ImageCLEF2019 Security - Forged File Discovery and Stego Image Discovery Tasks

Amilcare Gentili[1-2][0000-0002-5623-7512] and Paolo Y Gentili[3] [0000-0002-8239-8571]

[1] San Diego VA Health Care System, San Diego, CA USA
[2] University of California, San Diego, CA, USA
[3]Massachusetts Institute of Technology, Cambridge, MA, USA
agentili@ucsd.edu

Keywords: Steganalysis, steganography, digital forensics, computer forensics.

Abstract. The ImageCLEF2019 Security challenge presented the following scenario: participants are professional digital forensic examiners collaborating with the police to look for images proving a suspect's guilt. The extension and signature of some images is forged, so that they look like pdf files. Additionally, steganography software was used to hide messages within some of the images. Our method for discovering the file type of forged images was to ignore the first 4 bytes of each file, as we noticed they were identical in all files, and compare the following bytes with the HEX signatures of common file types. This simple comparison allowed us to detect all forged files and recognize their original file type. For detecting if an image contains stego information, we manipulated the images to enhance artifacts caused by the steganographic encoding algorithms. We converted the images from RGB to YCbCR, as the encoding algorithm appeared to use only the Y component, and then we generated images using the least significant bits of the Y channel. Visual observation of these enhanced images allowed us to recognize images containing a hidden message with an F1 of 0.888 and a precision of 0.908.

1 Introduction

Steganography comes from the Greek words stegos, which means roof or covered, and graphia, which means writing. Steganography is the art and science of hiding the fact that a message is being sent. The goal of steganalysis is to identify suspected files, determine whether or not they have a payload encoded in them, and, if possible, recover that payload. The ImageCLEF2019 [1] Security Task [2] had 3 subtasks corresponding to the goals of steganalysis: Task 1: Forged File Discovery, Task 2: Stego Image Discovery and Task 3: Secret Message Discovery. We participated in the first 2 tasks. Detection of file type can often be accomplished by reading the HEX signature of the file, if only the file extension is altered, but it is more challenging when the HEX signature is also modified. Detection of hidden messages in images is generally handled with

statistical analysis. Since jpg images are compressed with lossy compression algorithms, one can look for inconsistencies in the way this data has been compressed. Simple steganographic encoding algorithms will produce artifacts that are detectable. More advanced steganography algorithms try to make distortions to the image indistinguishable from the image's noise. In practice, however, this is often improperly simplified to make the modifications to the image resemble white noise as closely as possible, rather than analyzing, modeling, and then consistently emulating the actual noise characteristics of the image. Many steganographic systems simply modify the least-significant bit (LSB) of a sample; this causes the modified samples to have not only different noise profiles than unmodified samples, but also for their LSBs to have different noise profiles than their higher-order bits.

2 Methods

2.1 Forged File Discovery

For the forged file discovery task participants are presented with the hypothetical scenario in which they are a professional digital forensic examiner collaborating with the police, who suspect that there is ongoing fraud in the Central Bank. After obtaining a court order, the police gain access to a suspect's computer in the bank for the purpose of looking for images to prove the suspect's guilt. However, the police suspect that he has managed to change the extension and signature of some images, so that they look like pdf files. The goal of this challenge is to examine if an image has been forged, perform detection of altered (forged) images (both in extension and signature) and predict the actual type of the forged file.

Dataset

The data set provided for the ImageCLEF 2019 - Forged File Discovery task [2] included 2,400 files in the training set and 1,200 files in the test set. All the files had pdf extensions. In the training set 1,200 files were real pdf files, 400 were jpg, 400 were gif, and 400 were png files.

Analysis

We attempted to use the file-profiling tool DROID [3]. DROID stands for Digital Record Object Identification. It is a free software tool developed by The National Archives that can help to automatically profile a wide range of file formats. DROID was able to distinguish the files that were not forged from the files that were forged, but was not able to detect the original file type of the forged file. After opening the files with a HEX editor, we noticed that the first four bytes of each file were the same "25 50 44 46", but the next few bits were different based on file type. "25 50 44 46" are always the first 4 bytes in the HEX signature of pdf files. After observing that forged files had the first four bytes of the file HEX signature overwritten with "25 50 44 46", but the rest of the HEX signature was still intact, distinguishing original from forged files became a trivial task.

Table 1. HEX signature of different file types

File Type	Forged HEX Signature	Original HEX Signature
png	25 50 44 46 0D 0A 1A 0A	89 50 4E 47 0D 0A 1A 0A
jpg	25 50 44 46 00 10 4A 46 49 46 00 01	FF D8 FF E0 00 10 4A 46 49 46 00 01
gif	25 50 44 46 39 61	47 49 46 38 39 61
pdf		25 50 44 46 2d

We created a python script to read the first 12 bytes of each file, ignore the first 4 bytes, and compare the next few bytes with the original HEX signatures. If the 5th through 8th bytes are "0D 0A 1A 0A" the file is png, if the 5th through 12th bytes are "00 10 4A 46 49 46 00 01" the file is jpg, if the 5th and 6th bytes are "39 61" the file is gif, and otherwise the file is pdf.

2.2 Stego Image Discovery

The goal of this second challenge is to examine images and identify those that have been altered to hide steganographic content.

Dataset

The data set provided for the ImageCLEF 2019 - Stego Image Discovery task included 1,000 files in the training set and 500 files in the test set. In the training set, 500 images contained a stego message.

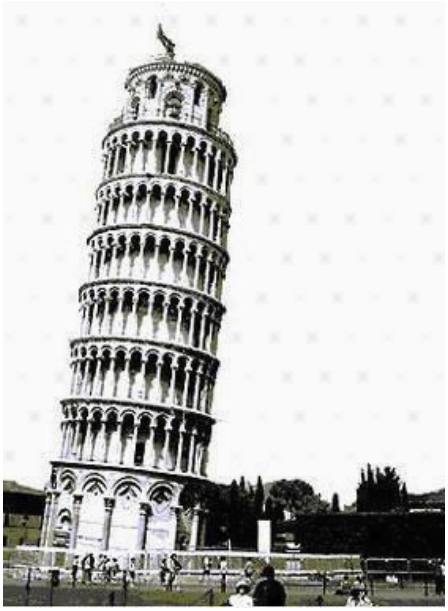

Fig. 1. 8x8 pixel squares with slightly different intensity are present with a repetitive pattern, best seen on solid background.

Analysis

Visual inspection of the images revealed repetitive patterns in the images containing hidden messages. See Figure 1.

After converting the images to YCbCR where Y is the luminance component and Cb and Cr are the blue-difference and red-difference chroma components, it was noticed that the repetitive square pattern was only present in the Y component and was particularly evident when images of the 3 least significant bits of the luminance component were created. Visual observation of the enhanced images was sufficient in most cases to distinguish original images from images containing a hidden message.

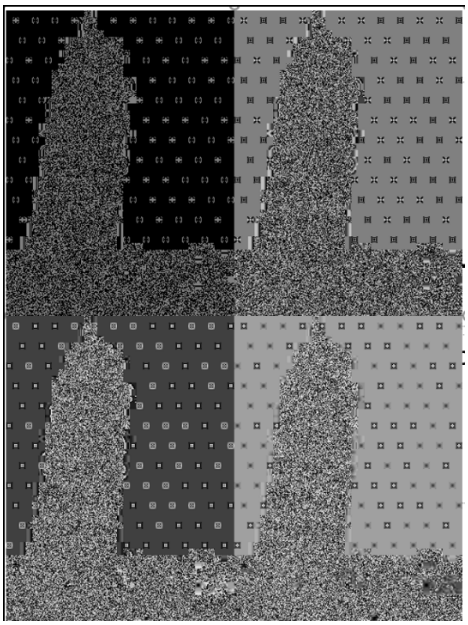

Fig. 2. Images of the least significant bits of the luminance channel enhance the pattern created by the hidden message in the image

3 Results

3.1 Forged File Discovery

File HEX signature are 5 to 12 bytes long. As the forgery of the images was fairly simple -- the extension was changed to pdf and the first four bytes of the image were changed, but the rest of the HEX signature was unchanged, detecting forged images was trivial once we noticed that only the first 4 bytes were altered in the forged files. Comparing the HEX signature of the file, after ignoring the first 4 bytes, we were able to achieve a perfect score on the first submission, with an F1 of 1.0 and a Precision of

1.0 -- skipping the first 4 bytes and comparing what was left of the file's HEX signature was sufficient to reach a perfect score.

3.2 Stego Image Discovery

Using the enhanced images based on the least significant bits of the luminance channel, it was possible to achieve good results on images with uniform color backgrounds, but it was more difficult with images with lots of fine detail. The visual review of the enhanced images led to an F1 of 0.888 and a precision of 0.908. Visual review was fairly accurate, because the luminance component was used to store the hidden information. Human sight is very sensitive to changes in luminosity. If the hidden message was stored in one of the chroma components, it would have been more challenging as the human eye is less sensitive to changes in color.

4 Conclusion

Forged image discovery was fairly simple once it was noticed that only the first 4 bytes of the HEX signature were altered, since using the remaining part of the HEX signature was enough to recognize the original file type.

Detecting stego images was more challenging, but using enhanced images based on least significant bits of the luminance channel makes the visual classification much easier. Although the creation of enhanced images based on the least significant bits of the luminance channel was automated, the classification of the images as containing a hidden message was manually performed. The next step will be to automate the classification part, too.

References

1. Ionescu, B., H. Müller, R. Péteri, Y.D. Cid, V. Liauchuk, V. Kovalev, D. Klimuk, A. Tarasau, A.B. Abacha, S.A. Hasan, V. Datla, J. Liu, D. Demner-Fushman, D.-T. Dang-Nguyen, L. Piras, M. Riegler, M.T. Tran, M. Lux, C. Gurrin, O. Pelka, C.M. Friedrich, A. Garcia, S. de Herrera, N. Garcia, E. Kavallieratou, C.R. del Blanco, C.C. Rodríguez, N. Vasillopoulos, K. Karampidis, J. Chamberlain, A. Clark, and A. Campello. ImageCLEF 2019: Multimedia Retrieval in Medicine, Lifelogging, Security and Nature. in Proceedings of the Tenth International Conference of the CLEF Association (CLEF 2019). 2019. Lugano, Switzerland: (LNCS) Lecture Notes in Computer Science, Springer.
2. K Karampidis, N. Vasillopoulos, C.C. Rodríguez, C.R. del Blanco, E. Kavallieratou and N. Garcia. Overview of the ImageCLEF security 2019 Task. Proceedings of the 10th International Conference of the CLEF Association (CLEF 2019), CLEF 2019 Working Notes. CEUR Workshop Proceedings (CEUR- WS.org), 2019. ISSN 1613-0073, http://ceur-ws.org/Vol-2380/.
3. DROID https://www.nationalarchives.gov.uk/information-management/manage-information/preserving-digital-records/droid/ last accessed 24 May 2019.