Textural Features Based Universal Steganalysis

Bin Li[a,b], Jiwu Huang[*a], Yun Q. Shi[b]

[a]Guangdong Key Laboratory of Information Security Technology
Sun Yat-sen University, Guangzhou 510275, P. R. China
[b]Department of Electrical and Computer Engineering
New Jersey Institute of Technology, Newark, NJ 07102, USA

ABSTRACT

This paper takes the task of image steganalysis as a texture classification problem. The impact of steganography to an image is viewed as the alteration of image texture in a fine scale. Specifically, stochastic textures are more likely to appear in a stego image than in a cover image from our observation and analysis. By developing a feature extraction technique previously used in texture classification, we propose a set of universal steganalytic features, which are extracted from the normalized histograms of the local linear transform coefficients of an image. Extensive experiments are conducted to make comparison of our proposed feature set with some existing universal steganalytic feature sets on gray-scale images by using Fisher Linear Discriminant (FLD). Some classical non-adaptive spatial domain steganographic algorithms, as well as some newly presented adaptive spatial domain steganographic algorithms that have never been reported to be broken by any universal steganalytic algorithm, are used for benchmarking. We also report the detection performance on JPEG steganography and JPEG2000 steganography. The comparative experimental results show that our proposed feature set is very effective on a hybrid image database.

Keywords: steganalysis, steganography, texture classification, local linear transform

1. INTRODUCTION

Recent years witness growing interests in the field of digital steganography and steganalysis[1,2,3]. Steganography refers to the technology of embedding secret data into cover media without drawing suspicion. The media carrying the secret message, often called stego, can be selected from various formats, such as digital image, audio, video, text, etc. On the other side of the game, steganalysis aims to break the steganography by getting a better result than random guessing on classifying cover media and stego media. The state-of-the-art steganalytic schemes can be divided into two categories. One is called specific steganalysis[4-6], which aims to break a specific steganographic algorithm. The other category gets its name by universal steganalysis or blind steganalysis[7-16]. Universal steganalysis is more attractive in practical use because of its ability to work with many steganographic algorithms and even generalize to unknown algorithms. We focus our work on universal steganalysis for digital images in this paper.

Generally, most of the universal steganalytic algorithms are based on the techniques of pattern classification[17]. Two or three major steps may be involved. The first step is feature extraction or called feature formulation. The "universal" property is mainly contributed by good features, which usually change along with the size of embedding payload. Thus the larger embedding payload size, the easier the classification. The second and optional step is feature selection, which is used to identify a subset of the features for best discriminating cover and stego media. The final step is coming up with a supervised-learning algorithm to construct a feature-based classifier.

Effective steganalytic features can reflect statistical differences between cover and stego media. Avcibas *et al.*[7] proposed to use several image quality metrics as features to describe image quality degradation introduced by data hiding. Later, the authors presented a steganalytic scheme with features measured by binary similarity to characterize the correlation between bit planes[8]. Farid's feature set[9] and Lyu *et al.*'s [10] are collected from the probability density function (PDF) moments of quadrature mirror filter (QMF) based decomposition and the PDF moments of cross-subband prediction errors. By using denoising techniques, Holotyak *et al.*[11] and Goljan *et al.*[12] estimated stego noise (which we usually defined as the difference between a cover image and its stego version) in the finest decomposition level of

* Send correspondence to Jiwu Huang. E-mail: isshjw@mail.sysu.edu.cn. Phone: (86)20-3933-2715. Fax: (86)20-8411-3673.

Security, Forensics, Steganography, and Watermarking of Multimedia Contents X
edited by Edward J. Delp III, Ping Wah Wong, Jana Dittmann, Nasir D. Memon
Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 6819, 681912, © 2008 SPIE-IS&T · 0277-786X/08/$18