MBNA Publishing House Constanta 2021

Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

Comparative analysis of audio steganographic instruments

To cite this article: M. PREDA, S. BÎRLEANU and C. RĂCUCIU, Proceedings of the International Scientific Conference SEA-CONF 2021, pg.199-202.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-21-025

Comparative analysis of audio steganographic instruments

M Preda, S Bîrleanu, C Răcuciu

Bucharest, Romania
mirela.preda@mta.ro

Abstract. One of the most important concerns in the communications field is the security of information. Transmitting digital information has become facile due to Internet connections, still, the shared content might became vulnerable. Content can be protected by being included in a digital file that transports it safely, hidden and know only by the sender and the receiver. This feature is made possible by the steganographic instruments by inserting hidden information in a wide range of multimedia files. The study focuses on the analysis and the comparison of four software instruments specially designed for audio steganography, reporting to the criterias of hidden information quantity, robustness and imperceptibility.

1. Introduction

The technique of stenography is not new, it has been around since ancient times, when people found a way to send secret messages through hidden tattoos or invisible ink [1]. But nowadays, due to the increased performances of computing and communication techniques, steganography is becoming a more accessible process.

There are many types of files that can carry a hidden message. It can be an image, an audio, a video or a text, but in this article we will analyse the audio files, which has better features, such as high stability, reproducibility and noise immunity [2]. The goal is, of course, to insert the hidden message without leaving traces and without arousing suspicion from those who have access to the steganographic file. Choosing audio files to carry hidden content also encounters difficulties, because the human auditory system is more sensitive than the human visual system [3].

2. Steganography instruments

The etymology of the word steganography comes from the Greek language and is composed of "Stegos" which means "cover" and "graphy" meaning "writing", defining it as "covered writing" [4]. What is important to be mentioned in the case of steganography is that the hidden message (text, image, audio, video) is not altered.

There is currently a large variety of software tools that use steganographic algorithms and create steganographic files that can be transmitted online. In this article, steganographic files were made using four software tools dedicated to audio steganography.

2.1. DeepSound

It is a software tool available on https://deepsound.en.uptodown.com/windows and allows the insertion of hidden content in different audio file formats: wav, wma, mp3, water, flac, cda. To provide high security, the steganographic file can be encrypted with the AES (Advanced Encryption Standard) symmetric encryption algorithm with a 256-bit key, a fairly secure algorithm. Embedded mode can be

performed in three modes, Low, Normal and High, and the amount of hidden information depends on them.

2.2. SilentEye

The application is available on https://achorein.github.io/silenteye/ and accepts image files in JPEG or BMP format and audio files in WAV format, offering several parameters that can be adjusted (embedding that can be done either on a single channel either on both, the distribution of the hidden content, the sound quality), and also the encryption that can be applied with the AES 128 or AES 256 algorithm.

2.3. Steganofile

It is a simple steganography tool, without parameters that can be modified, and imposes a password of at least 4 characters as a security condition to protect the file. There is no information about the supported file format or supported sizes.

It is available at https://www.softpedia.com/get/Security/Encrypting/Steganofile.shtml.

2.4. DeEgger Embedded

The tool creates steganographic materials for several types of files and allows hiding more files in a single or in multiple hosts. It is easy to use and has a simple Quick Mode interface. It is available at http://deegger-embedder.findmysoft.com.

3. Analysis

The same files were used in all software tools. An audio wav file of 7.6MB, mono type with 16KHz sampling frequency, was used to transport the same hidden PNG image in size of 0.5MB, 1 MB and 2 MB. The process diagram in this comparative study is described in Figure 1 below.

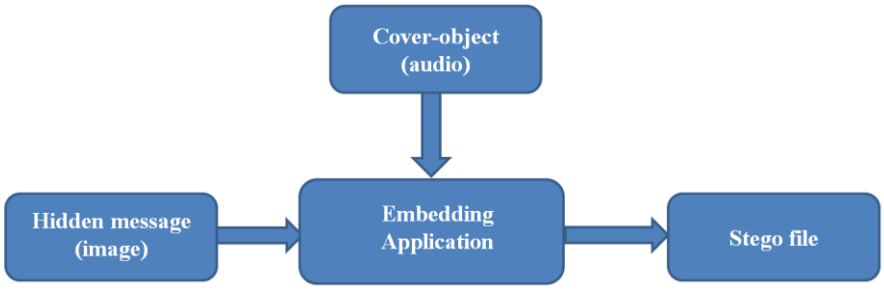

Figure 1. Steganography application scenario for this paper

Three criterias are used to evaluate steganographic software tools: capacity, imperceptibility and robustness.

3.1 Capacity

The capacity is given by the embedding rate, which provides information related to hidden information quantity (Table 1).

Table 1. Characteristic Embedding rate

	Low	Normal	High
DeepSound	0.5	0.25	0.11
SilentEye	0.32	0.19	0.06
Steganofile		undefined	
DeEgger		undefined	

Table 2, Table 3 and Table 4 show that the hidden file could be inserted or not, using the four steganographic software presented in this paper.

Table 2. DeepSound simulation.

	Low	Normal	High
0.5 MB	Yes	Yes	Yes
1 MB	Yes	Yes	No
2 MB	Yes	No	No

Table 3. SilentEye simulation.

	Low	Normal	High
0.5 MB	Yes	Yes	No
1 MB	Yes	Yes	No
2 MB	Yes	No	No

Table 4. Steganofile and DeEgger Embedder simulations.

	Steganofile	DeEgger Embedder
0.5 MB	Yes	Yes
1 MB	Yes	Yes
2 MB	Yes	Yes

3.2. Imperceptibility

PSNR (Peak Signal to Noise Ratio) and MSE (mean square error) are used to analyze the quality of a stego file, which reflects imperceptibility. If the PSNR value is higher than 36 dB, then the human ear cannot differentiate between the original audio file and the steganographic file [5].

Table 5, Table 6 and Table 7 show the measurements performed, calculating the PSNR for each stego file.

$$\text{PSNR} = 10 \log_{10} \left(\frac{Max^2}{MSE} \right),$$

$$\text{MSE} = \frac{I}{N} \sum_{I=1}^{N} (C_i - S_i)^2,$$

where C_i is sample value of original audio stream and S_i represents the sample value of embedded audio stream.

Table 5. DeepSound PSNR.

	Low	Normal	High
0.5 MB	50.9	73.89	86.04
1 MB	50.6	74.26	-
2 MB	49.84	-	-

Table 6. SilentEye PSNR.

	Low	Normal	High
0.5 MB	25.67	34.61	-
1 MB	23.23	31.54	-
2 MB	19.89	-	-

Table 7. Steganofile and DeEgger Embedder PSNR.

	Steganofile	DeEgger Embedder
0.5 MB	Inf	Inf
1 MB	Inf	Inf
2 MB	Inf	Inf

3.3. Robustness

Robustness is a feature that measures resistance to attacks. The analysis found that DeepSound and SilentEye provide increased security due to encryption with symmetric algorithms (AES). Therefore, if a steganographic file is detected and the hidden content is extracted, it cannot be accessed as is protected by encryption.

4. Conclusion

Following the comparative analysis, the advantages and disadvantages of software tools can be highlighted. SilentEye is below the PSNR threshold of imperceptibility and has the lowest embedding rate of the analyzed instruments, but offers a good security of the transmitted content, encrypted with AES. DeepSound can be a good solution, in addition to AES encryption, the PSNR level is higher than imperceptibility threshold. The other two, Steganofile and DeEgger Embedded, offer lower security, do not have a strong encryption algorithm, but allows the insertion of a larger and more flexible amount of data.

References

[1] Provos N and Honeyman P 2003 Hide and seek: an introduction to steganography. *IEEE Security & Privacy* 3;1(3):**32**-44.

[2] Sadkhan S B, Mahdi A A and Mohammed R S 2019 Recent Audio Steganography Trails and its Quality Measures. *First International Conference of Computer and Applied Sciences (CAS),* **238**-243.

[3] Bhalshankar and Satish 2015 Audio Steganography: LSB Technique Using a Pyramid Structure and Range of Bytes, *International Journal of Advanced Computer Research* ISSN 2277-7970.

[4] Sara, Khosravi, Abbasi Dezfoli Mashallah and Yektaie Mohammad Hossein 2011 A New Steganography Method Based On Hiop (Higher Intensity Of Pixel) Algorithm And Strassen's Matrix Multiplication. *Journal of Global Research in Computer Sciences* 2 (2011): **6**-12.

[5] Ahmed A. Alsabhany *et al* 2020 *J. Phys.: Conf. Ser.* **1551** 012011