Técnicas de Eseganografía en señales de audio.

Darío A. Villarreal, Esteban J. 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 decribiremos 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 Tranformada Wavelet Discreta. Finalmente evaluaremos los resultados obtenidos mediante técnicas objetivas y subjetivas.**

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

I. Introducción

La esteganografía es una disciplina que se dedica a 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. Pese a que es usada desde la antigüedad, esta disciplina ha suscitado mucho interés en las últimas décadas, especialmente en el área de la seguridad de la información dado el crecimiento del uso de la red de comunicaciones. La gran cantidad de información digital que circula en ella ha hecho que profesionales de la industria e investigadores prestaran especial atención en la seguridad de los datos digitales, siendo las principales disciplinas la criptografía, esteganografía y watermarking.

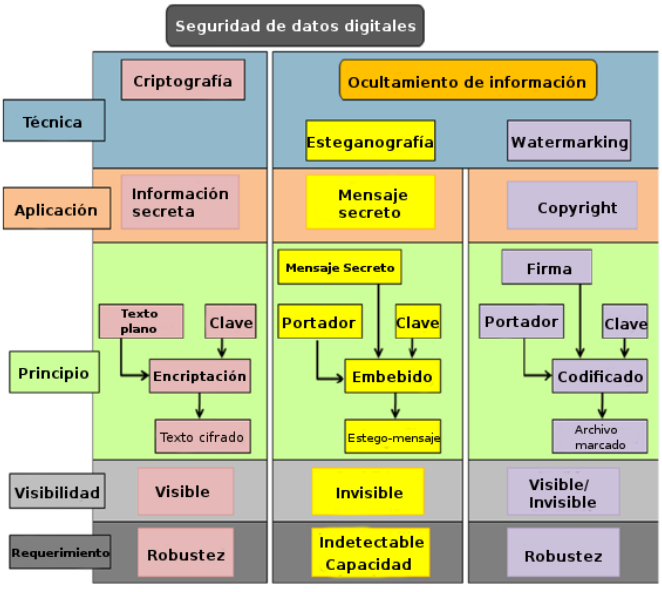

Fig. 1. Disciplinas de segudidad de datos digitales

La criptografía busca evitar que cierta información pueda ser leída por personas sin autorización, por lo que su principal requerimiento es la robustez ante los intentos de descifrado. El watermarking busca dejar una huella (visible o invisible) identificable y robusta ante ataques y compresión en imágenes, audio y vídeo. Para el diseño de técnicas esteganográficas los tres parámetros a tener en cuenta son la capacidad de ocultamiento de información, la imperceptibilidad y la robustez, pero es imposible obtenerlos al mismo tiempo. Por ejemplo, los métodos con más capacidad son sensibles al ruido y la compresión, mientras que los métodos robustos presentan una baja capacidad de ocultamiento de información.

Entre las aplicaciones prácticas de la esteganografía digital se encuentran la conunicación encubierta, inclusión de copyright en archivos multimedia, ocultar ejecutables para obtener datos de uso o acceso a un equipo remoto, entre otros.

En este trabajo repasaremos brevemente las principales técnicas de esteganografía digital en archivos de audio, luego implementaremos dos de ellas y finalmente analizaremos los resultados obtenidos.

II. Clasificación de métodos esteganográficos

A. En el dominio del tiempo

1) Bit menos significativo: Se trata de embeber la información modificando los bits menos significativos de una señal. Presenta imperceptibilidad con una alta capacidad de ocultamiento de información. Dado que es el método mas simple, la seguridad del canal de información se ve fácilmente comprometida bajo un simple análisis de los bits menos significativos. Para evitar que la información pueda ser reconstruida por personas sin autorización, se pueden tomar las siguientes medidas: encriptar el mensaje antes de su embebido, seleccionar el bit a codificar y el siguiente frame que contandrá información mediante los bits mas significativos del frame. El método es muy suceptible a ruidos, compresión y filtrado, los cuales eliminan o deterioran el mensaje oculto.

2) Echo hidding: Esta técnica se basa en introducir pequeños ecos en la señal portadora, mediante la convolución en el tiempo con un impulso determinado, quedando la señal con las mismas características estadísticas y perceptivas. La información es ocultada manipulando tres parámetros de la señal de eco: la amplitud inicial, el offset y la tasa de decaimiento. Esta técnica prácticamente no es utilizada debido a su baja capacidad de embebido y robustez.

3) Intérvalos de silencio: Este método consiste en embeber la información en los intervalos de silencio en una señal de habla. Primero se determina la cantidad y duración de dichos intervalos en muestras para luego disminuir su duración restándole x cantidad de muestras, donde $0 < x < 2^{nbits}$ y $nbits$ es la cantidad de bits necesarios para representar un valor del mensaje a ocultar. En el proceso de extracción, se calcula el módulo entre la longitud del intervalo y nbits para recuperar el valor oculto. Este metodo presenta una alta imperceptibilidad, pero baja capacidad.

Presenta robustez antes ruido y filtrado, pero no ante algunos algoritmos de compresión.

B. En el dominio de la frecuencia

1) Magnitud del espectro:
2) Inserción de tono:
3) Espectro de fase:
4) Amplio espectro:
5) Dominio Cepstral:
6) Wavelets:

C. En la codificación/decodificación

1) Modicicación de los codebooks:
2) Ocultamiento en el fujo de bits:

III. Implementación en el dominio temporal

IV. Implementación en el dominio frecuencial

V. Evaluación de resultados

VI. 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/ejasmp/ejasmp2012.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. Seppa?nen, "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.