steganalysis aims to detect the presence of steganogram. In the last two decades, both the steganography and steganalysis experienced a precipitous development. There are three reasons are there why the research on steganalysis has attained a greater attention. Originally, sensing the occurrence of hidden messages, that can be castoff as a clandestine communication among terrorists or illegal groups. Then the greater achievement of steganalysis aids to increase the security of information hiding/steganography and watermarking. Steganalysis finds to be helpful in computer forensics, cyber warfare, criminal activities and etc. At last, it stimulates the researchers to construct the enhanced numerical model for multimedia which leads to the great successful application on other fields such as digital forensics. In the recent works, the best detectors are known to be the supervised learning for detecting the steganographic methods. In this chapter, we propose to study several recent machine learning algorithms available for steganalysis of images. The objective of this chapter is to present the efficiency of using machine learning algorithms in detecting stego objects.

Since many image formats are hugely available on the communication networks, JPEG images are the utmost frequently castoff images for data hiding purpose. The primarily steganographic procedures opted for the JPEG format was JSteg (Upham, n.d.), Outguess (Provos et al., 2001), F5 (Westfeld et al. 2001), Steghide (Hetzl et al., 2005) followed by Model-based Steganography (Sallee et al., 2005). Thereby Outguess and JSTEG obviously alters the DCT coefficient histogram, whereas the ancient attacks purely depended on first-order statistics of DCT (Discrete Cosine Transform) coefficients (Zhang et al., 2003). After, substantially more promising detectors were designed as possibility ratio trials with an id of well DCT coefficient cover models (Thai et al., 2015; Hastie et al, 2009).

The promising detectors for F5 and nsF5 (Fridrich et al., 2007) along with for Steghide, Model-Based Steganography are presently designed as classifiers skilled on features since DCT- quantized coefficients, the JRM (JPEG Rich Model) (Kodovský et al., 2012). When the features are mined from the residuals in the spatial domain, namely JPEG – phase – aware features, J-UNIWARD and UED (Guo et. 2012; Lerch-Hostalot et al., 2016) are perfectly detected by using such a feature-based model. Example of such features is GFR (Song et al., 2015), PHARM (Holub et al., 2015), DCTR (Holub et al., 2015) and etc. The concept of such a design is the JPEG phase notion, which is, the residual location in the 8*8 grid of JPEG. By rending the informations gathered from the residuals by their segment, further promising stego detector can be built.

Steganographic Methods

- **Steghide:** The practical LSB implementation for images and audios are dome by Steghide. It may modify the original algorithm by adds a graph to lessen the amount of pixel modification. To enhance the hiding security, the hidden messages are properly encrypted and compressed before the message is embedded. Following that pseudo-random sequence is generated equation the passphrase as seed. This corresponding sequence belongs to the image pixels and the LSB bits are modified the sequence message bits. To enhance the visual imperceptibility, the LBS bit that