NYASHA MASHANDA

MSHNYA010

EEE4114 PROJECT

STEGANOGRAPHY

“Truth is found neither in the thesis nor the antithesis, but in an emergent synthesis which reconciles the two.” — Georg Wilhelm Friedrich Hege

There is more to steganography than that which meets the eye - pun intended.

Introduction

The internet has allowed people to share copious amounts of information at an ever-increasing rate and this has made communication much easier. When two entities are communicating, its most likely that they don't want other people to listen into their conversation. This gives rise to the need of ensuring that information is transmitted securely even if the medium is hacked into. Two methods that try to achieve securing data in that manner are cryptography and steganography. Cryptography renders the structure of data so that it is not readable without possession of additional information. Steganography maintains the structure of data and instead hides the data inside another message. The advantage of using steganography over cryptography is that cryptography will attract undue attention as people will try to figure out/ decrypt the message while steganography will not attract any attention as the secret message is embedded in another message, that is if done properly. It is possible to conceal a text file, image or media within another text file, image or audio. When information is concealed inside an audio file, this is called audio steganography. On the other hand, when information is concealed inside an image file this is called image steganography.

How is it achieved?

For steganography to occur, there must be two things:

1. a benign file that any entity can have access to
2. a message to be sent to a specific entity.

The message is encapsulated inside the benign file called the "cover" file to create a stego file. It is this stego file that is sent to other entities but only the intended recipient can extract the message from the stego file through a specific method.

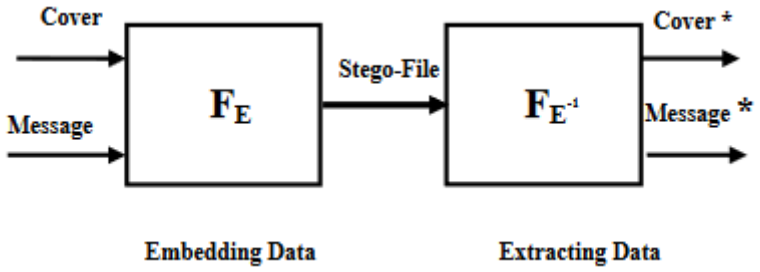


Figure 1 *shows the process of steganography*

General Applications of steganography

Steganography offers the potential capability of hiding the existence of confidential information, the hardness of detecting the hidden information and enhancement of the secrecy of the encrypted data[1]. As a result, steganography is widely used in confidential communication and secret data storing by and between individuals, business entities, government entities and even rogue entities. *There is an electromagnetic spectrum of possible users of steganography.* Inside the government, steganography is mainly used by the military to convey messages securely. On the other end of the spectrum, steganography is also used by terrorist as indicated by the New York Post in the referenced article[2].

[1] KIT-STEGROUP, http://datahide.org/BPCSe/applications-e.html

[2] New York Post, "Terrorists using eBay and Reddit to send coded messages: Mossad", https://nypost.com/2015/03/01/terrorists-using-ebay-and-reddit-to-send-coded-messages-mossad/

Digital watermarking is also one of the application areas of steganography. In this area, steganography is used to protect intellectual property from emerging theft by hiding a digital signature inside the digital file. Interestingly, this has been used in the healthcare industry by hiding information in DNA sequences to protect intellectual property[3]. One can also hide a digital signature inside an image for which they own copyrights. This can be used in the future if there be any need to claim copyrights.

Aim

This paper will focus on audio steganography- concealing information inside digital audio. The first step is to come up with an **algorithm** that will be able **to create a stego track** through **modulation** and also extract the message on the receiving side. In a paper written by Sumit Arora, this was done using a already-made application. The resulting stego track was too noisy and could easily give the impression that there was something else in the sound file, thereby attracting unwanted attention[4]. Additionally, my aim is to find ways in which the **hiddenness of the message can be maximised** so that it very difficult for a listener to suspect that there is another file/message inside the cover file. In this project, I also go an extra step to find ways in which the **quality of the extracted message is maximised**.

Overview of Audio Steganography

The word steganography comes from the Greek word steganos which means covered and graphein which means to write. Therefore, steganography is the art of covering information to enable secret communication. Audio steganography simply exploits the limitations of the Human Auditory System (HAS). Due to the anatomy of the human ear, humans can only pick up sounds within the frequency range of 20 – 20 000 Hz. Frequencies below 20 Hz, infra-sounds and above 20 000 Hz, ultrasounds are inaudible to the human ear. The hearing ranges of other animals differ from that of HAS.

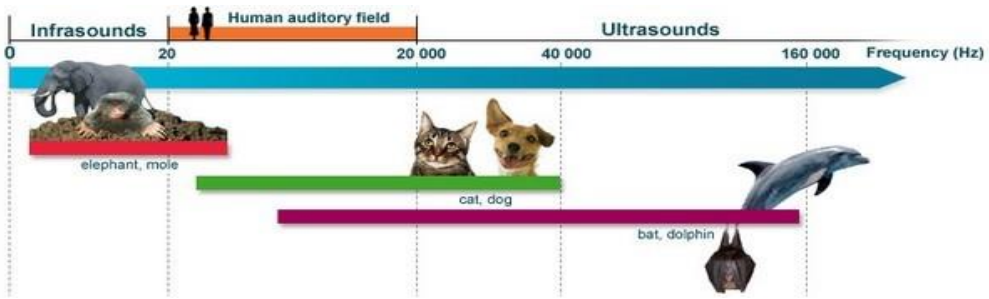


Figure 2 *shows the hearing range of different animals*

Image source: Cochela

The HAS is also known to degrade as people age and a result, the audible range significantly becomes narrower. Therefore, there are sound frequencies that a young person can hear while older people cannot perceive the sound. Interestingly, using the extent of young people's audible range, other governments have found it useful to deter young people from congregating outside of shops and marts by using

[3] Clelland, T.,Risca, V.,Bancroft, C. "Hiding Information in DNA Microdots", https://www.researchgate.net/publication/12921709_Hiding_messages_in_DNA_microdots

[4] Sumit Kumar Arora, "Audio Steganography: The art of hiding secrets within earshot", https://medium.com/@sumit.arora/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-1-of-

irritating ultrasounds that only young people can hear. This is done in an aim to reduce anti-social behaviours that come as a result of these gatherings[5].

Given these findings, one way to achieve Audio Steganography is through the use of infra-sounds and ultrasounds, accompanied by an audio signal that is within the audible range. Moreover, the human ear is not as sensitive to phase changes hence this can be exploited for steganographic purposes. It should be noted that studies have shown that long exposure to infrasound can cause unpleasant feelings like awe and fear[6] and in other cases a feeling akin to sea-sickness[7]. However, I have not found studies that soundly prove or disapprove that long exposure to ultrasounds may be harmful. Sounds very close to ultrasounds are however perceptible, but very irritating to the human ear.

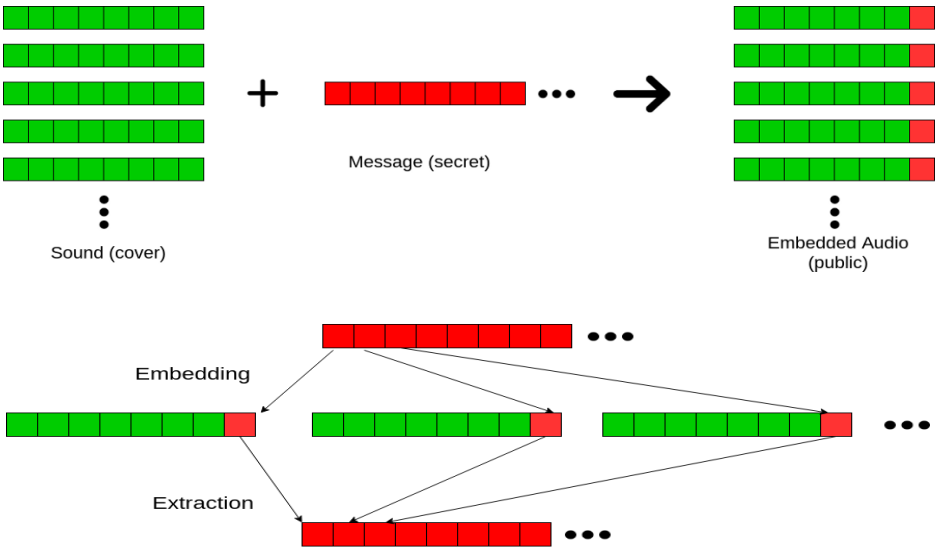
Audio Steganographic methods

Least Significant Bit (LSB) Algorithm

Audio files are usually stored in digital form. This means that the varying signal levels are represented by 8-bit, 16-bit or more binary numbers. In any binary number, the last bit is called the least significant bit and the value of this bit can be altered such that when the stego track and original track are played, a person can not perceive any difference with their ears. This is usually true if the bit representation is of a higher order. Below is an 8-bit number showing a least significant bit of zero.

1	0	1	0	1	0	1	0

Using the digital property of audio files and how the least significant bit can be altered without causing any perceptible changes on the overall file, the least significant bit algorithm is used to embed audio files with messages. In the following case, an example is given whereby the cover file has 1-byte representation for each value. The message signal is first broken down into individual bits. The individual bits are embedded to the least significant position of a cover byte, thereby replacing the least significant bit. The stego track is then sent to the intended recipient who simply extracts the message from the least significant bits.



[5] Sumit Kumar Arora, "Audio Steganography: The art of hiding secrets within earshot", https://medium.com/@sumit.arora/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-1-of-2-6a3bbd706e15

[6] "Infrasound linked to spooky effects", MSNBC. 7 September 2007

[7] King, Simon, "Wind farm effect on balance 'akin to seasickness", News Corp Australia

Figure 3 *shows how the LSB algorithm works.*

It should be noted that almost 50% of the times, the least significant bit of the cover track is unchanged as the bit matches with the bit from the message. This increases the robustness of the stego file.

Phase coding

The phase coding method works by substituting the phase of a cover track with a reference phase that represents the message that an entity wishes to send. If done properly, phase coding is one of the effective audio steganographic techniques. This is because that slight in changes in phase are not as perceptible to the human ear as noise is. Therefore it is very difficult for the listener to perceive and suspect that there might be a message signal embedded in the track.

Frequency Modulation based steganography.

Frequency modulation of a sound signal, if done properly will move the signal to the "inaudible" range. Inaudibility will mainly depend on the age and even gender of an individual. However, based on research[8], most individuals above the age of 23 cannot hear frequencies above 17.5 kHz. Therefore, one can mix a modulated sound signal (message) and an audible sound signal to form a stego track that will hide the message. In the following experiments, I aim to find ways of minimising signal degradation inside the stego file and ensure that the message is also extracted with the highest quality.

Experiment I

How the size of carrier frequency affects the stego file quality and extracted message quality

Procedure

Step I: Modulate message with a carrier frequency of 17.5 kHz. Filter out the required right sideband using a high-pass filter. *A band pass filter was created through convolving a low-pass filter and high pass filter since creating the bandpass directly was not working in Matlab.*

Step II: Create a stego track by mixing the modulated message with the cover message. *The algorithm was written in such a way that the stego track is added to the file directory. Stego1.wav is for the first carrier freuquency of 17.5 kHz.*

Step III: Send the stego track to the intended recipient through any means.

Step IV: At receiving end, filter out the modulated message signal through applying a filter with the same characteristics as that used in step I.

Step V: Demodulate the extracted signal to get the message.

Step VI: Repeat Steps I – V using a carrier frequency of 20 kHz

Step VII: Repeat Steps I – V using a carrier frequency of 25 kHz

[8] [8] Sumit Kumar Arora, "Audio Steganography: The art of hiding secrets within earshot", https://medium.com/@sumit.arora/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-1-of-2

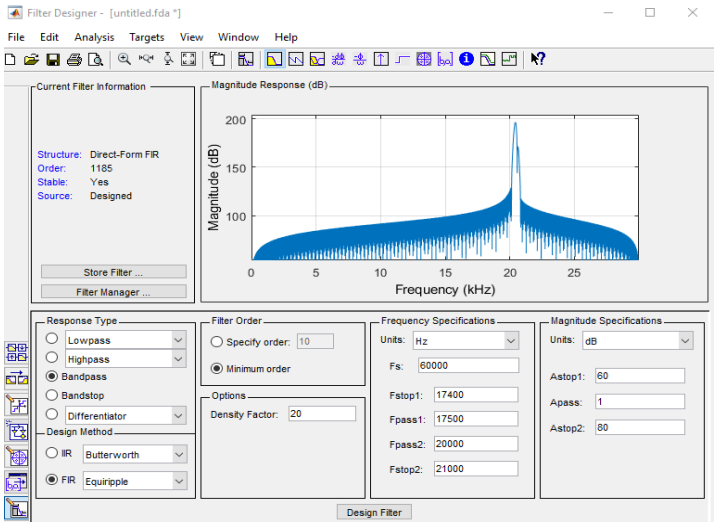


Figure 4 *shows the frequency spectrum of the unwanted bandpass filter*

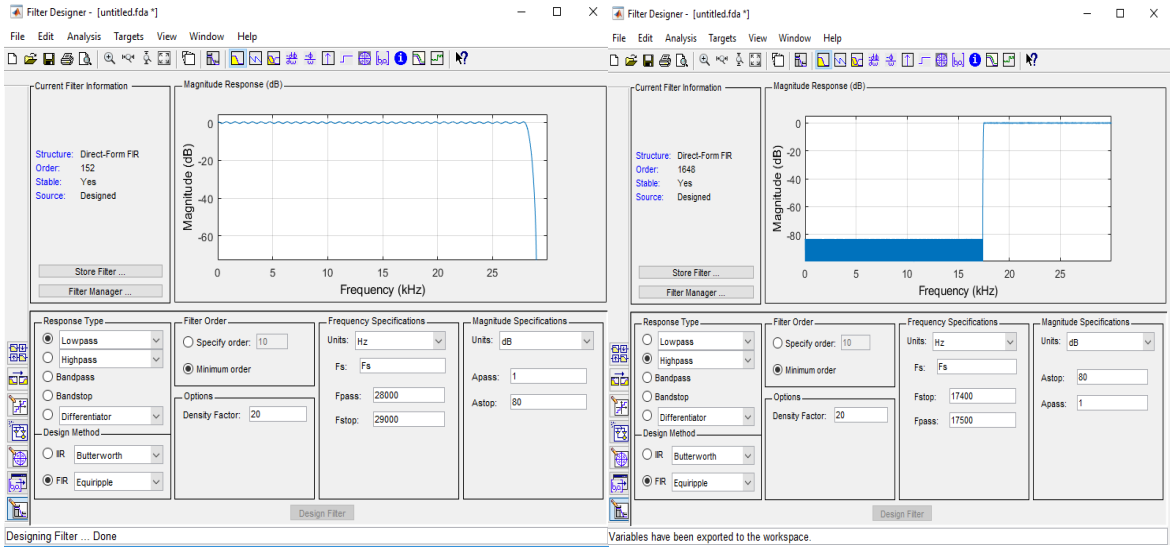


Figure 5 *shows a lowpass + highpass filter used to create the bandpass filter*

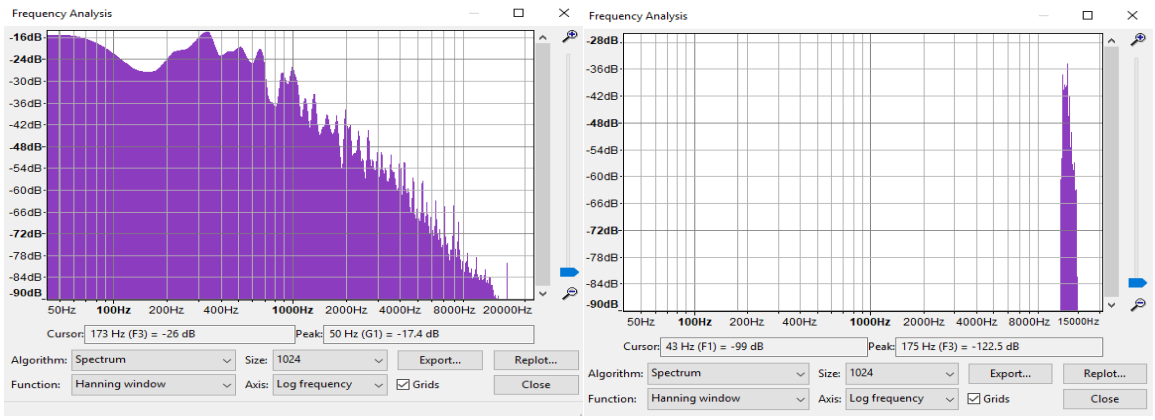


Figure 6 *shows the frequency spectrum of cover signal next to the modulated message signal*

There is more to steganography than that which meets the eye - pun intended.

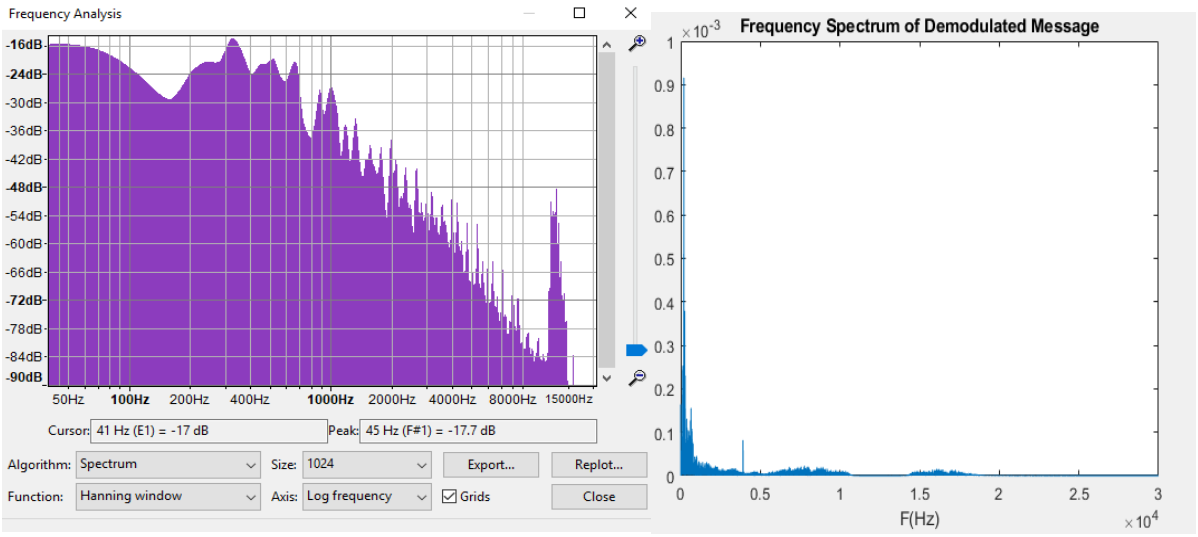


Figure 7 *shows the frequency spectrum of stego track next to the demodulated message signal*

Results

Carrier Frequency (kHz)	Stego Sound Quality	Extracted Message Sound Quality
17.5	bad	better
20	good	good
25	better	bad

Table 1 *shows results from Experiment I*

The results can be evaluated through listening to the stego files and extracted message files. In order to make playing the sound files easy, *Audacity* was used - one can easily drag and drop the file on an audacity window to listen at it. It is important to ensure that there is no other track in the track space to avoid listening to two tracks at the same time.

Stego Results

Quality of a stego file is determined by how difficult it would be for an unintended recipient to suspect that there might be another message hidden in the track. Therefore, a stego file is of high quality if it is highly unlikely that an unintended recipient will detect the presence of a hidden message. I used my ear to measure the sound quality of the stego file. *It should be noted that by doing this, I am not claiming that my ear is the standard measuring tool of sound quality*. From listening to the resulting stego files, increasing the carrier frequency, has resulted in a high quality stego track. This could be attributed to the fact that shifting a signal to a higher frequency further pushes it into the inaudible range.

Extracted Message Results

The quality of the message signal is determined by how easy it is to hear the message in the extracted signal. If the intended recipient can easily extract and hear the actual message, then the message signal is of high quality. The inverse is also correct. From the results the received, signal quality degrades as the size of the carrier frequency is increased.

There is more to steganography than that which meets the eye - pun intended.

Conclusion

There is a trade-off between the quality of the stego file and the quality of the extracted message. This means, to get a high sound quality received message, the quality of the stego track must be sacrificed and vice-versa is true. To ensure that we get the best of both sides, I decided to shift my carrier frequency to 20 kHz.

Experiment II

How the varying the amplitude of the message signal affects the stego track and extracted message sound quality

Procedure

Before combining the message track and the cover track to create the stego file, the amplitude of the modulated message signal is reduced in order to reduce the audibility of the hidden signal. The amplitude was reduced by a factor of 1, 0.1 and then 0.01. Steps I-V were repeated using these multipliers. The results for this experiment were submitted in the following files (stego1,4-5.wav and extracted1,4-5.wav files). It should be noted that the carrier frequency is 20 kHz.

Stego results

The quality criteria for stego files was the same as that in step I. It was found that the sound quality of the stego file increases significantly as the amplitude of the message signal is reduced. This is what is expected as the message signal is suppressed.

Amplitude Multiplier	Stego Sound Quality	Extracted Message Sound Quality
1	good	good
0.1	Very good	bad
0.01	excellent	Very bad(inaudible)

Table 2 *shows results from Experiment II*

Extracted Message Results

The quality criteria for the extracted message signal was the same as the one applied in step I. The sound quality of the extracted message signal decreased significantly when the amplitude of the message signal was reduced. The extracted message signal became inaudible as a result of the reduction in amplitude.

Conclusion

Again, there is a trade-off between the sound quality of the stego signal and extracted the message signal. However, in order to ensure that the intended listener can easily hear the message, I decided that the amplitude not be reduced by any factor.

Experiment III

In the third experiment, I wanted to investigate what would be the effect of removing the high-frequency components from the message before demodulation. I found that this did not improve the quality of both the stego track and extracted message track (results stored in stego 7-9.wav and extract7-9.wav) and as a result decided not to apply this step in the algorithm.

There is more to steganography than that which meets the eye - pun intended.

Final Conclusion

Modulation-based steganography is a convenient way of hiding information and there is a need to ensure that the hidden information is as secure as possible. Increasing the size of the carrier frequency improves the sound quality of the stego track but degrades the quality of the extracted message. Reducing the amplitude of the message track improves the quality of stego file by making the message signal less audible. However, it also degrades the quality of the extracted signal. Therefore, it is necessary that the carrier frequency not be too high or too low when carrying the message but be a moderate value. For this exercise, I decided that the carrier frequency be 20 kHz to ensure the good sound quality of both the stego track and extracted message. Whilst, reducing the amplitude of the message is very attractive as it ensures better sound quality for the stego file, I decide not to implement it as it significantly affected the sound quality of the extracted message.

In conclusion, it is best to modulate the signal to a higher frequency is the hiddenness of the message is to be maximised and also if the quality of the extracted message is to be reasonable. The reader should also note that there a trade-off between the sound quality of a stego track and that of the extracted message.

*Notes: 1) I have attached the **results files**, **Matlab algorithm** to this document. 2) It is necessary to ensure that all files are within the same directory so as not to get errors. 3) The references are put at the bottom of the appropriate pages.*