Técnicas de Esteganografía 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, seguridad de la información**

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.

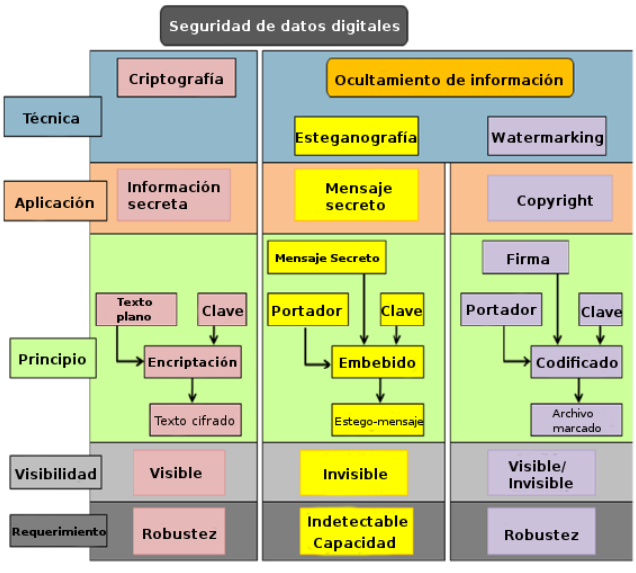

Fig. 1. Disciplinas de segudidad de datos digitales

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. Estos parámetros se grafican como los vértices de un triángulo equilátero, donde acercarse al cumplimiento de uno es alejarse de los otros. 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. Métodos esteganográficos [1]

A. En el dominio del tiempo

- Bit menos significativo (LSB)
  - Los bits menos significativos de cada muestra son reemplazados por la información a codificar
  - Ventajas: Simples de codificar. Alta capacidad de embebido
  - Desventajas: Fácil de extraer y destruir
  - Tasa de ocultado de información: 16kbps
- Echo hidding
  - Se incorporan ecos en el audio portador por convolución para embeber el mensaje.
  - Ventaja: Resistende a algoritmos de compresión con pérdida
  - Desventaja: Baja capacidad y seguridad.
  - Tasa de ocultado de información: 50bps
- Intérvalos de silencio
  - Se usa el número de muestras de los intervalos de silencio para esconder información.
  - Ventaja: Resistende a algoritmos de compresión con pérdida
  - Desventaja: Baja capacidad.
  - Tasa de ocultado de información: 64bps

B. En el dominio transformado

- Magnitud del espectro
  - Usa las bandas de frecuencia para ocultar información
  - Ventaja: Alta capacidad,
  - Desventaja: Baja robustez a manipulaciones simples de audio
  - Tasa de ocultado de información: 20kbps
- Inserción de tono

  - La información se codifica insertando tonos a frecuencias seleccionadas
  - Ventajas: Imperceptibilidad e indetectabilidad del mensaje embebido.
  - Desventaja: Baja capacidad. Los tonos son fácilmente detectables si se sospecha que hay información oculta, sería fácil reemplazar la información embebida.
  - Tasa de ocultado de información: 250bps
- Espectro de fase
  - Se modula la fase de la señal portadora.
  - Ventajas: Es robusto frente a manupulaciones del audio. Para recuperar la información se necesita la señal original.
  - Desventaja: Baja capacidad.
  - Tasa de ocultado de información: 333bps
- Dispersión en el espectro (spread spectrum)
  - Se dispersa la información a ocultar en todo el espectro de frecuencias.
  - Ventajas: Su alta redundancia la hace muy robusta ante distorsiones de la señal.
  - Desventaja: Vulnerable al modificado de la escala temporal de la señal
  - Tasa de ocultado de información: 20bps
- Dominio Cepstral
  - Se modifican los coeficientes cepstrales para embeber la señal.
  - Ventajas: Robusto ante operaciones de procesamiento de señales.
  - Desventaja: Incorpora distorsiones perceptibles.
  - Tasa de ocultado de información: 54bps
- Wavelets
  - Se modifican los coeficientes wavelets para codificar la información.
  - Ventajas: Alta capacidad de embebido.
  - Desventaja: Recuperación con pérdida de información.
  - Tasa de ocultado de información: 70kbps

C. En la codificación/decodificación

- Modificación de los codebooks
  - Se modifican los parámetros de los diccionarios de codificado y decodificado.
  - Ventaja: Robusto
  - Desventaja: Baja capacidad de embebido.
  - Tasa de ocultado de información: 2kbps
- Ocultamiento en el flujo de bits
  - Se le modifican los bits menos significativos del flujo de bits resultantes del proceso de codificado.
  - Ventaja: Robusto
  - Desventaja: Baja capacidad de embebido.
  - Tasa de ocultado de información: 1.6kbps

III. Implementación en el dominio temporal: Bit menos significativo (LSB)

La modificación LSB es una de las técnicas de esteganografía más simples y provee una alta capacidad. Esta ténica consiste en ocultar el mensaje en el o los bits menos significativos de cada muestra de audio. Incrementando el numero de bits a modificar se introduce mas ruido y si dicho ruido supera un determinado umbral es percibido y la técnica falla. Por lo tanto usando mas LSBs se incrementa la capacidad pero se pierde transparencia.

Dada su simplicidad, esta técnica de LSB es vulnerable al estegoanálisis. Realizando un análisis de la señal se podría detectar fácilmente el mensaje secreto. Para evitar que el mensaje pueda ser recuperado por un tercero se propone encriptar previamente le mensaje y utilizar una de las siguientes variantes o una conbinación de las mismas.

1) Seleccion de Bit: Esta técnica utiliza los primeros dos bits mas significativos (MSBs) de cada muestra para decidir que bit de la misma va a contener el bit del mensaje secreto. El mensaje secreto se ocultara en uno de los primeros tres LSBs de cada muestra.

Si los primeros dos MSBs de la muestra son iguales a 00, el tercer LSB sera reemplazado con un bit del mensaje secreto. Si los primeros dos MSBs de la muestra son iguales a 01, el segundo LSB sera reemplazado con un bit del mensaje secreto y si los dos primeros MSBs son 10 o 11, el primer bit sera reemplazado por un bit del mensaje secreto. De esta manera se introduce una aleatoriedad en la seleccion de los bits donde se ocultara el mensaje.

2) Seleccion de Muestra: Otra manera de agregar aleatoreidad es usar sólo algunas muestras de la señal para ocultar el mensaje, seleccionando la próxima muestra que contandrá el mensaje medinate los primeros tres MSBs de la muestra actual. Es decir si i es la muestra actual, los primeros tres MSBs de i determinaran el numero de muestras salteadas entre dos bits consecutivos del mensaje secreto. Por ejemplo si los primeros tres MSBs de la primera muestra ($i = 1$) son iguales a 010, entonces la proxima muestra que contendrá el siguiente bit del mensaje secreto sera $i + 3 = 4$. Luego, la próxima muestra estará determinada por los tres primeros MSBs de la muestra 4 y así sucesivamente. Este método brinda una mayor aleatoreidad que el anterior pero decrementa notablemente la capacidad.

IV. Implementación en el dominio transformado

Este método se basa en embeber la información en los bits menos significativos de los coeficientes enteros de la transformada wavelet discreta. En este trabajo utilizamos la familia de wavelets Haar por ser las mas simples, rápidas y eficientes en lo que al cálculo se refiere y la transformada LWT (Lifting Wavelet Transform) para obtener coeficientes enteros. En caso de no usar dicha transformada obtendríamos coeficientes reales y deberíamos escalarlos para su posterior pasaje a binario. Luego, para mejorar la imperceptibilidad se emplearon umbrales calculados sobre el tamaño del coeficiente embebiendo menos bits en coeficientes pequeños y evitando embeber información en los tramos silenciosos del archivo de audio.

$$Th_i = \begin{cases} nbits - fijos - 1 & si \quad C_i \geq 2^{nbits-1} \\ nbits - fijos - 3 & si \quad 2^{nbits-1} \geq C_i \geq 2^{nbits-3} \\ nbits - fijos - 5 & si \quad 2^{nbits-3} \geq C_i \geq 2^{nbits-5} \\ nbits - fijos - 7 & si \quad 2^{nbits-5} \geq C_i \geq 2^{nbits-7} \\ 0 \quad \text{en otro caso.} \end{cases}$$

Donde Th es el vector umbral que indica cuandos bits embeberemos en cada coeficiente, C es el vector de coeficientes, $nbits$ es el tamaño en bits del coeficiente wavelet entero, $fijos$ son los MSBs que no se tocarán. El vector Th calculado en

el decodificado del mensaje es igual al usado en el codificado, por lo que el mensaje es recuperado íntegro y sin necesidad de que el receptor conozca previemente este vector. Esto es interesante ya que el algoritmo se adaptará a la señal portadora para embeber la mayor cantidad de información posible sin comprometer la transparecia del codificado, logrando una gran capacidad e imperceptibilidad a la vez.

V. Evaluación de resultados

A. PEAQ

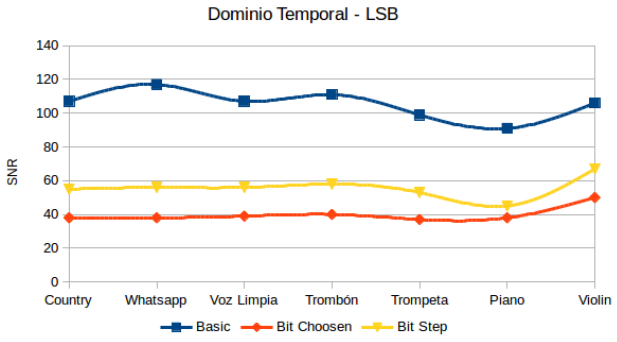

Fig. 2. Leyenda

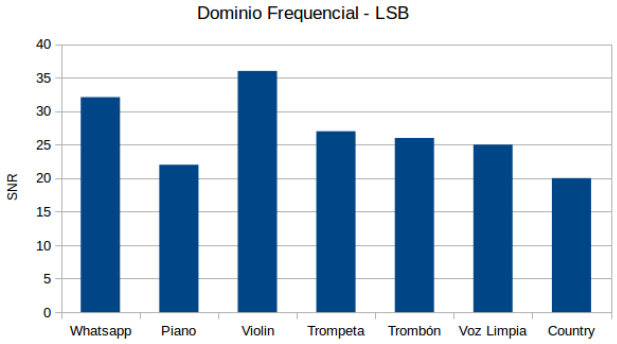

Fig. 3. Leyenda

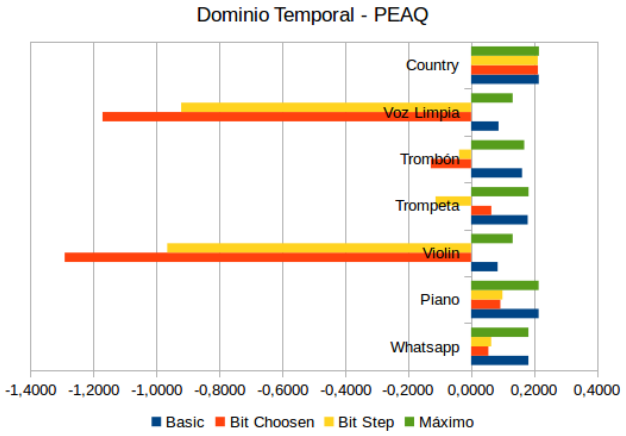

Fig. 4. Leyenda

VI. Conclusiones

Referencias

[1] 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

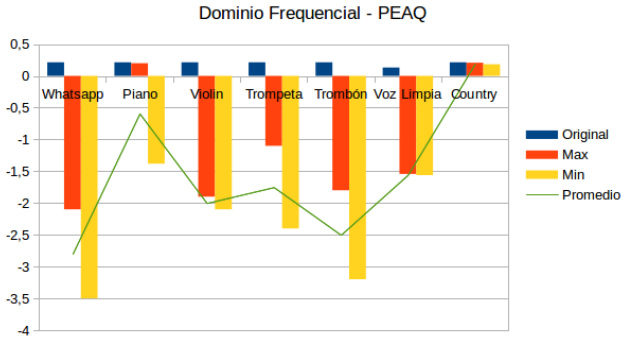

Fig. 5. Leyenda

[2] 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

[3] 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

[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.