# STEGANOGRAPHIE SONORE

Source :

[*https://callicode.fr/pydefis/SteganoAudio/txt*](https://callicode.fr/pydefis/SteganoAudio/txt)[*https://doc.lagout.org/Others/Steganographie%20%20techniques.pdf*](https://doc.lagout.org/Others/Steganographie%20%20techniques.pdf)[*https://solusipse.net/blog/post/basic-methods-of-audio-steganography-spectrograms/*](https://solusipse.net/blog/post/basic-methods-of-audio-steganography-spectrograms/)[*http://www.iicybersecurity.com/audio-steganography.html*](http://www.iicybersecurity.com/audio-steganography.html)[*https://medium.com/@sumit.arora/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-2-of-2-c76b1be719b3*](https://medium.com/@sumit.arora/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-2-of-2-c76b1be719b3)[*https://pdfs.semanticscholar.org/c74a/460cbf3263b3081bd56810e4968bccea12a5.pdf*](https://pdfs.semanticscholar.org/c74a/460cbf3263b3081bd56810e4968bccea12a5.pdf)[*http://www.expertmultimedia.ch/Technique/Technologie/formats-audio/la-compression-audio*](http://www.expertmultimedia.ch/Technique/Technologie/formats-audio/la-compression-audio)[*http://www.expertmultimedia.ch/Technique/Technologie/formats-audio/le-format-wav*](http://www.expertmultimedia.ch/Technique/Technologie/formats-audio/le-format-wav)[*http://www.expertmultimedia.ch/Technique/Technologie/formats-audio/le-format-mp3*](http://www.expertmultimedia.ch/Technique/Technologie/formats-audio/le-format-mp3)

# Introduction :

“Steganography is technique and art of hiding a secret message in carrier file so the existence of the secret messages cannot be known. “

“Words of steganography are divided into “stegos” and “grafia” which each has meant “cover” and “writing” combine the word become “covered writing” . “

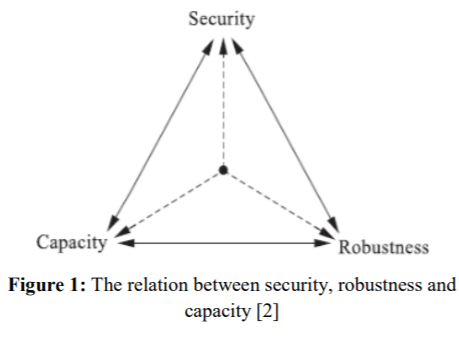
Deux étapes importantes dans la stéganographie : la compression avec l’insertion des datas et la décompression et l’extraction des datas. La stéganographie existe sur plusieurs supports : le texte, les images, les vidéos et aussi, dans le cas qui nous intéresse : l’audio.

Plusieurs points importants concernant la stéganographie et son application :  
  
*a. Embedding Capacity : Data is embedding in a larger data called cover or carriers file. The embedded capacity is the amount of data that can be hidden or embedded on the cover and will be compared to the cover size, because if the size of data that will be inserted on the cover is greater than the cover size then steganography can’t be done.*

*b. Undetectability: Data should be hidden or embedded into a carrier file in such way that any secret message or information can’t be seen accidentally in the original file by anybody.*

*c. Robustness: This is the capability of the embedding algorithm to store embedded data even after going through the process of compression and decompression a file.*

*d. Security: In most cases, security, including perception transparency of the hidden data is considered the most important issue of hiding data in any different formats. The definition of security in steganography cases is as likely to be embedded secret messages unknown to outsider people that have no connection between sender and recipients.*

*e. Tamper Resistance: Resistance to intentional malfunction or sabotage of a product or system by users that have access to it. One of the important things for steganography is how strong the carrier file that used for embedding a secret message or file will not easy to be cracked by users.*

Stéganographie sonore :

”Audio Steganography: Human Auditory System(HAS) is more sensitive than Human Visual System(HVS), that is one of the reasons that makes embedding message in audio file in any different method is more difficult than other formats.”

Règle d’or :   
volume des informations à cacher < 20-25% de la taille du fichier initial

Différentes méthodes utilisées :

1. LSB Coding
2. Parity Coding
3. Echo Data Hiding
4. Frequency modulation-based Steganography
5. Phase coding
6. Etc…

Différents formats possibles :

1. MP3
2. WAV
3. FLAC
4. MIDI
5. Etc…

* LSB Coding:

The least significant byte of carrier file is replaced with the bytes of the secret message. Generally, the rightmost bit is chosen for the replacement, because considered as the LSB as it has the least impact on the quality of file.

* Parity Coding:

Most robust approach. Parity coding is one of the most robust audio steganographic approach. In place of breaking a signal into individual samples, this approach breaks a signal into separate samples and inserts each bit of the confidential information from a parity bit. If the parity bit of a chosen region does not match the secret bit to be encoded, the procedure inverts the LSB of one of the samples in the region. Hence, the sender has different choices in encoding the secret bit.

* Echo data hiding:

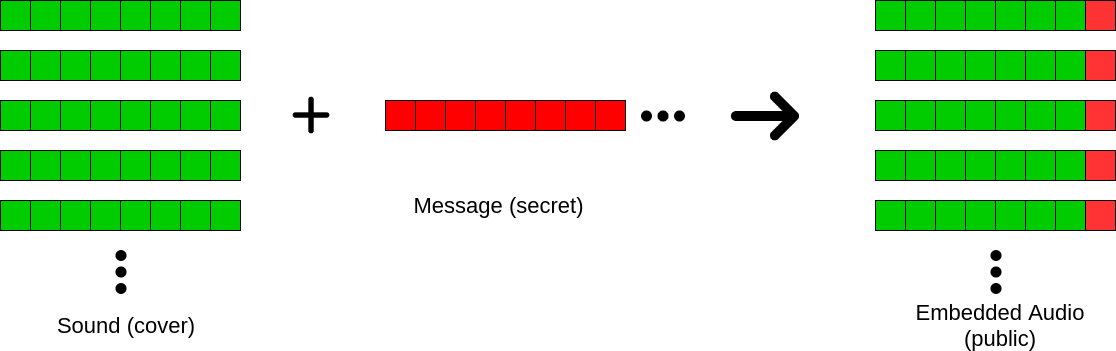
Inserts confidential information in a sound file by presenting an echo into the discrete signal. Echo hiding has benefits of delivering a high data transmission rate. Only one bit of confidential information could be encoded if only one echo was created from the original signal. Therefore, before the encoding procedure begins the original signal is broken down into blocks. When the encoding procedure is done, the blocks are concatenated back together to deliver the final signal.

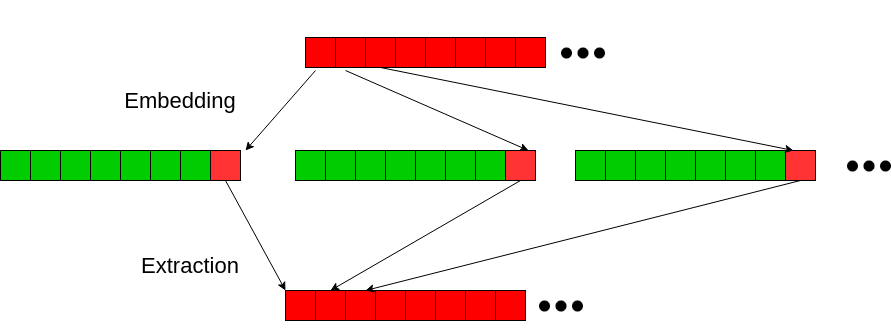
* Frequency Modulation based Steganography

The main idea of this algorithm is that we will conceal our secret audio in the near-ultrasound range while keeping our public audio data in the normal hearing range.

# LSB Coding :

In the simplistic form, LSB algorithm replaces the LSB of each byte in the “carrier” data with one bit from the “secret” message. This concept is visualized in the diagram below.

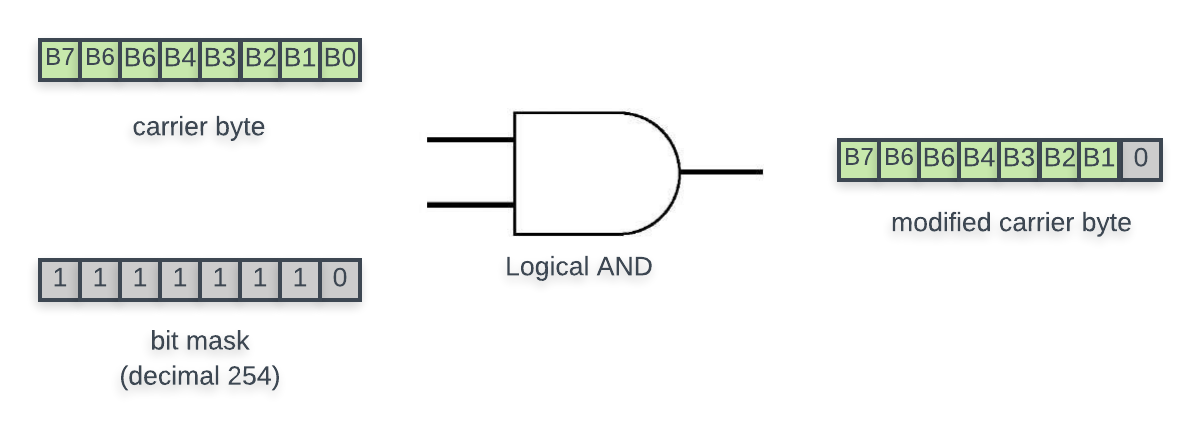
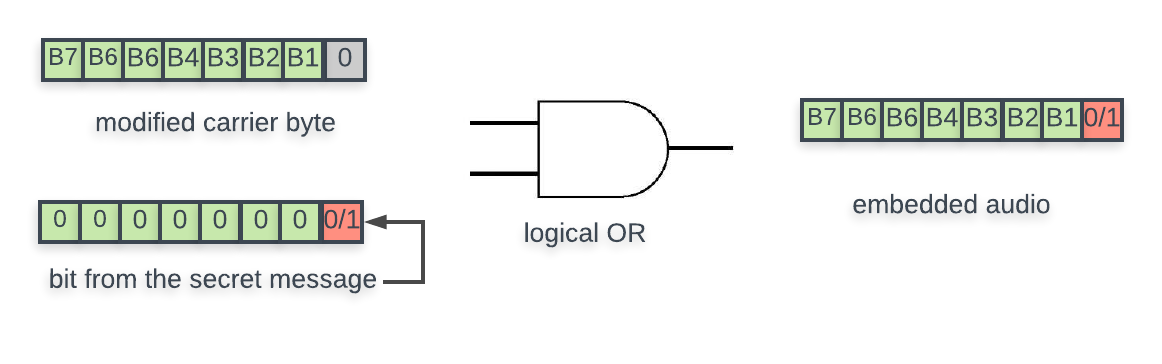


The sender performs “embedding” of the bits of secret messages onto the carrier data byte-by-byte. Whereas the receiver performs the “extraction” procedure by reading LSB bits of each byte of received data, this way the receiver reconstructs the secret message.

The main idea here is that we are trying to exploit the human perception of the integrity of the carrier signal. LSB steganography is very popular for Image Steganography. And the change in LSB affects the color just so slightly that the change in color is not generally perceptible to the human eye. However, the human ear is more sensitive to slights changes in sound and hence the “noise” that we are adding would have a higher chance of being noticed.

Implementation:

We will perform logical AND operation between each byte of carrier audio (the “song”) and a bit mask that resets the LSB of carrier byte.

Then we will perform a simple logical OR operation between the modified carrier byte and the next bit (0 or 1) from the secret message.

# Quels formats audios ?

Le grand problème de la stéganographie sonore réside dans le fait que l’oreille humaine est bien plus sensible que sa vue, et donc, il faut faire très attention à ne pas trop altérer un son sinon l’oreille humaine sera capable d’entendre la différence avec le son d’origine. Le choix du format est donc assez important. Choisir du WAV (non compressé) permet plus de modification possible sans trop en altérer la qualité (donc plus simple) mais est bien plus dur à échanger dut à son poids par rapport à du MP3.

Format WAV :

Un fichier audio non compressé est enregistré par défaut au format WAV. Un son d'une minute peut occuper entre 644Ko et 27Mo. La taille de ce fichier dépend de la fréquence d'échantillonnage, du type de son (mono ou stéréo) et du nombre de bits utilisés pour l'échantillonnage (8 ou 16 bits).

Structure d'un fichier WAV :

Le taux d'échantillonnage peut varier entre 11kHz, 22kHZ et 44kHz, avec un échantillonnage sur 8 ou 16 bits.

Le volume d'un fichier WAV stéréo pour 1 minute échantillonné à 44kHz en 16 bit est de :

60 (secondes) \* 44000 (taux d'échantillonnage) \* 2 (stéréo) \* 2 (16 bits = 2 octets) = 10.56Mo.

En comparaison, un morceau de musique compressé en MP3 à 128kbps et à 44kHz a une taille de 3Mo environ (pour 3 à 4 minutes), soit environ 1Mo par minute. Pour un fichier compressé par divers procédés et dans divers formats (MP3, OGG, ...), on donne habituellement une valeur en kbps qui est en rapport avec le taux de compression (et donc le taux de perte).

Si on fait le calcul, on trouve qu'un WAV 44Khz / 16bits / Stéréo est à 1375Kbps. Donc, un MP3 compressé à 128Kbps a un taux de compression de 11 pour 1.

Format MP3 :

**La compression MP3**

**Une compression destructrice,**c'est une compression qui est réalisée en perdant de l'information. Cela signifie que si l'on décompresse le signal compressé à l'aide d'une telle technique, on ne retrouvera pas le signal de départ.

**Parmi les techniques de compression destructrices,**on a essentiellement des méthodes qui exploitent les propriétés de l'oreille humaine. Cette dernière entend les fréquences situées dans la gamme 20Hz à 20kHz. Si un morceau contient des fréquences hors de cette gamme, on peut donc purement et simplement les supprimer sans perte de qualité audio puisque l'oreille ne les entend pas. En fait, on entend surtout correctement les fréquences situées dans la gamme 2kHz à 5kHz. En effet, il faut moins de 5dB pour entendre les fréquences de cette bande alors qu'il faut plus de 20dB pour entendre les fréquences situées en dessous de 100Hz ou au-dessus de 10kHZ. Ces constatations peuvent être exploitées pour réduire la taille des fichiers. On peut par exemple décider que toutes les fréquences au-dessus de 15kHz seront supprimées.

Le MP3 utilise aussi le **principe des fréquences masquées.**Si dans un groupe de fréquences, certaines ont un niveau sonore beaucoup plus élevé que d'autres, il n'est pas nécessaire de conserver les fréquences de niveau sonore faible : on ne les entendra pas. Enfin, si les deux voies d'un son stéréo présentent des séquences semblables, au lieu de dupliquer ces séquences, on en stocke évidemment qu'une et l'information qu'à ce moment-là, voie droite et voie gauche sont identiques.

Le MP3 utilise également **l'algorithme de Huffman (1952)**comme méthode de codage des informations. Cette méthode est utilisée dans tous les algorithmes de compression (compression de fichiers texte, compression d'images, compression de sons). Elle repose sur l'utilisation d'un code de longueur variable et la probabilité d'apparition d'un événement (en l'occurrence ici d'une fréquence). Plus une fréquence apparaît souvent, plus son code sera court (nombre de bits faible pour la représenter). Le fichier est lu une 1ère fois et on dresse un tableau des fréquences apparaissant et le nombre de fois où elles apparaissent. On en déduit le code approprié. Ce codage est utilisé en dernier lieu. C'est la phase finale de la compression. C'est un codage non destructeur.

**Le MP3 exploite en 1er lieu les propriétés de l'oreille pour réduire la taille d'un morceau, puis on traite l'aspect stéréo et enfin on applique des codages en terminant par le codage de Huffman.**