Signal Processing 98 (2014) 263–274

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Statistical detection of data hidden in least significant bits of clipped images

Thanh Hai Thai*, Florent Retraint, Rémi Cogranne[1]

ICD - LM2S - Université de Technologie de Troyes - UMR STMR CNRS, 12, rue Marie Curie - CS 42060 - 10004 Troyes cedex - France

ARTICLE INFO

Article history:
Received 17 June 2013
Received in revised form
18 October 2013
Accepted 21 November 2013
Available online 1 December 2013

Keywords:
Hypothesis testing
Natural image model
Optimal detection
Steganalysis
Information forensics

ABSTRACT

This paper studies the statistical detection of data hidden in the Least Significant Bits (LSB) plan of natural clipped images using the hypothesis testing theory. The main contributions are the following. First, this paper proposes to exploit the heteroscedastic noise model. This model, characterized by only two parameters, explicitly provides the noise variance as a function of pixel expectation. Using this model enhances the noise variance estimation and hence, allows the improving of detection performance of the ensuing test. Second, this paper introduces the clipped phenomenon caused by the limited dynamic range of the imaging device. Overexposed and underexposed pixels are statistically modeled and specifically taken into account to allow the inspecting of images with clipped pixels. While existing methods in the literature fail when the data is embedded in clipped images, the proposed detector still ensures a high detection performance. The statistical properties of the proposed GLRT are analytically established showing that this test is a Constant False Alarm Rate detector: it guarantees a prescribed false alarm probability.

1. Introduction

Steganography is the art and science of hiding communication. It aims to embed a secret message into host objects, or cover objects, to create so-called stego-objects. The stego-objects are then transmitted to the receiver via an insecure channel without raising suspicion of an adversary. The secret message can be retrieved by the receiver who knows in advance the hiding scheme and the secret key. In nowadays digital world, multimedia objects such as images, videos, and audios are often used as cover objects for steganography [4,11,19]. The communication channel provided by computer and network technologies helps to transmit the stego-objects easily and inconspicuously. Generally, steganographic techniques must satisfy two followings universal requirements [11]:

- The secret message must remain unchanged during or after the embedding process.
- The stego-object must remain unchanged or almost unchanged to the human eye.

The art of detecting hidden messages embedded in cover objects is called steganalysis. In the past decades, steganalysis has received a great attention from law enforcement agencies and media because the concept of steganography has been misused by anti-social elements and criminals over the internet [33]. Despite its intrinsic difficulty, the steganalysis is being developed and applied in many domains such as computer security, cyber warfare or national defence, to collect sufficient evidence about the

* Corresponding author. Tel.: +33 626300670.
E-mail addresses: thanh_hai.thai@utt.fr, thanhhai6587@gmail.com (T.H. Thai).

[1] With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission – Directorate-General Home Affairs (2centre.eu project). Research partially funded by Troyes University of Technology (UTT) strategic program COLUMBO.

0165-1684/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2013.11.027

presence of embedded message and to break the security of its carrier; see [33] and therein references for a survey of the methods available in the literature.

1.1. *State of the art*

The paper concerns the image-based steganography and focuses on the popular technique of hiding information in the Least Significant Bit (LSB) of the cover image. Only the LSB replacement technique is studied. It is probably the oldest embedding technique in digital steganography. In fact, this method is simple, easy to implement and is used in about 70% of available steganographic software on the Internet [22]. In addition, the LSB replacement inspires the majority of other steganographic methods. Understanding the LSB replacement mechanism is a good starting point before addressing more complex data hiding schemes.

Steganalysis methods of LSB replacement can be divided into four categories:

1. Structural detectors exploit all combinatorial measures of the artificial dependence between sample differences and the parity structure of the LSB replacement in order to estimate the secret message length. Some representatives in this category are the Regular-Singular (RS) [21], the Sample Pair Analysis (SPA) [13], and the triple/quadruple [26].
2. Weighted Stego-Image (WS) detectors [20,27] provide a computationally efficient estimate for the embedding rate of LSB replacement steganography. The key idea of WS is that the embedding rate can be estimated via the weight that minimizes the distance between the weighted stego image and the cover image. In contrast to structural detectors, the WS ones are mathematically better founded and have left much space for improvement of designing a more accurate and reliable detector.
3. Statistical detectors [5,8,9,12,14,30,46] consider cover image pixels as realizations of random variables and exploit artifacts resulting from changes of their statistical properties in stego-images due to message embedding. These detectors provide a formal view on the information hiding problem by formulating it in the framework of hypothesis testing theory and analytically expressing the test performance.
4. Universal or blind detectors [22,28,34,40,44] employ machine learning methods based on a set of selected informative features (e.g. image quality metrics, binary similarity metrics, DCT features, higher-order statistics of wavelet coefficients) to design an accurate classifier. Universal blind detectors are important because of their flexibility and ability to detect any steganographic scheme regardless of the embedding domain [33].

1.2. *Limitations of previous approaches*

In an operational context, for instance a steganalysis tool for law enforcement or intelligence agencies, the design of an accurate detector might not be sufficient. The most important and challenging problem is to provide a detector with analytically predictable results in order to guarantee a prescribed false alarm probability.

Both structural and WS detectors can provide overall acceptable detection performance. However, because these ad hoc detectors have a limited exploitation of image model and statistical methods, their performance remains analytically unestablished. It is only evaluated on large databases.

Besides, as in all applications of machine learning, the main difficulties for blind detectors are the choice of appropriate feature set and the analytic establishment of detection performance. The latter remains an open problem in the framework of statistical learning [38]. In addition, it has been observed that blind detectors are subjected to the well-known cover source mismatch [1,34] problem. Hence one needs images from the same camera to accurately train the classifier but such information might not be available or credible in practice.

On the opposite, by formulating the detection problem in the framework of hypothesis testing theory, only the statistical detectors proposed in [5,8,9,14,46] have been designed to warrant a prescribed false alarm probability. Unfortunately, these detectors lack an accurate model reflecting the statistical properties of natural images, even though adaptive regression models have been proposed in [8,9,14]. This leads to rather inaccurate estimation of both expectation and variance of pixels due to modeling errors. Besides, none of the prior detection schemes have introduced the clipping phenomenon which is due to the imaging system limited dynamic range. It has been observed [1] that using overexposed or underexposed areas of a natural image can significantly improve the detection performance but this has never been introduced in a detector.

1.3. *Main contributions of the paper*

The approach proposed in this paper involves the theory of statistical hypothesis testing [31]. It aims to design a statistical test for the steganalysis of LSB replacement scheme in a natural raw image. The main contributions are the following:

- Far from the Additive White Gaussian Noise (AWGN) model widely used in image processing, the proposed methodology is based on the heteroscedastic noise model which describes more accurately natural images [16,17,24]. The heteroscedastic property gives the variance of a pixel as a linear function of its expected value. This property, which has not yet studied in prior detectors, is considered in this paper to reduce estimation errors on expectation and variance of pixels.
- Instead of using a local regression model [5,8,9,14,46], this paper proposes to exploit a state-of-the-art denoising method [16]. This method is used together with the heteroscedastic noise model to significantly improve the estimation of pixels expectation and variance resulting in a higher detection performance.
- The clipping phenomenon, which makes the so-called *clipped* pixels being overexposed or underexposed, is taken