

# Técnicas de Eseganografía en señales de habla.

Darío A. Villarreal, Esteban Zeller y Matías A. Eberhardt

*Trabajo Práctico Final de Procesamiento Digital de Señales, II-FICH-UNL.*

**Resumen**—En este trabajo haremos una breve clasificación de las técnicas de esteganografía existentes y su diferenciación con otras disciplinas de protección de datos digitales. Luego describiremos e implementaremos dos de dichas técnicas: Modificación del Bit Menos Significativo (LSB, Least Significant Bit) en el dominio temporal y en el dominio frecuencial se ocultará la información en los coeficientes de la Transformada Wavelet Discreta. Finalmente evaluaremos los resultados obtenidos mediante técnicas objetivas y subjetivas.

**Palabras clave**—esteganografía, data hiding, watermarking

## I. INTRODUCCIÓN

La esteganografía es una disciplina que se basa en ocultar mensajes u objetos dentro de otros llamados portadores de modo que su inclusión pase desapercibida. Básicamente explota las limitaciones de la percepción humana, ya que nuestros sentidos presentan límites para percibir pequeñas alteraciones en las señales.

## II. DISCIPLINAS DE PROTECCIÓN DE DATOS DIGITALES

Encriptación vs Esteganografía vs Watermarking

## III. CLASIFICACIÓN DE MÉTODOS ESTEGANOGRÁFICOS

### IV. IMPLEMENTACIÓN EN EL DOMINIO TEMPORAL

### V. IMPLEMENTACIÓN EN EL DOMINIO FRECUENCIAL

## VI. EVALUACIÓN DE RESULTADOS

## VII. CONCLUSIONES

## REFERENCIAS

- [1] A. Delforouzi y M. Pooyan, "Adaptive Digital Audio Steganography Based on Integer Wavelet Transform." en *IIH-MSP*, B.-Y. Liao, J.-S. Pan, L. C. Jain, M. Liao, H. Noda, y A. T. S. Ho, Eds., pp. 283–286. IEEE, 2007. [Online]. Disponible: <http://dblp.uni-trier.de/db/conf/iih-msp/iih-msp2007.html#DelforouziP07>
- [2] N. Cvejic y T. Seppänen, "Increasing the capacity of LSB-based audio steganography." en *IEEE Workshop on Multimedia Signal Processing*, pp. 336–338. IEEE, 2002. [Online]. Disponible: <http://dblp.uni-trier.de/db/conf/IEEEmsp/msp2002.html#CvejicS02>
- [3] F. Djebbar y B. Ayad, "Comparative Study of Digital Audio Steganography Techniques." *EURASIP J. Audio, Speech and Music Processing*, vol. 2012, p. 25, 2012. [Online]. Disponible: <http://dblp.uni-trier.de/db/journals/ejasp/ejasp2012.html#DjebbarA12>
- [4] R. J. Anderson y F. A. P. Petitcolas, "On the limits of steganography." *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 474–481, 1998. [Online]. Disponible: <http://dblp.uni-trier.de/db/journals/jsac/jsac16.html#AndersonP98>
- [5] M. Asad, J. Gilani, y A. Khalid, "An enhanced least significant bit modification technique for audio steganography," en *Computer Networks and Information Technology (ICCNIT), 2011 International Conference on*, pp. 143–147, July 2011.
- [6] Y. Huang, C. Liu, S. Tang, y S. Bai, "Steganography Integration Into a Low-Bit Rate Speech Codec." *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1865–1875, 2012. [Online]. Disponible: <http://dblp.uni-trier.de/db/journals/tifs/tifs7.html#HuangLTB12>
- [7] N. Cvejic y T. Seppänen, "A wavelet domain LSB insertion algorithm for high capacity audio steganography," en *Digital Signal Processing Workshop, 2002 and the 2nd Signal Processing Education Workshop. Proceedings of 2002 IEEE 10th*, pp. 53–55, Oct 2002.
- [8] S. Shirali-Shahreza y M. Manzuri-Shalmani, "High capacity error free wavelet Domain Speech Steganography," en *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, pp. 1729–1732, March 2008.