High frequency audio steganography

Practical application
and comparissons with other techniques

Teodor Paius, coord. Septimiu Crivei

March 12, 2019

Abstract

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. This paper will focus on the domain of digital signal processing and audio concealment of messages. Apart from other common environments such as images or plain text, sound also represents a good way of transmiting hidden messages. The techniques present in this thesis can be applied not only to the target range of human hearing but can also be implemented with some degree of resemblance to other domains of higher frequencies (radio waves or elctro-magnetic waves).

Contents

Chapter 1

Theoretical background

The commonly stated range of human hearing is 20 Hz to 20 kHz. Under ideal laboratory conditions, humans can hear sound as low as 12 Hz and as high as 28 kHz, though the threshold increases sharply at 15 kHz in adults, corresponding to the last auditory channel of the cochlea. Humans are most sensitive to (i.e. able to discern at lowest intensity) frequencies between 2,000 and 5,000 Hz. Based on this a good way of hiding information is exploiting this human weakness and encoding certain messages in audio files disguised as short sequences of high frequency signals.

1.1 Overview of steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.[4]

1.2 Overview of digital signal processing

To be able to analyze an analog(continous) signal in a digital environment, it must firstly be converted using and analog-to-digital converter. This process is composed of 2 major stages: discretization and quantization. This would transform a continous signal in a set of consecutive frames equidistant in time, and characterized by a certain amplitude.1.3

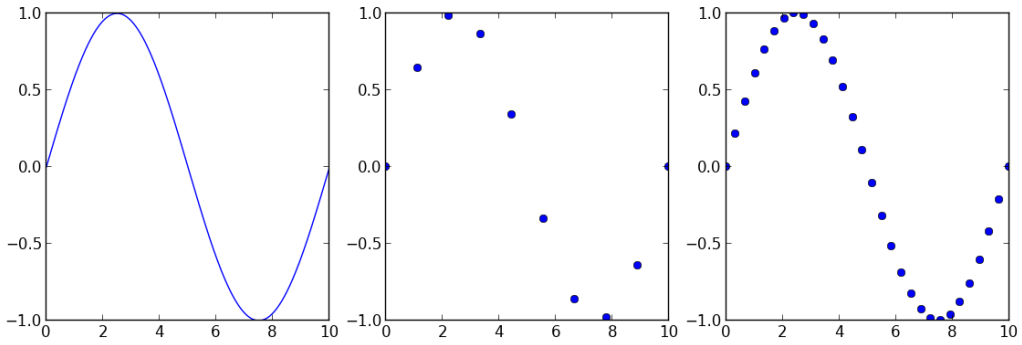

Figure 1.1: Continous signal splitted in discrete samples

The *Nyquist–Shannon* sampling theorem states that a signal can be exactly reconstructed from its samples if the sampling frequency is greater than twice the highest frequency component in the signal. In practice, the sampling frequency is often significantly higher than twice the Nyquist frequency[5]. In this case, where the target range is about 20-26 khz, a sampling rate of 48000 samples/second is almost at the limit, meaning that some higher frequencies might be omitted and loss of accuracy, so a higher sampling rate was chosen: 96000 samples/second.

1.3 Just a little bit of anatomy

Chapter 2

The application

For proving the concept of hiding information using high frequency signals, an python application was implemented

2.1 Chosen method

2.2 Limitations

2.2.1 Hardware limitations

2.2.2 Software limitations

2.3 Further improvements

Chapter 3

Comparison with existent methods

3.1 Other techniques

3.1.1 LSB *(least significant byte)* method

3.1.2 Phase coding

3.2 Advantages/disadvantages

Bibliography

[1] Katzenbeisser, S., Petitcolas, F.A.P.: Information Hiding: Techniques for steganography and digital watermarking. Artech House, Boston (1999)

[2] Mahendra Kumar Pandey, Girish Parmar, and Sanjay Patsariya:An Effective Way to Hide the Secret Audio File Using High Frequency Manipulation (2011)

[3] Ahmed Hussain Ali,Mohd Rosmadi Mokhtar and LoayEdwar George: A Review on Audio Steganography Techniques (2015)

[4] Pahati, OJ (2001-11-29). "Confounding Carnivore: How to Protect Your Online Privacy". AlterNet. Archived from the original on 2007-07-16. Retrieved 2008-09-02.

[5] Candes, E. J., Wakin, M. B. (2008). An Introduction To Compressive Sampling. IEEE Signal Processing Magazine, 25(2), 21-30. doi:10.1109/MSP.2007.914731