Report of ECI 2019 Course: " Introduction to Steganography and Watermarking "

Assignment E.316-N

Acha Francisco, Caldo Juan Pablo, Cardenas Rodrigo, Castagna Franco and Remedi Elias.

1 Introduction

Steganography is the procedure of insert information inside a data source without changing its perceptual quality. Digital steganography uses digital data sources as a cover for hidden information. Examples of digital covers are digital text files, image files and sound files among others.

In particular for digital image based steganography the pixel intensity is usually used for encoding information [REF] but other approaches are also widely used such as embedding information in the frequency domain.

There are available many software tools

In this report, five steganographic tools that hides text into a digital image were chosen to perform an assessment in terms of imperceptibility of the stego-image, capacity and robustness.

2 Materials and methods

2.1 Dataset

Since we want to evaluate performance of steganographic tools that hide text into an image, a image dataset is needed. We built a dataset containg images 20 of four types: N-type (landscapes and open nature), S-type (still life), P-type (portraits) and T-type (text). The complete dataset is then 80 images in total. N, S, P-type images were obtained and selected from Google images search engine queries. Namely, keywords for queries were *landscapes*, *still life* and *portrait* respectively. Right usage for the images was selected such that results were labeled for noncommercial reuse, and size of the images was set in medium [NOTA AL PIE DE LA FECHA]. Text images were collected from research papers by exporting pages as jpeg images. Table [REF] summarizes some basic features of the dataset used such as mean image size and mean file size. All the images in the dataset were stored as jpeg format. DECIR AHORA EL TAMAÑO MEDIO, Y LA MEMORIA DE CADA IMAGEN MOSTRAR UN EJEMPLO DE CADA TIPO

2.2 Description of selected software

2.2.1 *OutGuess*

2.2.2

2.2.3 *StegHide (v. 0.5.1)*

StegHide is an open source steganographic software that allows hide text using image or sound files as covers. (REF A LA PAGINA) It supports JPEG, BMP, WAV and AU file formats as cover files. *StegHide* performs steganography by means of a graph-theoretic approach. Data to be embedded is compressed and encrypted, Then a pseudo-random sequence of postions of pixels is created. On this positions secret data will be embedded. Then a graph-theoretic matching algorithm finds pairs of positions on the remaining pixels such that exchanging their values has the effect of embedding the corresponding part of the secret data. If there are not enough pixels with values that can be used to embed the data by exchanging, values are overwroute. This way, most of the embedding is done by exchanging pixel values and then the first-order statistics is marginally changed. A passphrase must be provided by the user for encryption and pseudo-random generator initialization. The same passphrase must be provided for data extraction from stego-file. The default encryption algorithm is Rijndael with a key of 128 bits altough others are available as well.

2.2.4

2.2.5 *SteganPEG*

2.3 Benchmarking

Some criteria and metrics needs to be established in order to to benchmark the selected software. In this section metrics for imperceptibility assessment are presented as well as criteria regarding capacity of storage for hidden data and tests for robustness evaluation.

2.3.1 Imperceptibility

2.3.2 Capacity

2.3.3 Robustness

3 Results

3.1 Imperceptibility

3.2 Capacity

3.3 Robustness

4 Discussion and Conclusion

5 References