ISSN 2007-9737

# LSB Algorithm to Hide Text in an Audio Signal

Bárbara Emma Sánchez Rinza[1], L. Gerardo Munive Morales[1], Alberto Jaramillo Núñez[2]

[1] Benemérita Universidad Autónoma de Puebla,
Facultad de Ciencias de la Computación Puebla,
Mexico

[2] Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE),
Departamento de Óptica, Puebla,
Mexico

brinza@hotmail.com

**Abstract.** The following work is to hide a text in an audio file using steganography employing the LSB algorithm. 3 melodies of different genres are used to see by which of the 3, the information is best hidden, without there being any noise in the melody that will contain the hidden message. This is quite important in steganography because it is required that information goes unnoticed. To do so, we programmed in Matlab, and in this case, our hidden message contains around 9429 characters.

**Keywords.**, Steganography, cryptography, WAV, information security.

## 1 Introduction

The word steganography comes from the Greek steganos (covered or secret) and graph (write or paint). It is the science of hiding information in a manner the existence of hidden message goes unnoticed, it allows us to use a variety of containers and algorithms to hide the information that wants to send, with this we only are recovered by a legitimate user who knows an algorithm for extracting the same. It is necessary to mention the difference between steganography and cryptology, that because a large number of occasions both concepts are combined to achieve greater protection to information as a result are often confused.

On the other hand, cryptography handles to encrypt and encode information so it is unintelligible, why is combined with steganography, so be encrypted and hidden information.

Once you have understood the difference between these sciences identify the various actors involved in the field of steganography:

a. Container Object: This is the entity that is used to carry the hidden message.

b. Stego-object: This is the container plus the object's hidden message.

c. Adversary: All those entities that are hidden information.

d. Steganalysis: The science of detection (passive attack) and/or cancellation (active attacks) of information hidden in different stego-objects, and the ability to locate useful information within the same (existence and size).

## 2 Development

This work focuses on 2 applications of steganography: confidential communication and storage of secret data and the protection of data alteration, in the same way, use an audio file with WAV format as a container object, because this file type is not a compressed format like MP3, as result, the WAV is a large file, which allows us to hide more data. The system to be developed will allow us to hide information (plain text) into a WAV audio file format, just as the reverse may be applied to obtain the data hidden process as shown in Figure1.

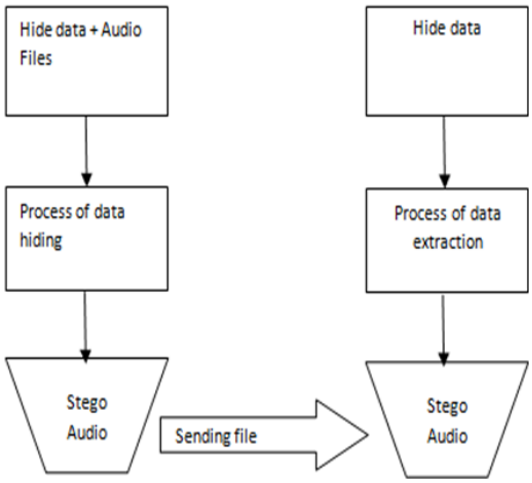


**Fig. 1.** Diagram of the overall system performance

In the diagram above, we can see the two processes that may carry out the system, except the "Send File", this complete user depend, during the concealment of data applies a steganographic algorithm to a container object, in this case, will be the LSB algorithm and the container object is an audio file in WAV format, as a result of this process, a stego-audio (i.e. when data are within the audio file) is obtained. In simpler words, the system will produce the stego-audio linking the text you want to hide, which is entered through a window in the system by the user and an audio file, just as the system will process the audio stego for hidden data. To hide information within the audio file will apply the algorithm LSB (Least Significant Bit), which is explained below.

## 3 LSB Algorithm

Like images, sound files can be modified so that they contain hidden information, such as copyright information; these modifications must be made so that a hacker cannot eliminate it, at least not without destroying the original signal. Methods incorporating data into sound files using the properties of the human auditory system (HAS).

The HAS perceives the additive random noise and disturbances in a sound file can also be detected. But there are some "holes" that may explode. While the SAH has a large dynamic range, which has a rather small differential range.

Replacing the least significant bit is the easiest way to embed information into a digital audio file. By replacing the least significant bit of each sample point with a binary message, LSB encoding allows a large amount of data to be encoded. LSB encoding, the transmission rate ideal data is 1 kbps by 1 kHz. In some implementations of LSB encoding, however, the two least significant bits of a sample are replaced with two message bits.

This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file. A new method that increases the maximum limit of four bits to extract a secret message from a sound file encoded LSB, the receiver needs access to the sequence of sample indices used in the process of embedding. Normally, the length of the secret message to be encoded is less than the total number of samples in a sound file.

One must then decide on how to choose the subset of samples containing the secret message and communicate that decision to the receiver. A trivial technique is to start at the beginning of the sound file and perform coding LSB until the message has been completely embedded, leaving the remaining samples unchanged.

This creates a security problem, however, in that the first part of the sound file will have different statistical properties than the second part of the sound file that has not changed.

A solution to this problem is to fill the secret message with random bits so that the message length is equal to the total number of samples. An example of how these algorithms works are shown in Figure 2.

There are two main disadvantages associated with the use of methods as LSB coding. The human ear is very sensitive and can often detect the minimum noise introduced into an audio file, second disadvantage is that it is not robust. If a sound file integrated with a secret message using LSB coding was resampled, the embedded information be lost.

Robustness can be improved somewhat by using a technique of redundancy while encoding the secret message. However, redundancy techniques reduce the transmission rate of data significantly.

## 4 Flow Diagram

As mentioned previously this system should allow the hide and extract information from a WAV audio file format, the following flowcharts help us understand in more detail how these processes work.

Figure 3 shows the first flowchart, in which we can observe the different processes that occur to generate the stego-audio

As can be seen from the above diagram (Figure 3) the system forces the selected audio file as a container object is properly formatted, otherwise not allowed to continue with the steganographic process, so with the text that is will hide, it will enter through a box, if this box is empty, the process does not continue, once you have selected the appropriate file and entered the information the steganographic process is carried out by generating so the stego-audio.

Now in the following diagram shown in Figure 3, we see how the hidden information is obtained.

Looking at the diagram above Figure 4 we can see that for the information can hide a single process is needed, also verified that the audio file is in the correct format, otherwise, you cannot continue with the process.

## 5 USER Interface

It is time to define the user interface, it has to be simple and intuitive to facilitate the use of the system to the user. In Figure 5 we can see the main window.

In this window we have five fundamental elements, the number one shows the operations you can perform system (hide and extract data), the number two found the "Hide Data" button, which when performing such action applies the algorithm LSB for hiding data in the container object, then at number three we found a text box, which will place the information you want to hide, the fourth element allows us to select the wave file to perform any operation mentioned in one element, finally, the item number five found a small text box which provides user help.

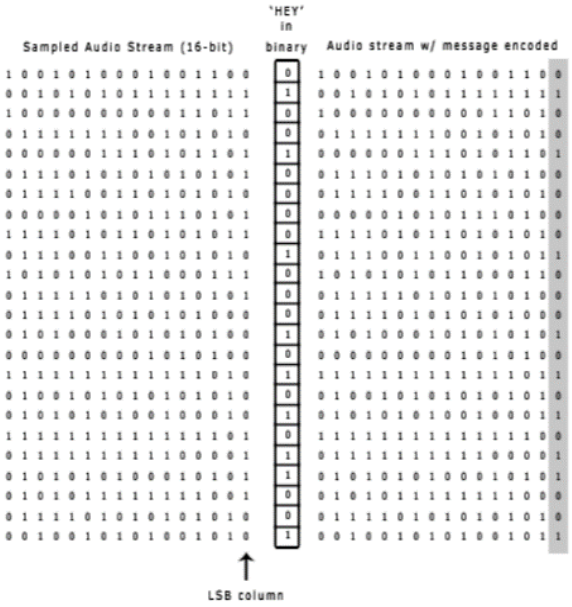


**Fig. 2.** Algorithm LSB

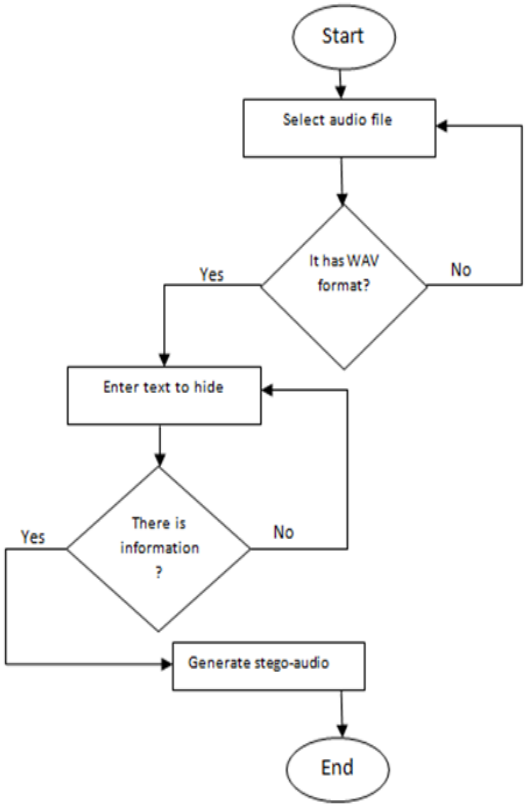


**Fig. 3.** Generating stego-audio

ISSN 2007-9737



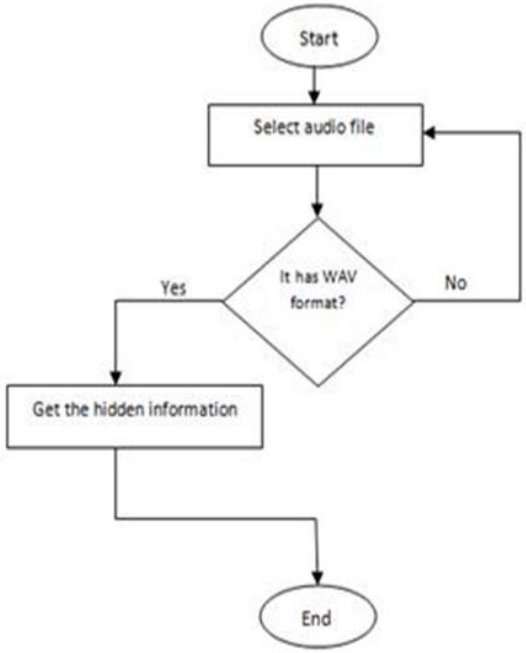


**Fig. 4.** Generating the hidden data

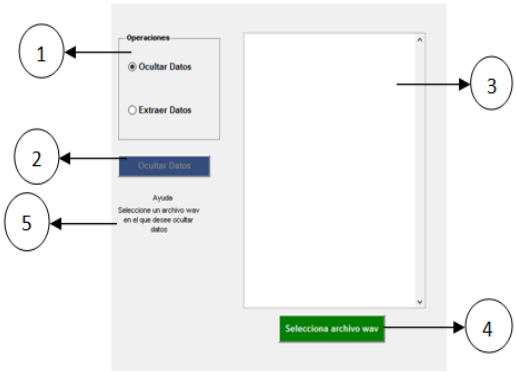


**Fig. 5.** Main Screen

**Table 1.** List of Audio Files

| Title | Artist | Musical genre |
|---|---|---|
| O Sole Mio | David Garrett | Instrumental |
| Moments | Noel Schajris | Pop |
| Before I Forget | Slipknot | Nü Metal |

## 6 Results

In the present work is accomplished hide text within an audio file, through the application of a steganographic algorithm, the audio file suffered minor modifications, now what remains is whether those changes affected somehow audio quality, raising suspicions about the contents of this file.

This analysis is necessary because, as mentioned previously the main objective of steganography is to hide information within a container object so that the content of the object passes unnoticed.

To test the efficiency of the system, data will be hidden in different audio files, that is to say, an instrumental song, a pop song, and finally, a rock song or nü metal, different amounts of data will be hidden will be used, they range from a couple of words to a complete text.

This is to verify that how much information can be hidden without affecting the quality of both audio and therefore know which "styles" are more viable for use as container objects.

Audio files that were chosen for the test are shown in Table 1. As you can see, these songs range from the quietest to the most "noisy". Each audio file will conceal 9429 characters and then get graphs in the frequency domain to analyze whether there is any difference between the original file and processing file, for it is necessary to determine a frequency range, this time will be used range between 100 and 3,000 Hz this is because the frequency range in which sound waves are perfectly audible.

First, a graph separately from the original audio and containing hidden data is obtained, finally, both files are graphed simultaneously to check for discrepancies between the two, for this process took the Matlab software. First, the song O Sole Mio is analyzed, the results are seen in Figure 6.

By observing both graphs, the first does not contain the message and the second already contains the hidden message, we can see that there is no difference between them, but to check it let's compare both graphs, the results can be seen in Figure 7.

And despite a large amount of hidden information we can find no distortion, then will be discussed the song titled "Momentos", the graphs shown in Figure 8.

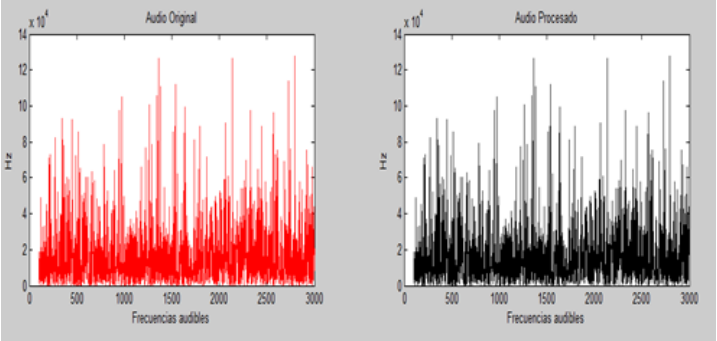


**Fig. 6.** Results of *O Sole Mio*

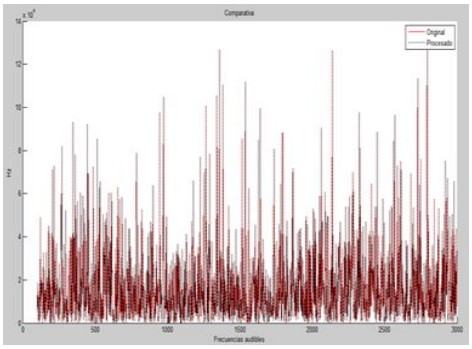

**Fig. 7.** Comparison of *O Sole Mio*

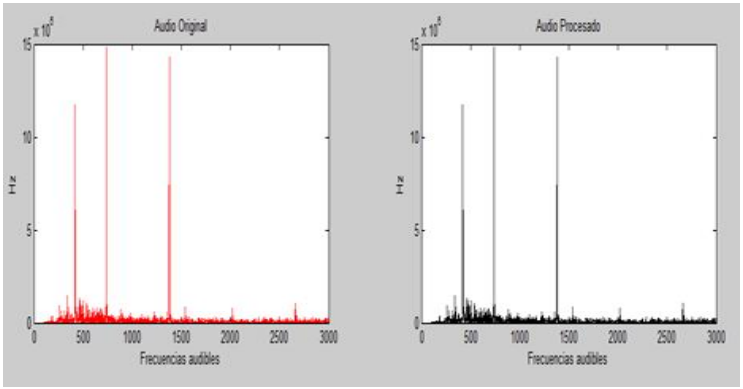


**Fig. 8.** Results of *Momentos*

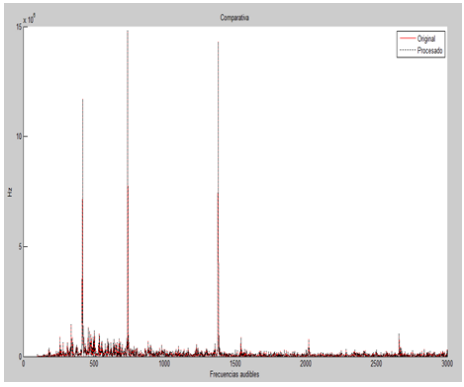

**Fig. 9.** Comparison of *Momentos*

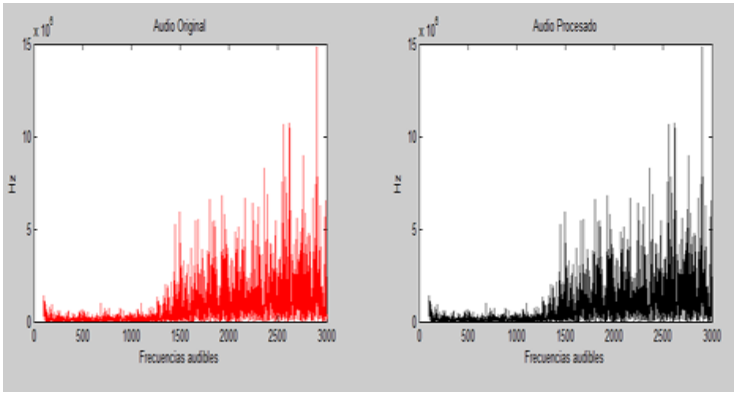


**Fig. 10.** Results of *Before I Forget*

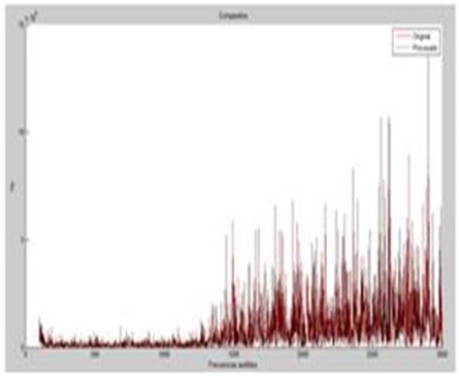

**Fig. 11.** Comparison of *Before I Forget*

There is no difference between the two files, to be sure we will compare the two graphs, and the result can be analyzed in Figure 9. By observing this comparison we can realize that there is still no difference between the two files, when the song does have not the information and when the song already has the hidden text. Finally, let us analyze the song Before I Forget, the resulting graphs are shown in Figure 10. It cannot be noticed the differences in the graphs, but were compared both graphs to be sure, the results are shown in Figure 11. When analyzing Figure 11 we can see that

indeed there is not some difference between the two files despite the great information that was hidden on the files.

## 7 Conclusion

As noted by hiding text within an audio file, the latter does not suffer alterations in audio quality in a range from 800 to 9429 characters, the only way that the contents can be altered is by altering in any way the container object. Similarly selecting three specific songs, we can see that any audio file is a good candidate for use as a container object.

Finally, when removing the hidden text, this is extracted almost perfectly except those letters contain special characters such as accents, umlauts, and tildes. Steganography is an effective method to hide information, which has been used throughout history.

We used the Matlab programming language to perform this work. We could appreciate a good performance of the program with very good results.

## References

1. **Nehru, G., Dhar, P. (2012).** A detailed look of audio steganography techniques using LSB and genetic algorithm approach. International Journal of Computer Science Issues (IJCSI), Vol. 9, No. 1, pp. 402–406.
2. **Díaz-Vico, J. (2010).** Esteganografía y estegoanálisis: Ocultación de datos en streams de audio vorbis. Master Dissertation Thesis, Facultad de Informática (UPM).
3. **Adhiya, K.P., Patil, S.A. (2012).** Hiding Text in Audio Using LSB Based Steganography. Information and Knowledge Management, Vol. 2, No. 3, pp. 8–15.
4. **Afrakhteh, M. (2010),** Steganography based on utilizing more surrounding pixels. Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, pp. 1–94.
5. **Wu, D.C., Tsai, W.H. (2013).** A steganography method for images by pixel-value differencing. Pattern Recognition Letters, Vol. 24, No. 9-10, pp. 1613–1626. DOI: 10.1016/S0167-8655 (02)00402-6.
6. **Malviya, S., Saxena, M., Khare, D.A. (2012).** Audio steganography by different method. International Journal of Emerging Technology and Advanced Engineering, Vol. 2, No. 7.
7. **Jayaram, P., Ranganatha, H.R., Anupama, H.S. (2011).** Information hiding using audio steganography – A survey. The International Journal of Multimedia & Its Applications (IJMA) Vol. 3, No. 3. DOI: 10.5121/ijma.2011.3308.
8. **Carvajal-Gámez, B.E. (2008).** Técnica de inserción de información en video aprovechando el mismo ancho de banda. Master Dissertation Thesis, Instituto Politécnico Nacional.
9. **Sánchez-Rinza, B.E., Morales-Salgado, M.R.G., Cortez-Olguín, C.O. (2015).** Security system for sending information containing hidden voice data by steganography (SIOVE) using MatLab. International Journal of Engineering and Innovative Technology (IJEIT), Vol. 5, No. 1. DOI: 10.17605/OSF.IO/GEYMJ.

*Article received on 29/07/2021; accepted on 30/09/2021.*
*Corresponding author is L. Gerardo Munive Morales.*