People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific research
M'hamed Bougara University, Boumerdes
Institute of Electrical and Electronic Engineering,
**Laboratory of Signals and Systems (LSS)**

# ALGERIAN JOURNAL OF SIGNALS AND SYSTEMS

**ISSN : 2543-3792**

Title: **A comparatives study of steganography and steganalysis tools**

Authors: **Leila BENAROUS [(1)], Mohamed DJOUDI [(1)], Ahmed BOURIDANE [(2)]**
Affiliation:
**(1) Dept. Computer Science, University of Amar Telidji (UATL), LAGHOUAT, ALGERIA**
**(2) Dept. Computer Science, University of Northumbria, Newcastle, UNITED KINGDOM**

Page range: **92-98**



**Volume : 1 Issue : 2 (December 2016)**

Laboratory of Signals and Systems
Address : IGEE (Ex-INELEC), Boumerdes University, Avenue de l'indépendance, 35000, Boumerdes, Algeria
Phone/Fax : 024 79 57 66
Email : lss@univ-boumerdes.dz ; ajsyssig@gmail.com

# A comparatives study of steganography and steganalysis tools

BENAROUS Leila,
Department: Mathematics and Computer Science
University of Amar Telidji, LAGHOUAT, ALGERIA
l.benarous@lagh-univ.dz

DJOUDI Mohamed,
Department: Mathematics and Computer Science
University of Amar Telidji, LAGHOUAT, ALGERIA
m.djoudi@mail.lagh-univ.dz

BOURIDANE Ahmed
Department: Computer Science and Digital Technologies
University of Northumbria, UK
ahmed.bouridane@northumbria.ac.uk

***Abstract*—** Steganography is one of the oldest methods of secure communication. It was an art at the beginning, now became a science. It aims to conceal secret messages or data inside an innocent cover. Steganalysis is the science that can detect and extract hidden data. Many steganography and steganalysis tools exist, a lot of them are free which makes it easy for anyone to use these tools. In this paper, a comparative study will be done between two widely used steganography tools (StegHide and OurSecret) and between three steganalysis tools StegSpy, StegSecret and Hidden data detector.

***Key words*:** steganography, steganalysis, StegHide, OurSecret, StegSecret, StegSpy, Hidden Data Detector.

## 1. Introduction

Images and videos represent the mostly used cover files for steganography due to that fact that they have a large capacity, are innocent and easily exchanged. There exist many algorithms and tools to do the embedding, modifying the LSB value, the DCT coefficients, Spread Spectrum, DWT, DFT, Hiding information in the Movement Vectors …etc. There are many algorithms in theory, and many free tools available. We choose to compare between two free steganography tools StegHide (Open-Source) [1] and OurSecret (Free) [2]. A previous study by Cheddad et al (2007) [3] was conducted to compare between free steganography tools including: Hide&Seek, Hide-In-Picture, Stella, S-tools, and Revelation. We have done the comparison basing on a set of metrics: Accepted format, capacity, change in size, change in quality, detection rate, the embedding of multiple files and the ergonomics. A comparative study between three free steganalysis tools: StegSpy [4], StegSecret [5] and Hidden Data Detector [6].

The paper is organized as follow: section I contains the comparative study between the steganography tools, section II contains the comparative study between the steganalysis tools, section III contains the result discussion, and section IV concludes the paper.

## 2. A Comparative Study between steganography tools

### *Introducing the tools*

- **StegHide**

StegHide is an open source tool under the Licence GPL, developed by Stefan Hetzl in 2003. It hides the data in images (JPEG, BMP) and audios (WAV, AU). The program compresses the data using the Zlib algorithm, the hidden data is encrypted using Rijndael (AES) algorithm, the integrity of the hidden data is verified using the checksum algorithm CRC32.

The program can be used in a text mode by command (see Table 1 for some options), the two important commands are:

- The embedding: Steghide embed –cf image.jpeg –ef secretdata.txt
- And the extraction: Steghide extract –sf image.jpeg

***Table 3***: Some of StegHide Options [1]

| Option | Signification |
|---|---|
| -ef | Used with the command embed, it means « embed file », it is added before the file to hide. |
| -cf | Used with the command embed, it means « cover file », it is added before the cover file. |
| -sf | Used with the command extract, it means « stego file », it is added before the stego file. The hidden file will be extracted with its original name. |

The tools randomly change the pixel values, the algorithm as described by its author works as follow:

- The secret data is compressed and encrypted.
- A sequence of positions of pixels in the cover file is created based on a pseudo-random number generator initialized with the passphrase. Of these positions those that already contain the correct value by chance are sorted out.
- Then a graph-theoretic matching algorithm finds pairs of positions such that exchanging their values has the effect of embedding the corresponding part of the secret data.
- The pixels at the remaining positions are also modified to contain the embedded data using LSB algorithm. [1]
- **OurSecret**

OurSecret is a free tool, it hides the secret data inside multimedia files of different types such as images and videos of different format. The tool has a graphical interface and it's so easy to use, both the embedding and the extraction can be done in three steps. The tool compresses the data and optionally encrypts it before the embedding. [2]

The algorithm of the tool was not officially described by its author, but when we have done our tests, we were able to how the embedding is done. We used Hex Editor [7] to compare between the stego files and the cover files. We found that the tools do not change the pixel's bits, but the embedding is rather done by adding the compressed (optionally encrypted) data at the end of the cover file. Although we were able to know how the embedding is done, we could not know the compression and the encryption algorithms used.

***Defining the Comparison Metrics***

To establish a successful comparative study, we have to define the comparison metrics, we choose the following metrics:

- Change in size: we compared between the size of the cover file and the size of the stego file after the embedding.
- Accepted Format: we tested the different format accepted by each tool as a cover file and as hidden data.
- The capacity: It is the limit of integration allowed by the software, it's here calculated as the maximal ratio between the size of the data and the size of the cover file where the embedding was possible.
- The possibility to embed multiple file at once using the same cover file.
- Detection Rate: measured by the use of 3 steganalysis tools, StegSpy, StegSecret and Hidden Data Detector.
- The change in quality: measured for images by calculating the PSNR.
- Ergonomics and ease of use.

***Results***

***Change in Size***

***Table 4**: comparative study between StegHide qnd OurSecret*

| | ***StegHide*** | ***OurSecret*** |
|---|---|---|
| ***Change in size*** | BMP : no change<br>JPEG : Reduced | Increased (≈ 87%) |
| ***Cover Formats*** | Images : BMP, JPEG | Images: JPEG, TIFF, PNG, PMB, GIF, JP2;<br>Videos: AVI, DIVX, FLV, MOV, MP4, MPEG, WMV. |
| ***Hidden data Formats*** | No constraint on the hidden data Format. | |
| ***Embedding limit*** | Size (HiddenData) < 17,5% * Size (CoverFile) | No limit |
| ***The embedding of multiple file*** | Impossible | Possible |

When we compared the size of the cover images of type BMP and the stego ones resulting from StegHide, we noticed that the size did not change, however, the JPEG images resulting from the same tools decreased in size after the embedding. The stego files created by OurSecret all increased in size with approximately 87% of the hidden data size:
Size (StegoFile) ≈ Size (CoverFile) + 87% * Size (HiddenData). (see Table 2)

***Accepted Format***

Steghide accepts only BMP and JPEG image Formats, while OurSecret accepted all the 13 tested file formats - images and videos (see table 2).

***The capacity***

Steghide changes the pixel values, it uses the graph-theory approach that's why the embedding was not possible all the time, if the hidden data is big, StegHide would print a message that the cover is too small for the embedded data. Basing on our tests the embedding was possible when: Size (HiddenData) < 17,5% * Size (CoverFile). OurSecret, on the other hand imposed no restriction on the size of the secret data (see table 2).

***The embedding of multiple files***

OurSecret allowed the embedding of multiple files at once, all the files were safely extracted. StegHide did not allow the embedding of more than a file at once, so we tried to reuse the stego file as a cover to hide a new data, only the new data was extracted successfully, the old one was destroyed (see Table 2).

**Detection Rate**

***Table 5**: Global Detection Rate*

| Detection Rate | | | |
|---|---|---|---|
| Tools | OurSecret | | StegHide |
| | Images | Videos | Images |
| StegSecret | 67% | 47% | 0% |
| StegSpy | 28% | 48% | 0% |
| Hidden Data detector | 39% | 80% | 100% * |
| * : JPEG Only. | | | |

To measure the robustness of both tools, we decided to calculate their detection rate using the three steganalysis tools StegSecret, StegSpy and Hidden Data Detector.

We found that the files treated by OurSecret was detected by all the three tools, while StegHide was detected by one tool only –Hidden Data Detector- For JPEG Images with the rate of 100% (See Table 6).

***Change in Quality (Peak Signal Noise Ratio)***

*Originally, it's a metric that measures the distortion between an original and a compressed image. It's calculated as follow:*

$$PSNR = 20log_{10}(\frac{MAX_f}{\sqrt{MSE}})$$

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

MSE: Mean Square Error
F : represents the matrix of the original image
g : represents the matrix of the compressed image
m: represents the total raw numbers, i represents the raw index,
n: represents the total number of the columns, j represents the index of the column
$Max_f$ : The max signal value in the original image [8]

We used this metric to measure the distortion produced by the embedding of the hidden data by the two steganography tools. We calculated the PSNR for images only and we used for that the application of Pascal BERTOLINO [8] (see Table 8). We found that StegHide changes the quality of the image but the results of the PSNR were between 37 and 75 db which means that it is not perceptible by human eye (see Table 4). OurSecret does not change the quality, the PSNR=∞ which means that the stego image and the cover image are identical in quality (see Table 5).

| Attribute | Identical images | Very good | Good | Acceptable | Bad |
|---|---|---|---|---|---|
| PSNR(dB) | ∞ | ≥40 | 40-35 | 30-35 | <30 |

***Table 6:*** *Defining the intervals of the image quality: PSNR(dB) [9]*

| | StegHide | OurSecret |
|---|---|---|
| Quality of the image (PSNR) | 37 – 75 db | ∞ |

***Table 7****: Change in Quality (PSNR)*

***Ergonomics***

| | StegHide | OurSecret |
|---|---|---|
| Ergonomics | Text Mode | Graphical Interface |
| Ease to use | Commands | Very easy (3 steps) |

***Table 8****: Ergonomics*

## 3. A Comparative Study between Steganalysis Tools.

### *Introducing the tools*

- **StegSecret**

It is a steganalysis open source software under the GPL license, to detect hidden data in multimedia files (images, audio, video). It was developed by Alfonso Muñoz in 2007. It is a cross platform tool written in java. It can detect hidden files by the LSB method in pseudorandom or sequential techniques (attack: chi-square and rs-attack ... etc.), The EOF method to BMP, JPEG and GIF, DCT method and the palette based steganography methods. It can detect more than 40 steganography tools by their signatures (DBSA v0.1). [5]

- **StegSpy**

A free software developed by Michael T. Raggo in 2004 to detect the use of steganography in a file. It can detect steganography applied by the tools: Hiderman, JPHideandSeek, Masker, JPegX, InvisibleSecrets ... etc. [4]

- **Hidden Data Detector**

It is a free tool developed by Digital Confidence, to detect hidden data in images (JPEG, JPEG2000, PNG, SVG), videos (AVI, MP4), audio (WAV, MP3), Microsoft Office, Star Office and OpenOffice files by checking documents properties, a change or alteration in its properties indicates the existence of hidden data. [6]

### *Defining the Comparison Metrics*

To compare between the steganalysis tools we choose the following metrics:

- The Number of accepted format
- The Searching mode

- The Rate of detection

***Results***

***The number of accepted format***

| Tools | StegSpy | StegSecret | Hidden Data Detector |
|---|---|---|---|
| Accepted Formats | BMP, JPEG, JPEG 2000, GIF, PNG, TIFF, AVI, WMV, MPEG, DIVX, FLV, MOV, MP4 | BMP, GIF, JPEG, JPEG 2000, PNG, TIFF, AVI, DIVX, FLV, MOV, MP4, MPEG, WMV | JPEG, JPEG 2000, PNG, AVI, MP4 |

***Table 9**: Accepted Format*

***The Searching Mode***

StegSecret searches for the stego files by directory, so does Hidden Data Detector. However, StegSpy verify if a file is stego or not, it accepts one input at a time. Which makes is quit hard to use for investigating a large quantity of images.

***Detection Rate***

| Tools | StegSpy | StegSecret | Hidden Data Detector |
|---|---|---|---|
| Detection Rate | 31.6% | 56.5% | 60.7% |

***Table 10:** detection rate of StegSpy, StegSecret and Hidden Data Detector*

We used the three tools to detect stego files created by the steganography tools StegHide and OurSecret basing on the accepted format, Hidden data Detector had the best detection rate followed by StegSecret and finally by StegSpy (see table 11). Hidden Data Detector detected with 100% the JPEG stego images resulted from StegHide and OurSecret and the AVI videos treated by OurSecret. StegSecret detects with 100% the BMP, JPEG and GIF images treated by OurSecret. StegSpy has a maximal detection rate of 60% for MPEG Videos treated by OurSecret.

**4. Discussion**

To establish a comparative study, comparison metrics should be considered. The set of metrics we choose to compare between the steganography tools are:

- Accepted format (cover and secret data)
- The change in size and quality (PSNR)
- Ergonomics and ease of use
- The capacity
- The possibility to embed multiple files
- And, detection rate (the robustness of the algorithm)

As for the comparison of steganalysis tools, the metrics are:

- The detection rate
- Searching Mode
- and, Accepted format

Both tools are free; OurSecret was used to embed data in images and videos.

- It is easy to use (graphical interface),
- It accepts many image and video formats as a cover file,
- It does not impose any constraint on the size of the hidden data,
- The quality of the image is preserved (PSNR=∞),
- It allows the embedding of multiple data files at the same time.
- The size of the stego file increases proportionally with the size of the hidden data,
- It was detected by all the steganalysis tools tested.
- The embedding of the data is at the end of file (EOF)

StegHide was used to embed data in images.

- It accepts only the JPEG and BMP images formats,

- It does not impose any restriction on the formats of the hidden data but certainly on the size that has to be basing on our tests less than 17,5% of the cover file.
- It changes the pixel's values, but we noticed that the quality is still preserved (PSNR >37db) i.e.: the change in quality cannot be detected by the human eye.
- It can be used in a text mode which requires a fairly high level of master ship.
- It does not allow the multiple embedding, when we re-used the stego file as a cover file and embedded another hidden data the old data was destroyed.
- The embedding algorithm is more difficult than OurSecret because the hidden data are spread randomly on the cover file,
- It is more robust against detection (it was detected by one tool only among the three steganalysis tools tested).
- It requires no installation (Windows) which implies that it is easier to erase its tracks (unlike the tool OurSecret that must be installed so it can change the file registers values).

## 5. CONCLUSION

In this paper, we have done a comparatives study of steganography tools (StegHide and OurSecret) and steganalysis tools (StegSpy, StegSecret and Hidden Data Detector). All the tools chosen are widely used and free.

OurSecret is a free. The tool embeds the secret data in the multimedia files (used here to embed data in images and videos). StegHide is an open source tool. The data is hidden inside image and audio files (used here to embed data in images).

The aim behind this comparative study is to understand how and where the embedding is done. However, the decision of which tool is better is always up to the final user, basing on his needs:

- The importance of the information,
- The desired level of security,
- The duration for which the information must be kept secret and undetected,
- The communication channels used,
- The level of mastery, and intentions.

The use of steganalysis tools was to detect the robustness of the two steganography tools StegHide and OurSecret. Having used them, we decided to compare between them basing on their detection rate, ease of use, number of accepted format and searching mode. Taking all the criterias into consideration StegSecret seems the best. However, in term of detection rate, Hidden Data detector is the best, not to forget that both Hidden Data Detector and StegSecret search by directory while StegSpy is mono input and does the research by file which is penalizing while investigator hard disk full of images.

### *References*


[1] H. Stefan, "StegHide," 13 04 2015. [Online]. Available: http://Steghide.sourceforge.net.

[2] "OurSecret," Secure Kit, [Online]. Available: http://www.securekit.net/oursecret.htm. [Accessed 13 04 2015].

[3] A. Cheddad, J. Condell and K. C. a. P. McKevitt, "A Comparative Analysis of Steganographic Tools," *The 7th Information Technology and Telecommunication Conference IT&T 2007,* p. 29, 2007.

[4] B. Englehardt, "StegSpy," Spy hunter, 2003 -2004. [Online]. Available: http://www.spy-hunter.com/stegspydownload.htm. [Accessed 13 04 2015].

[5] A. Muñoz, "StegSecret," Source Forge, 2007. [Online]. Available: http://stegsecret.sourceforge.net/. [Accessed 13 04 2015].

[6] "Hidden Data Detector," Digital Confidence, 2010. [Online]. Available: http://www.digitalconfidence.com/Hidden-Data-Detector.html. [Accessed 13 04 2015].

[7] "Free Hex Editor," hddSoftware, [Online]. Available: http://www.hhdsoftware.com/free-hex-editor. [Accessed 20 06 2015].

[8] "Peak Signal-to-Noise Ratio as an Image Quality Metric," White Papers, 11 09 2013. [Online]. Available: http://www.ni.com/white-paper/13306/en. [Accessed 07 03 2015].

[9] P. Bertolino, "Software," [Online]. Available: http://www.gipsa-lab.grenoble-inp.fr/~pascal.bertolino/software.html. [Accessed 13 04 2015].

[10] B. KHALED, " Approche par marquage pour l'évaluation de la qualité d'image dans les applications multimédias," Novembre 2012.