Digital Investigation 9 (2013) 235–245

Contents lists available at SciVerse ScienceDirect

Digital Investigation

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

A study on the false positive rate of Stegdetect

Omed S. Khalind [a,*], Julio C. Hernandez-Castro [b], Benjamin Aziz [a]

[a] School of Computing, University of Portsmouth, Lion Terrace, Portsmouth PO1 3HE, UK
[b] School of Computing, University of Kent, UK

ARTICLE INFO

Article history:
Received 3 October 2012
Received in revised form 8 January 2013
Accepted 24 January 2013

Keywords:
Stegdetect
Steganalysis
Steganography
Digital forensics
Computer forensics
Tool analysis
False positives

ABSTRACT

In this paper we analyse Stegdetect, one of the well-known image steganalysis tools, to study its false positive rate. In doing so, we process more than 40,000 images randomly downloaded from the Internet using Google images, together with 25,000 images from the ASIRRA (Animal Species Image Recognition for Restricting Access) public corpus. The aim of this study is to help digital forensic analysts, aiming to study a large number of image files during an investigation, to better understand the capabilities and the limitations of steganalysis tools like Stegdetect. The results obtained show that the rate of false positives generated by Stegdetect depends highly on the chosen sensitivity value, and it is generally quite high. This should support the forensic expert to have better interpretation in their results, and taking the false positive rates into consideration. Additionally, we have provided a detailed statistical analysis for the obtained results to study the difference in detection between selected groups, close groups and different groups of images. This method can be applied to any steganalysis tool, which gives the analyst a better understanding of the detection results, especially when he has no prior information about the false positive rate of the tool.

1. Introduction

The word steganography is derived from two Greek words (*stegano* and *graphos*) that respectively mean covered and writing. It can be defined as the art and science of hiding secret messages in different media (images, audio, video, text, etc.) so that it can be correctly received by another party without raising suspicion by an observer (Chandramouli and Memon, 2003). The main difference between steganography and cryptography is that the former tries to hide the very existence of the information exchange, while the latter is only interested in the secrecy of the exchanged contents, not of the exchange itself.

To perform steganography we need both an embedding and an extraction process. Hiding of the message is done by embedding it into the object called the cover-object and the extraction of the message is done by feeding the stego-object (cover-object + secret message) and the key to the extraction algorithm.

Steganography has some points in common with digital watermarking, they are both part of the larger field – information hiding, but there are differences between the two. The main difference is that steganography focuses more on the imperceptibility property of the stego-object, while robustness is the main concern for digital watermarking.

1.1. Basic terminology

In this section we explain the terms we use in the rest of the paper. Secret message is the information to be hidden. Cover-object is the carrier of the secret message

* Corresponding author. Tel.: +44 7709020299.
E-mail addresses: Omed.khalind@port.ac.uk, omedsaleem@yahoo.com (O.S. Khalind), J.C.Hernandez-Castro@kent.ac.uk (J.C. Hernandez-Castro), Benjamin.Aziz@port.ac.uk (B. Aziz).

1742-2876/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.diin.2013.01.004

and could be any digital media (text, image, video, audio, etc.). Stego-object is the modified cover-object after embedding the secret message in it. Stego-algorithm is the procedure of embedding the secret message into the cover-object. Stego-key is the key used in the embedding process and is required by the receiver for the extraction process of the secret message. Steganalysis is the art and science of detecting hidden contents. A steganalyst is the one who applies steganalysis techniques for detecting hidden messages. False positives are the cases where the steganalysis tool incorrectly detects the presence of hidden content.

1.2. Steganography in images

Almost all types of digital media, where there is some sort of redundancy, could be used for steganography. Multimedia objects are considered excellent media for hiding secret messages because of the numerous formats having high degrees of redundancy (Chandramouli and Memon, 2001). Moreover, using digital images as cover-objects generally provides large embedding capacity and could easily go unnoticed. Image steganography could be applied in spatial and transform domains. In spatial domain, data embedding is done by manipulating pixel values of an image bit-by-bit, whereas in transform domain, data is embedded after transforming the image to coefficients resulting from applying a discrete cosine transform (DCT) or a discrete wavelet transform. As mentioned by Eggers et al. (2002), the final stego image should look very similar (if not identical) to the cover image and no difference should be noticed by the human eye.

1.3. Steganalysis

To illustrate steganalysis, we can imagine the scenario of Simon's prisoner problem. In this scenario, Alice and Bob are imprisoned in a jail and are monitored by a warden, Wendy. Alice and Bob want to discuss an escape plan and they can do so only if they could make their communication hidden by using a steganographic method for hiding their secret message exchanges. Now as discussed in Kharrazi et al. (2004), steganalysis can be defined as a set of methods that help Wendy to detect the existence of a secret message inside the stego-object without requiring any knowledge of the secret key and in some cases, even the algorithm of the embedding process. The absence of previous knowledge makes the steganalysis process in general very complex and challenging. In this setting, Wendy (the active warden) can sometimes actively stop and modify any message she feels uncomfortable with and in other scenarios, she is only supposed to pass messages between the two communicating parties (passive warden).

Similarly to cryptanalysis, steganalysis techniques could be classified into:

- Stego-only attack, when the steganalyst only has the stego-object for analysis.
- Known cover attack, when the steganalyst has both stego and cover objects for analysis.
- Known message attack, which is the case when the steganalyst knows the hidden message.
- Chosen stego attack, is the case when the steganalyst has both the stego-object and the embedding algorithm.
- Chosen message attack, is when the steganalyst uses a known message and steganography algorithm for future analysis after creating a stego-object.
- Finally, the known steganography attack, the steganalyst has the cover-object, steganography algorithm, and stego-object for analysis (Kessler, 2004).

1.4. Steganalysis in digital images

Despite the difficulties in defining a *normal* or a *clean* image, it is one of the requirements of statistical-based image steganalysis, in order to decide whether the image under investigation departs significantly from the *average*. To arrive to this, a number of different image characteristics are usually observed after the evaluation of many cover and stego images (Johnson and Jajodia, 1998). The idea is that the insertion of data will inevitably alter some of the image characteristics. Image steganalysis could be defined as applying any of the multiple steganalytic techniques on image files.

1.5. Stegdetect

A number of steganalysis tools (software) are available on the Web for different types of algorithms and for various digital media. In this paper we focus on Stegdetect, an automated tool developed to detect hidden content in digital images. Stegdetect can detect secret content in images embedded with a number of different steganographic tools like jsteg, jphide, outguess, f5, appendX, camouflage and alpha-channel (Provos, 2008). Moreover, it also shows the level of confidence in its detection by appending stars (*), (**), (***). A single star means low confidence and three stars mean high confidence.

Stegdetect uses statistical test for detecting hidden contents and is capable of finding the method used in the embedding process. It is a very popular tool among security and forensic practitioners and can be considered a de facto

Table 1
The rate of sensitivity independent results of 40,303 images from Google.

Sensitivity	Error	Appended	Alpha-channel	Camouflage	Skipped (false positive likely)	jsteg			f5		
						(*)	(**)	(***)	(*)	(**)	(***)
0.1–10	3.16%	0.76%	0.01%	0.02%	10.76%	0.02%	0.00%	0.00%	0.00%	0.00%	0.01%