

Audio Watermarking

Marcas de Agua en Audio Digital: Conceptos y aplicaciones

`emilia.gomez@iua.upf.es`

`http://www.iua.upf.es/mtg`


Esquema

- A. Introducción
- B. Watermarking
- C. Descripción de un sistema de marcas de agua
- D. Aplicaciones
- E. Fingerprinting vs watermarking
- F. Aplicación que utiliza las dos técnicas:
verificación de integridad

Motivación

- Posibilidad de copia sin pérdidas de un fichero en formato digital
- Se requieren tecnologías de protección del contenido audiovisual:
 - **Watermarking**: marcas de audio
 - **Fingerprinting**: identificación de audio
- Ejemplo: un compositor pone una obra en la web

Conceptos

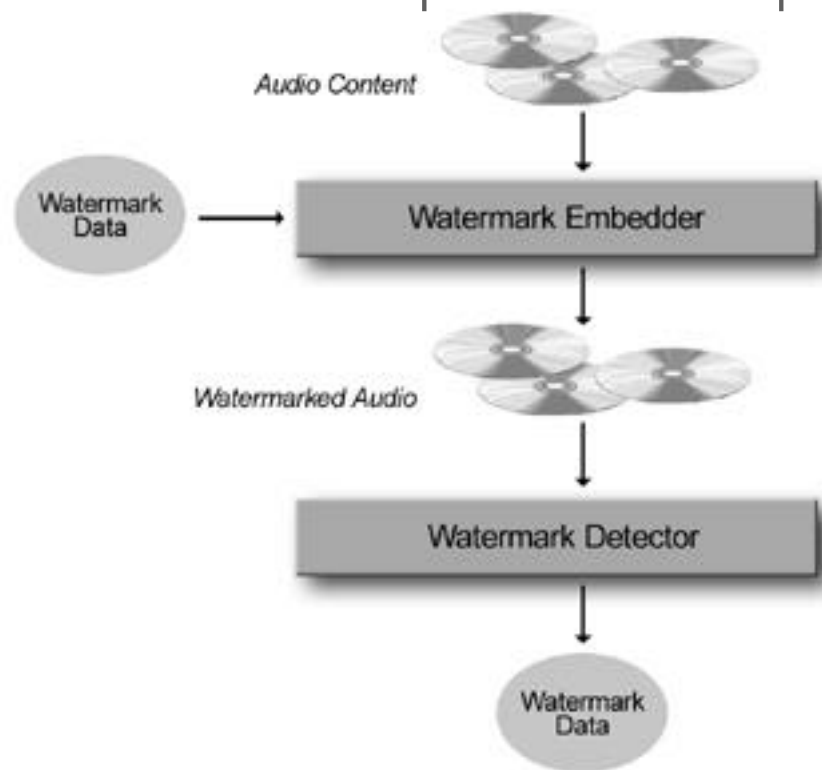
- Criptografía (*Cryptography*)
la información se cifra
 - Esteganografía (*Steganography*)
 - Comunicación punto a punto
 - Baja P_e en la transmisión
 - Marcas de agua (*Watermarking*)
 - Comunicación punto a multipunto
 - Robusto frente a ataques
 - Identificación (*Fingerprinting*)
tipo de watermarking (insertar una identificación única)
- 
- INFORMATION
HIDING**

Definición de Watermarking

- Insertar una marca (*watermark*) en la señal de audio: un **mensaje oculto**
- La marca se integra en la señal de audio: **no necesita espacio de almacenamiento**
- Puede contener cualquier información que se quiera (ISBN, información sobre el autor, estudio de grabación, cliente que compró la copia de la grabación...)
- Es inaudible, **indetectable**
- Puede leerse con el software adecuado

Ventajas

- Hacen posible que se pueda **establecer responsabilidad** sobre copias de un determinado trabajo en el dominio digital.
Ejemplo: este audio lo puso en Napster Pepito

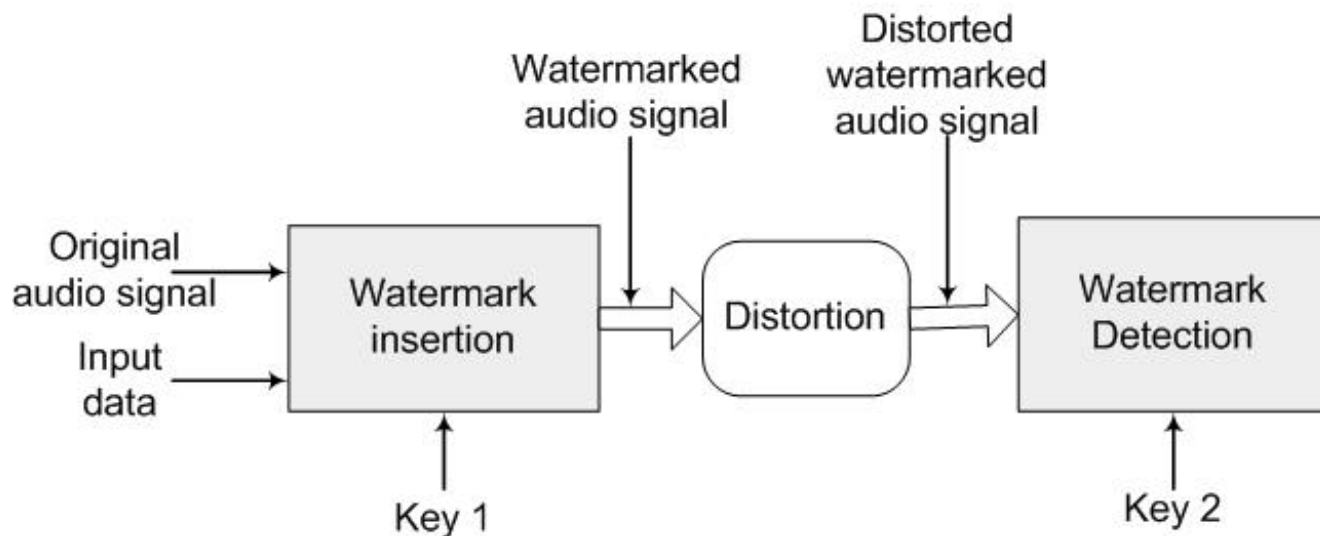


Historia del watermarking

- Herodoto 484-426 a.C.
- George Sand a Alfred de Musset S. XIX
- S. XX: Muchas publicaciones en *digital watermarking* de imágenes, desde los años 80.

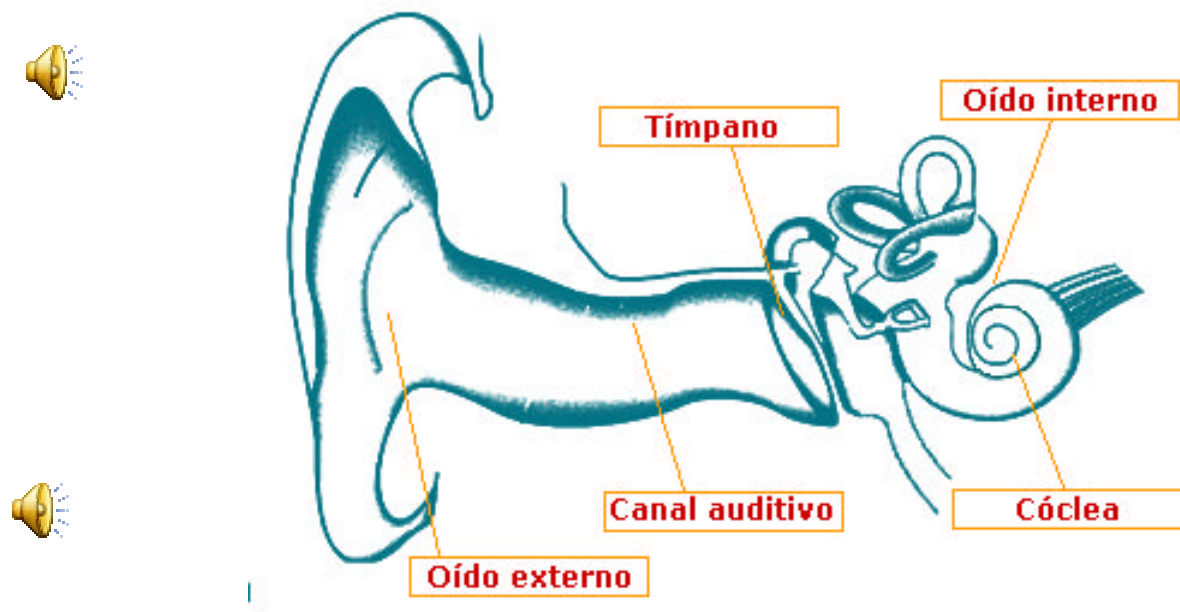
Propiedades del watermark

1. **Inaudible** (generalmente)
2. **Robusta** (transmisión, cambio de soporte, transmisión, etc)
 - Detectable únicamente por personas autorizadas
3. **Resistente** a ataques
 - Simétrico o asimétrico



1. Inaudible

El grado de audibilidad depende de la aplicación



Utilización de un modelo psicoacústico, que explota las características del sistema auditivo humano

2. Robusta

La marca debe ser robusta ante operaciones « *permitidas* »:

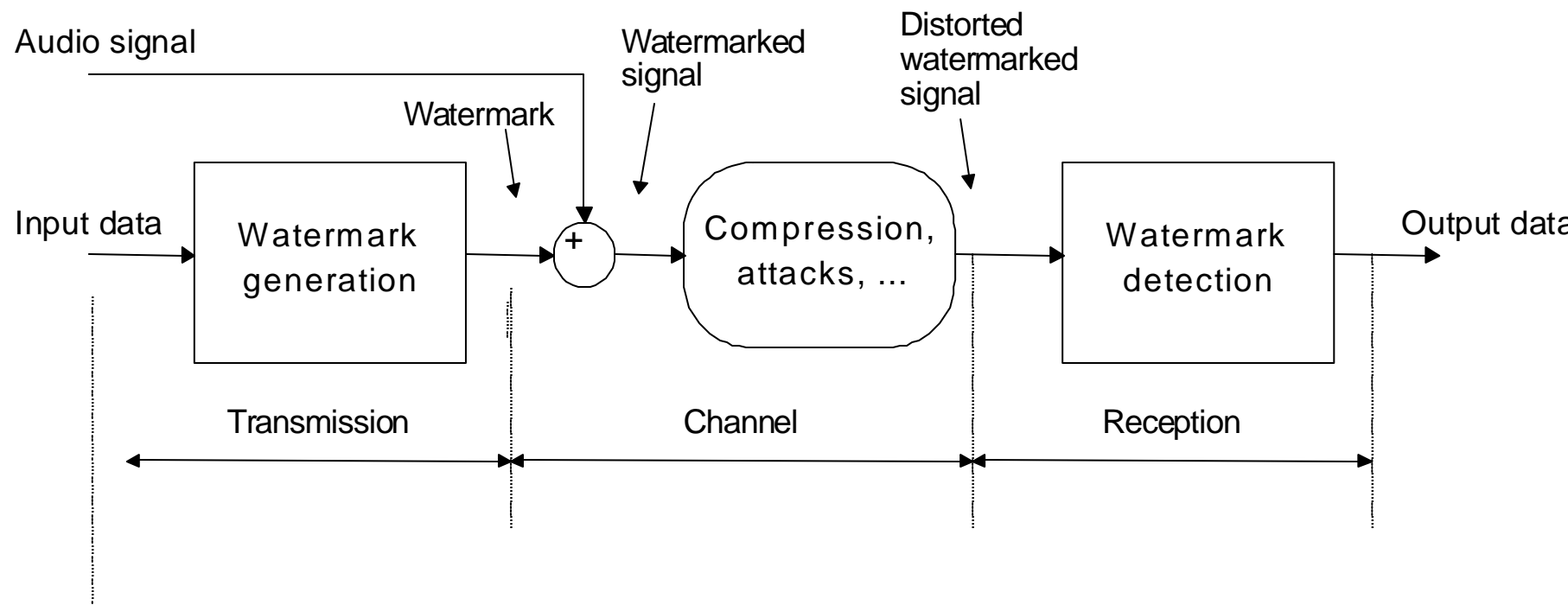
- Codificación
- Transmisión (ruido aditivo)
- Conversión AD/DA (cambio de soporte)
- Compresión (con o sin pérdidas, MPEG)



3. Resistente

- La marca debe ser resistente a ataques intencionados:
 - Que intenten eliminarlo
 - Que intenten hacer que no se pueda descodificar.
 - Que intenten modificar los datos de la marca.

Se puede ver como un canal de comunicación



Propiedades del canal

Fuerte ruido de canal

- Potencia de la señal de audio \gg potencia de la marca
- Audio: ruido fuertemente coloreado
- Ruido blanco de canal de transmisión
- Distorsiones (compresión MP3, AD/DA conversion, ...)
- Ataques *intencionados*

$$\frac{S_w^2}{S_x^2} \approx -20dB, \text{ ancho de banda } W \approx 20 \text{ kHz}$$

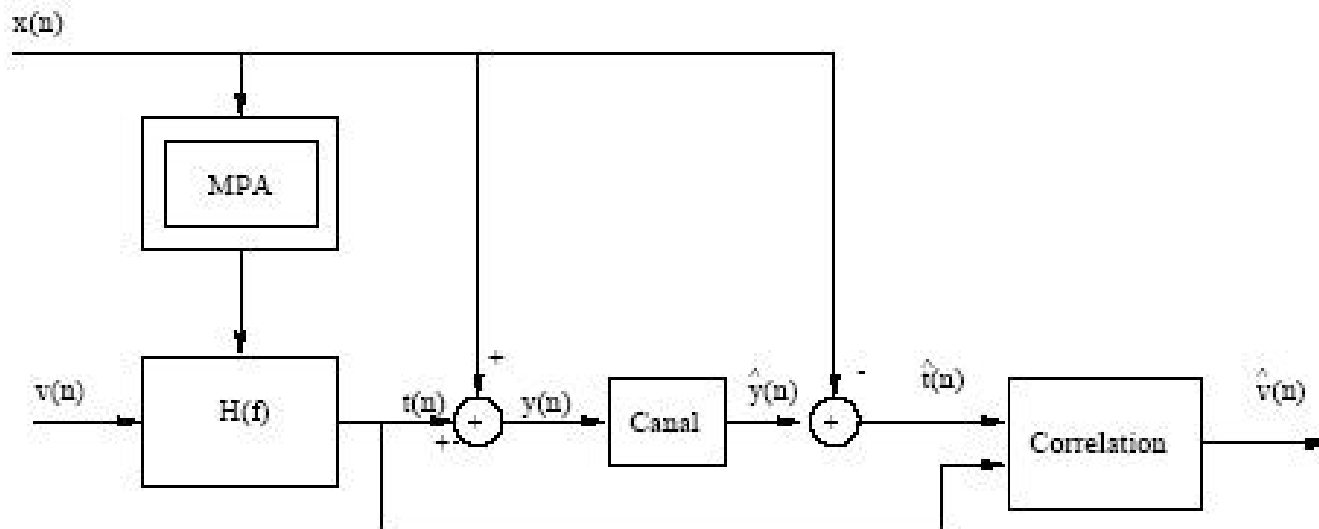
En teoría \Rightarrow Rate $R = W \log_2(1+SNR) \approx 300 \text{ bps}$

Simulaciones : $R \approx 100 \text{ bit/s}$

Aproximaciones al problema

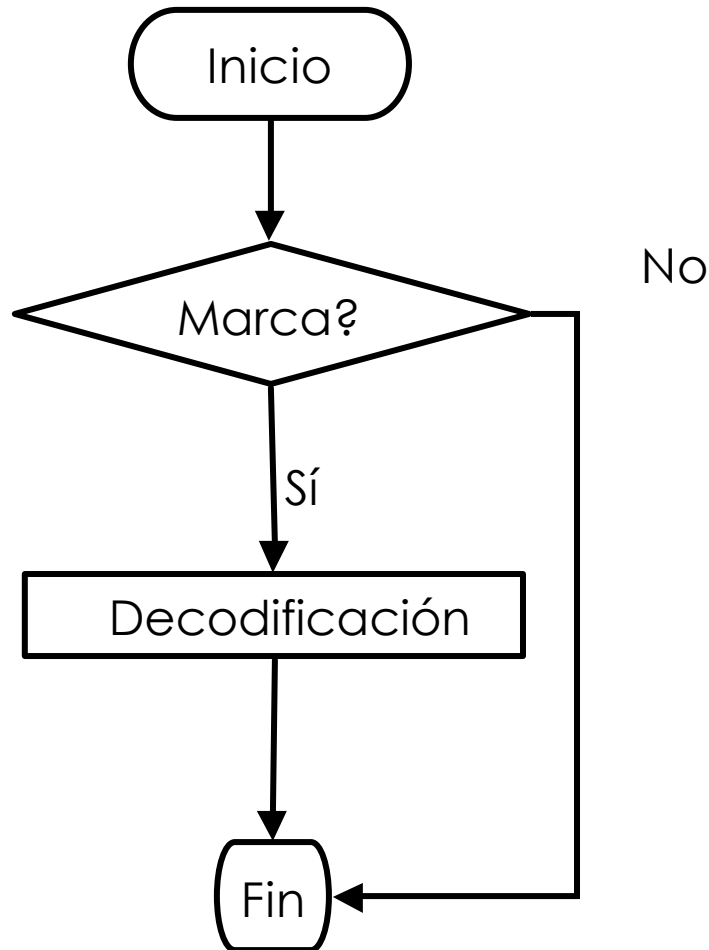
1. **Spread-spectrum** watermarking: dominio frecuencial (Boney 1996, Garcia 1999)
2. **Echo-hiding** watermarking: dominio temporal (Bender et al. 1996, Neubauer 2000)
3. **Bit-stream** watermarking: flujo de bits generado por un codificador de audio (Lacy et al. 1998 MPEG-AAC)

Spread-Spectrum



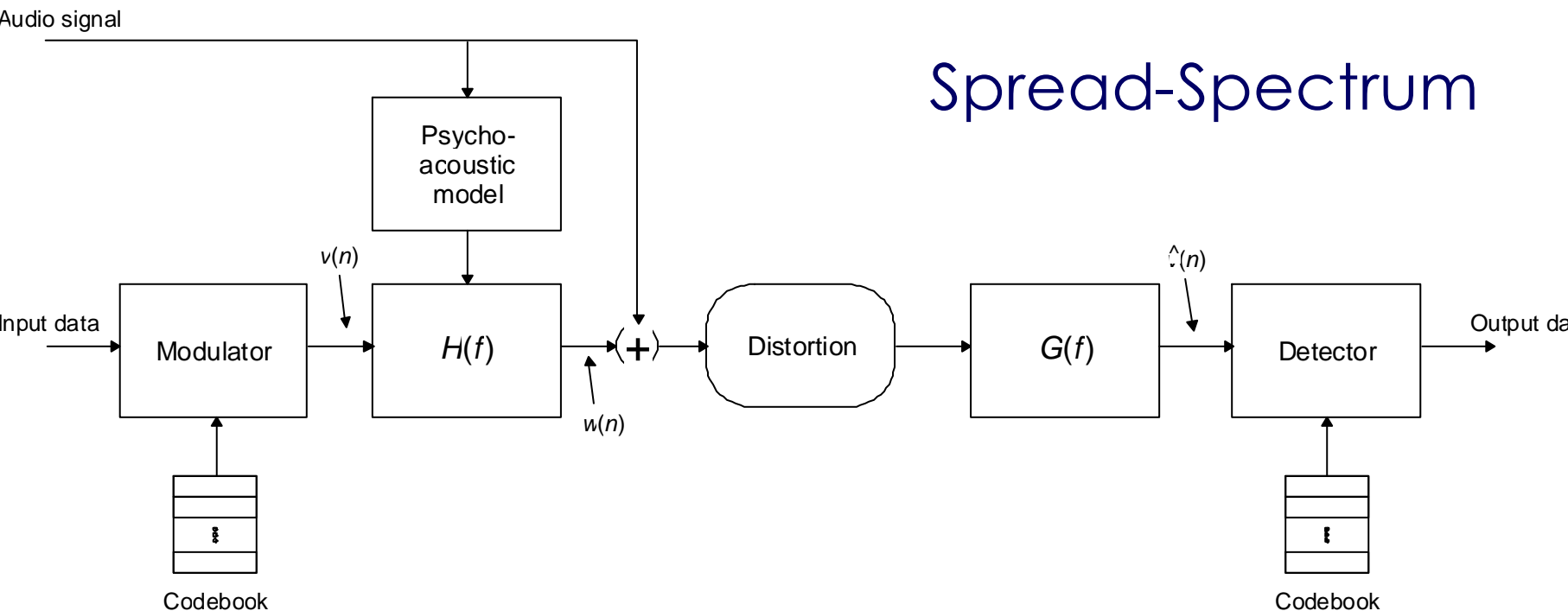
- Boney & Tewfik 1997
- Se quiere detectar si se ha insertado o no una marca
- $v(n)$: señal. Se conoce $x(n)$ (señal original) y $t(n)$ tanto en emisión como en recepción. Se puede calcular $t(n)$ en recepción si se sabe que existe.

Esquema estándar



Test de Hipótesis

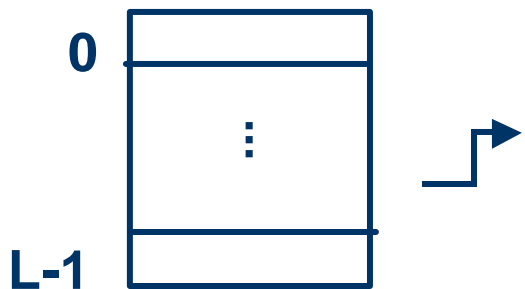
Teoría de la detección



- Elección de la modulación empleada (diccionario de símbolos)
- $H(f)$: maximiza la potencia del watermark $w(n)$
- $G(f)$: estimación de la señal $v(n)$ en recepción $\Rightarrow v(n)$ (Filtro adaptado: Wiener)
- Señal observada: $[v(mN) \dots v(mN+N-1)]$

Construcción de $v(n)$

Transmisión de una serie de mensajes,
de palabras de un diccionario



$$\vec{v}_i(n) = [v_i(0) \Lambda v_i(N-1)]^t$$

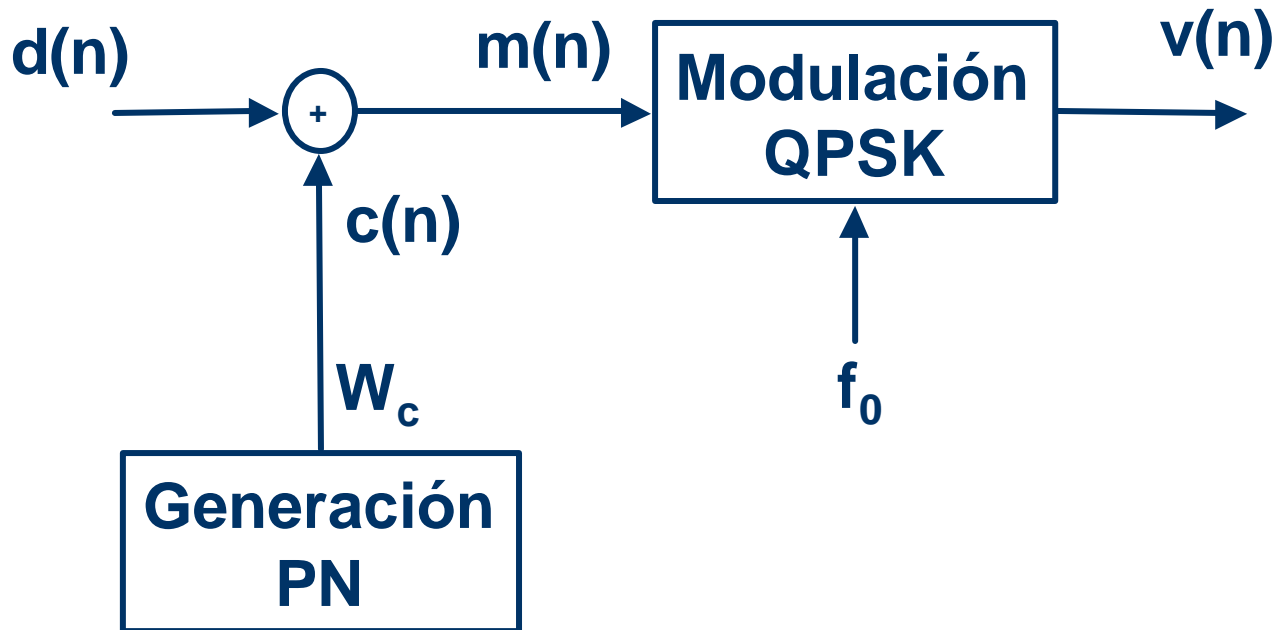
Diccionario de símbolos

codebook

$$v = \{v_i(n)\}, i = 1 \text{K } M$$

Construcción del codebook

QPSK (2 bits, 4 símbolos) + Ensanchamiento de espectro (DS):
secuencia PN de longitud N_c



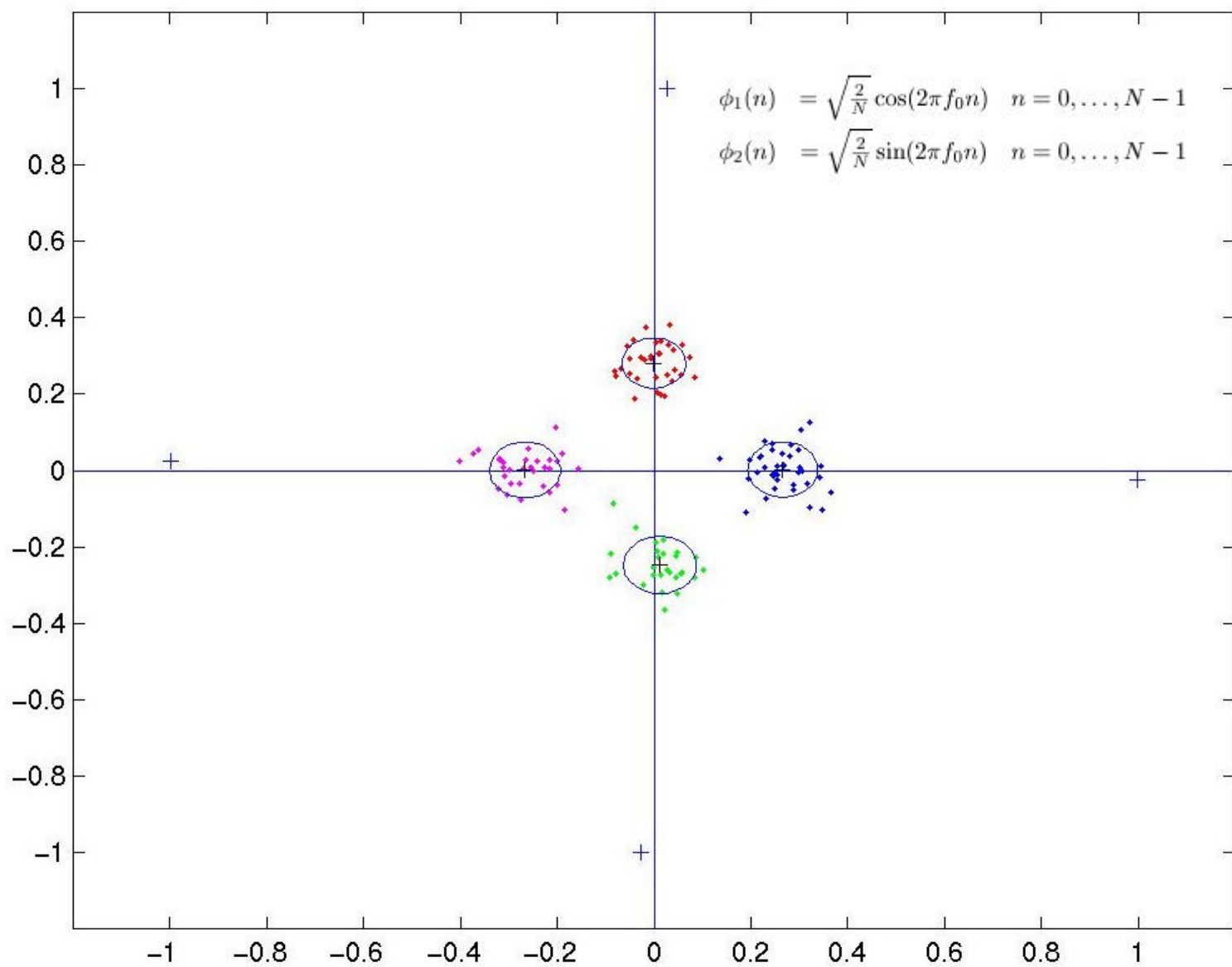
Parámetros del codebook

- Frecuencia de la portadora f_0
 - Secuencia utilizada para el ensanchamiento de espectro, W_C de longitud N_C
- Diccionario $S(f_0, W_C)$

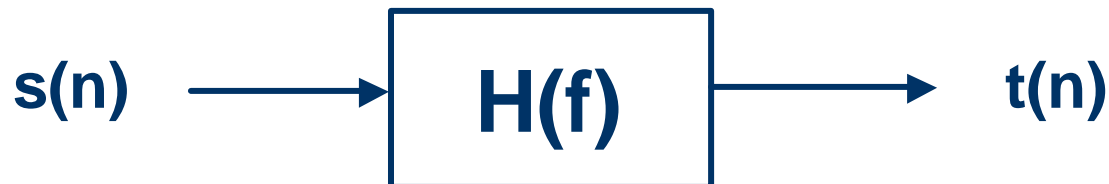
Si los parámetros en recepción \neq Parámetros en transmisión



$$P_e \approx 0.5$$



Construcción del watermark $w(n)$



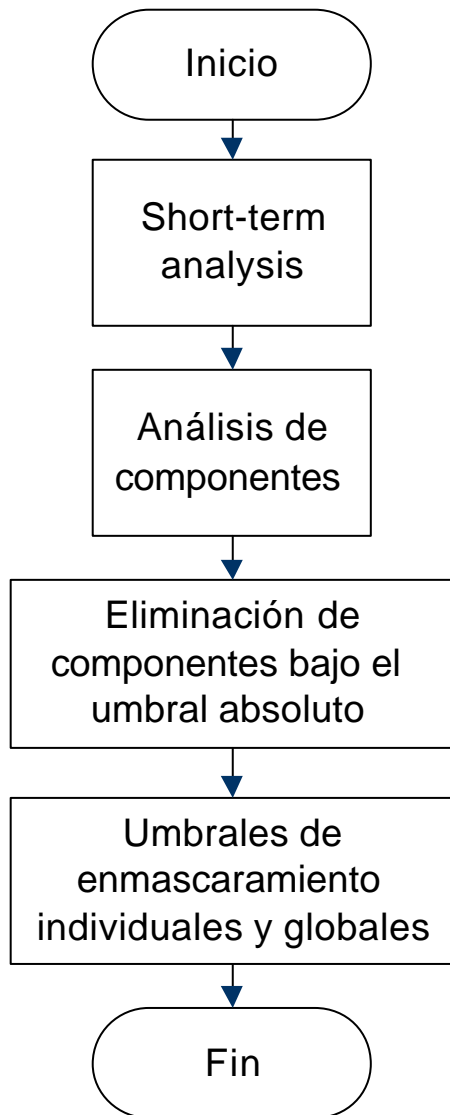
Definición de un límite de enmascaramiento

$$S_{mask}(f)$$

Condición de inaudibilidad:

$$S_T(f) = s^2 \cdot |H(f)|^2 \leq S_{mask}(f)$$

Modelo psicoacústico II



Componente tonal: máximo local

$$S(k) - S(k + j) \geq 7dB$$

$$j \in [-2, +2] \text{ si } 2 < k < 63$$

$$j \in [-3, -2, +2, +3] \text{ si } 63 \leq k \leq 127$$

$$j \in [-6, \dots, -2, +2, \dots, +6] \text{ si } 127 \leq k \leq 250$$

Componentes tonales separadas < 0.5 Barks

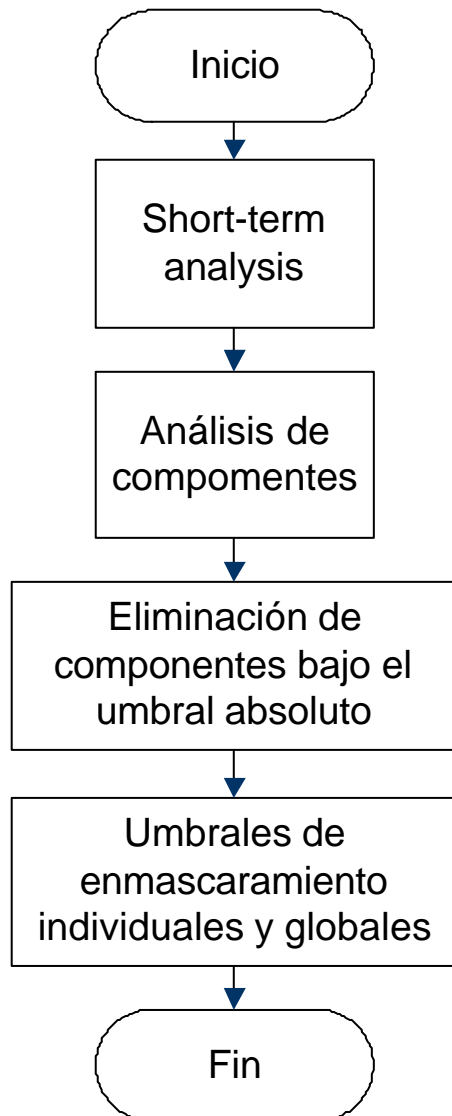
$$1 \text{ Bark} \approx \frac{f}{100} \text{ para } f < 500Hz$$

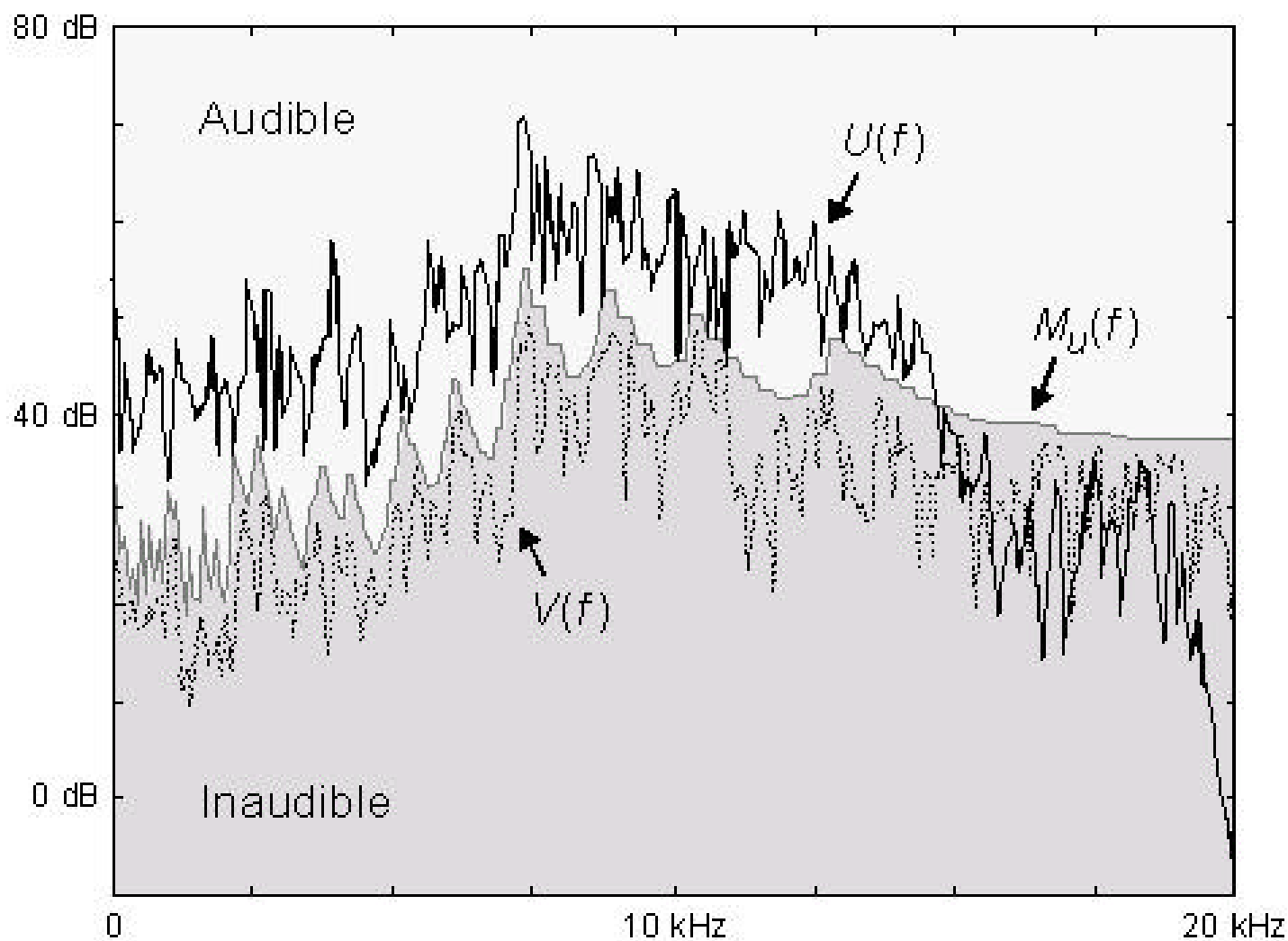
$$1 \text{ Bark} \approx 9 + 4 \log\left(\frac{f}{1000}\right) \text{ para } f > 500Hz$$

Modelo psicoacústico II

Límites de enmascaramiento
individuales y globales

$$S_m(f_2) = 10 \cdot \log_{10} \left[10^{\frac{S_a(f_2)}{10}} + \sum_{j=1}^{N_t} 10^{\frac{P_2(f_2, f_1, P_1)}{10}} + \sum_{j=1}^{N_n} 10^{\frac{P_2(f_2, f_1, P_1)}{10}} \right]$$






Señal marcada = **marca + música** (ruido de canal)

- $x(n)$ = ruido fuertemente coloreado σ_x^2 muy variable (hasta 100 dB)

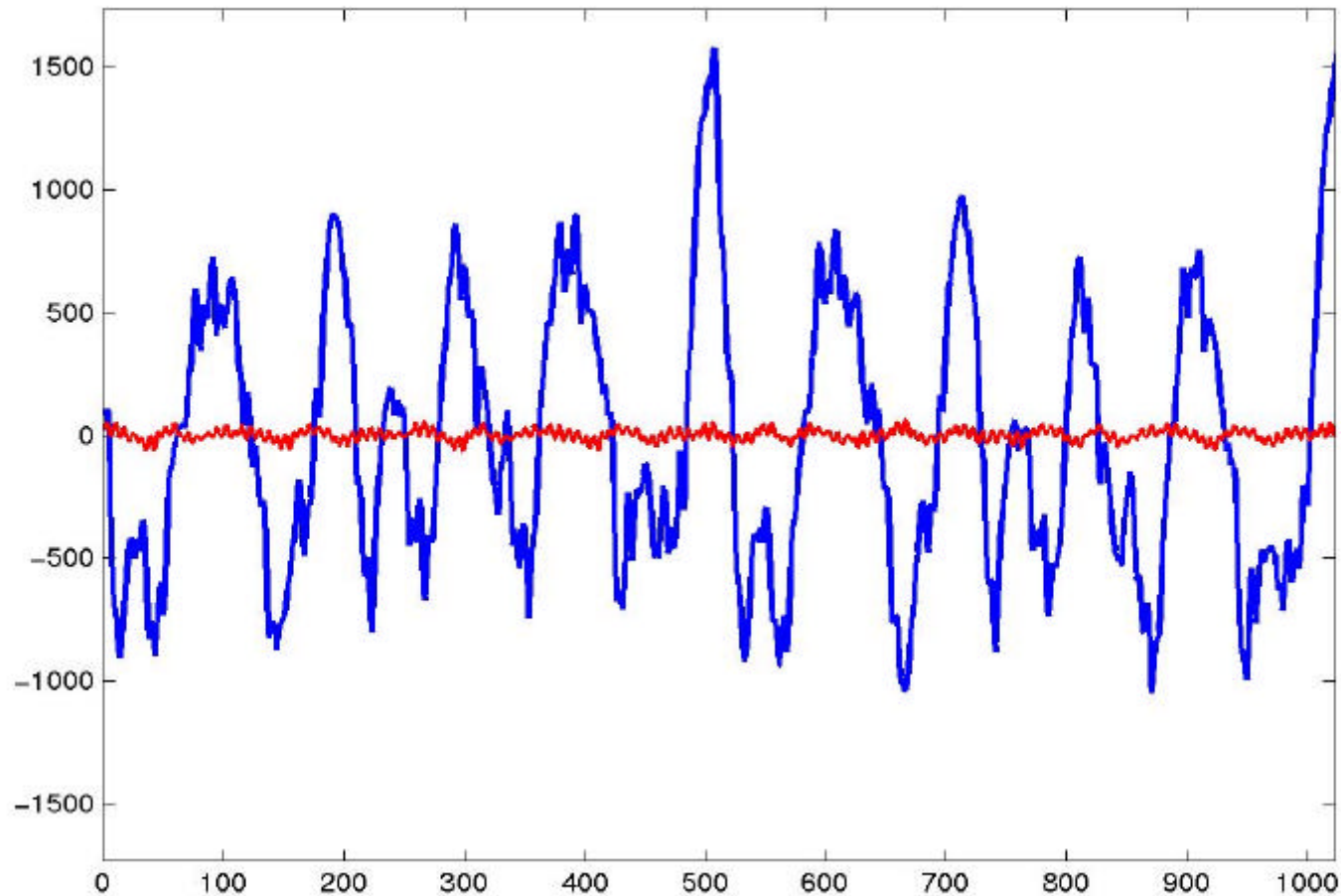
$$\frac{s_w^2}{s_x^2} \approx -20dB$$

- CD-16 bits  $SNR \approx 100dB$
- Para que P_w no sea ridícula respecto a P_x , $w(n)$ filtrada por $H(f)$, $\max(P_w)$

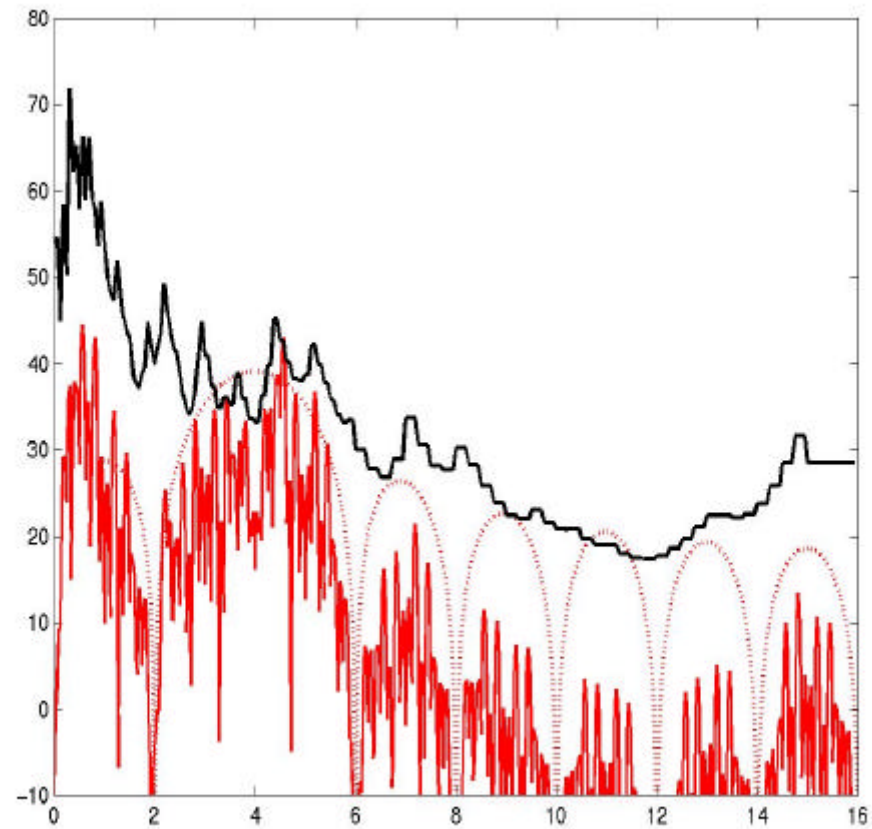
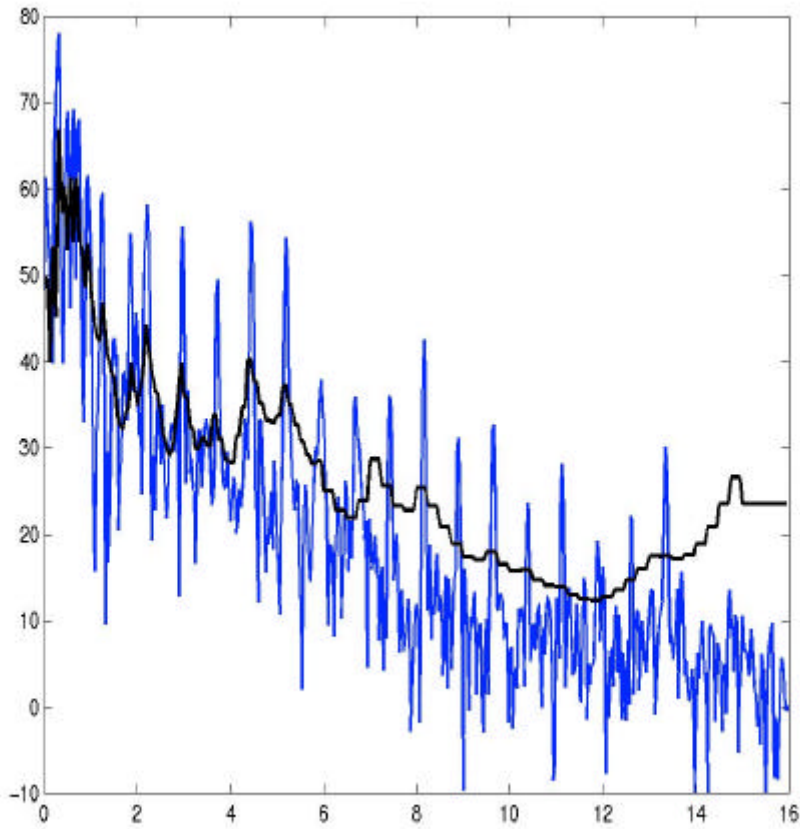
Observaciones

- El umbral de enmascaramiento $H(f)$ se actualiza aproximadamente cada 20 ms
- Se puede intentar *blanquear* la contribución de la señal de música $x(n)$ a través de un entrelazador

Señal en el dominio temporal

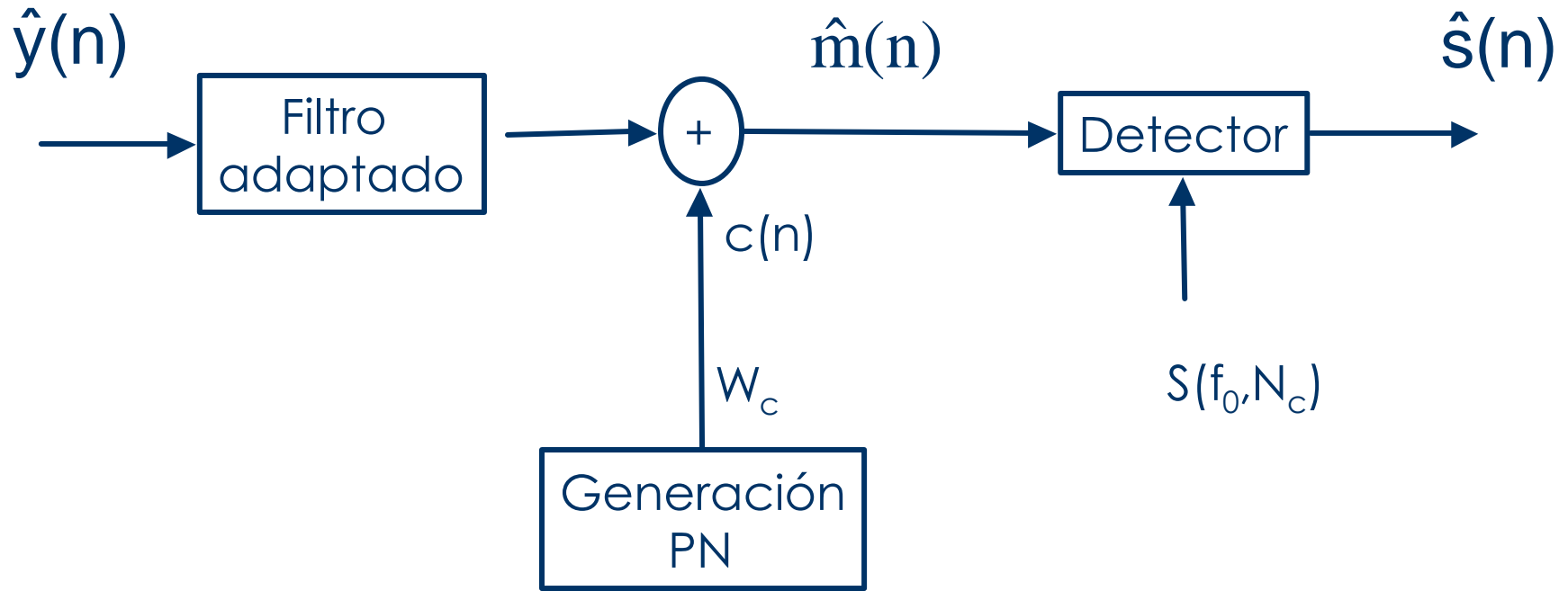


Espectros

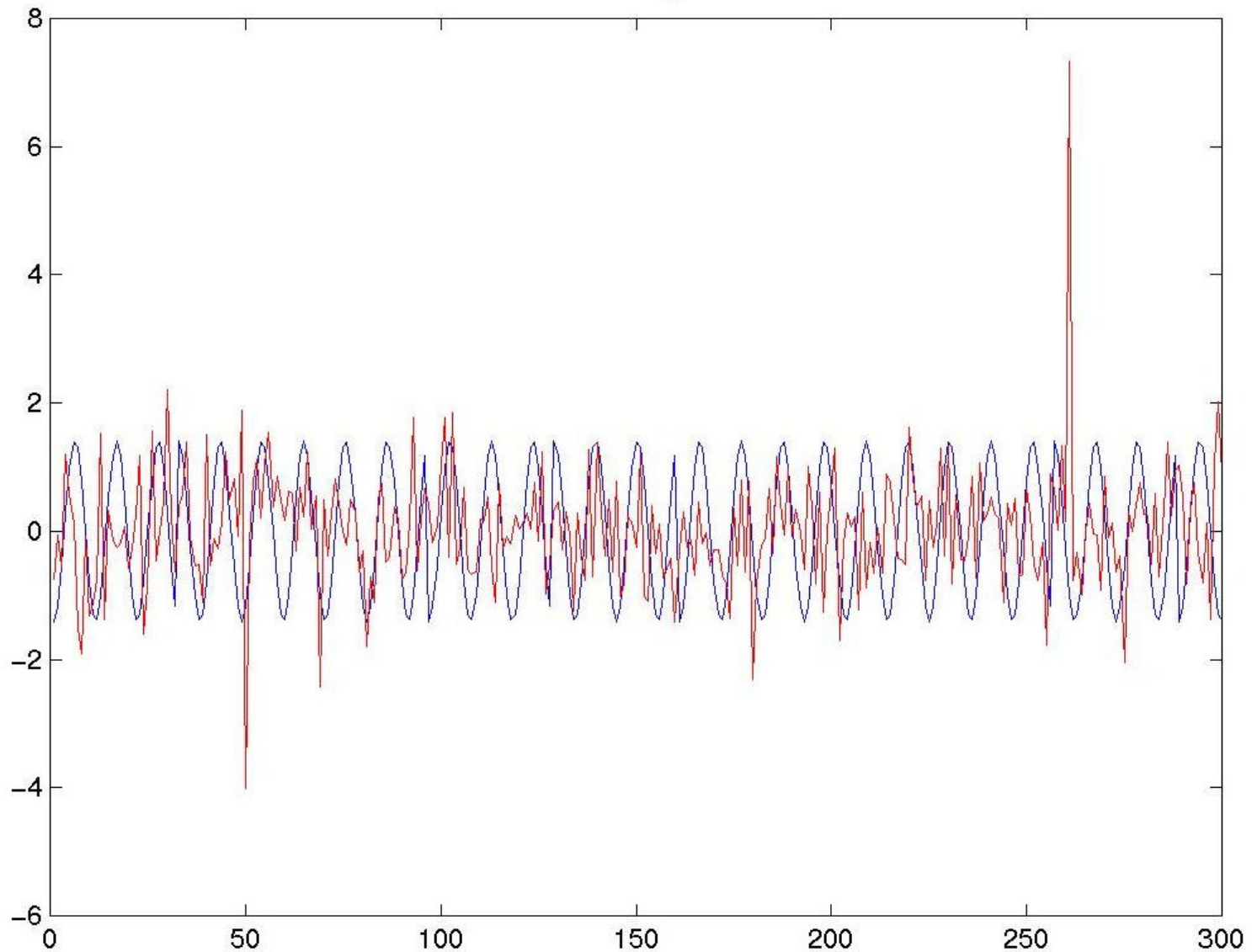


$X(f), W(f)$ e $Y(f)$

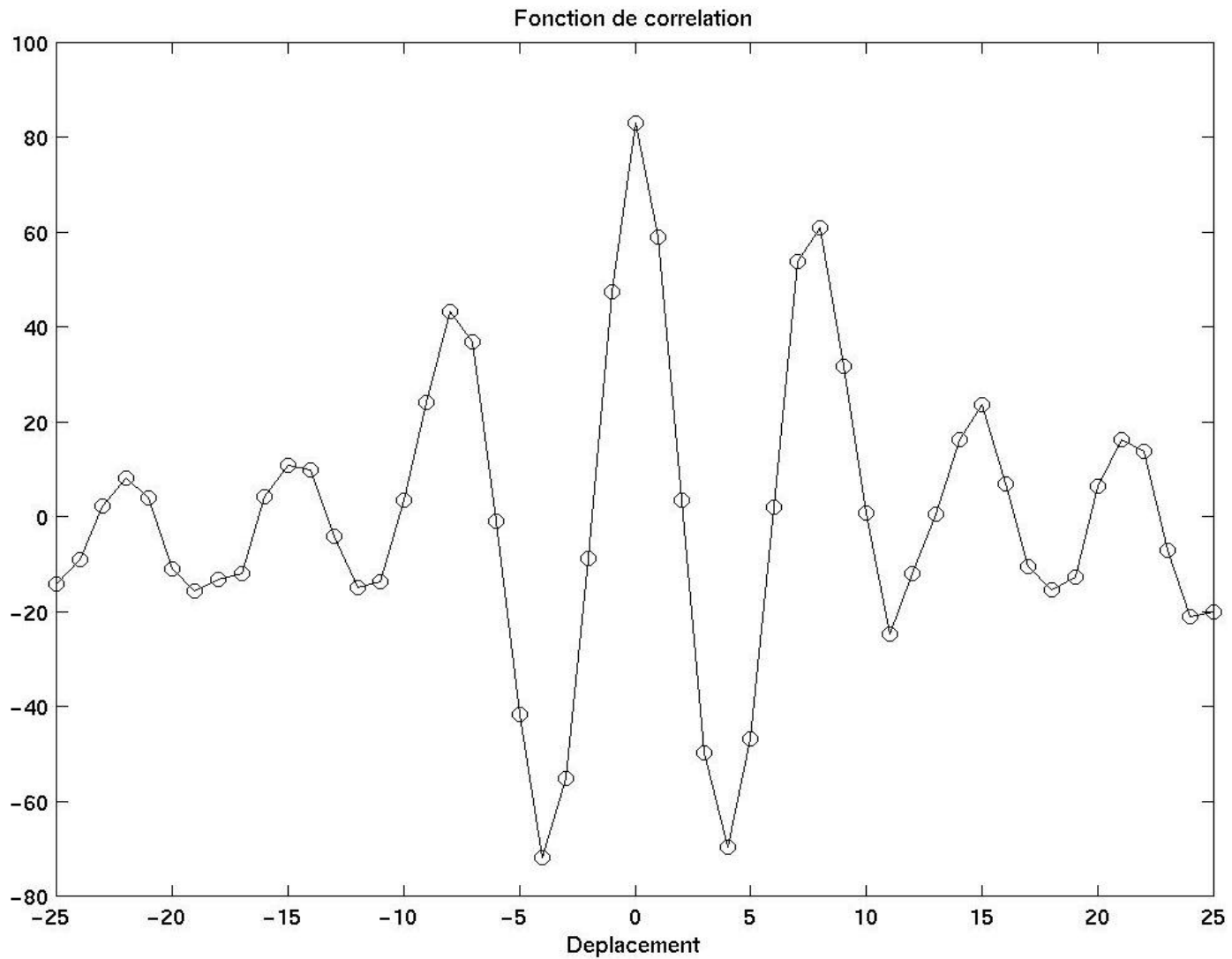
Detección del watermark



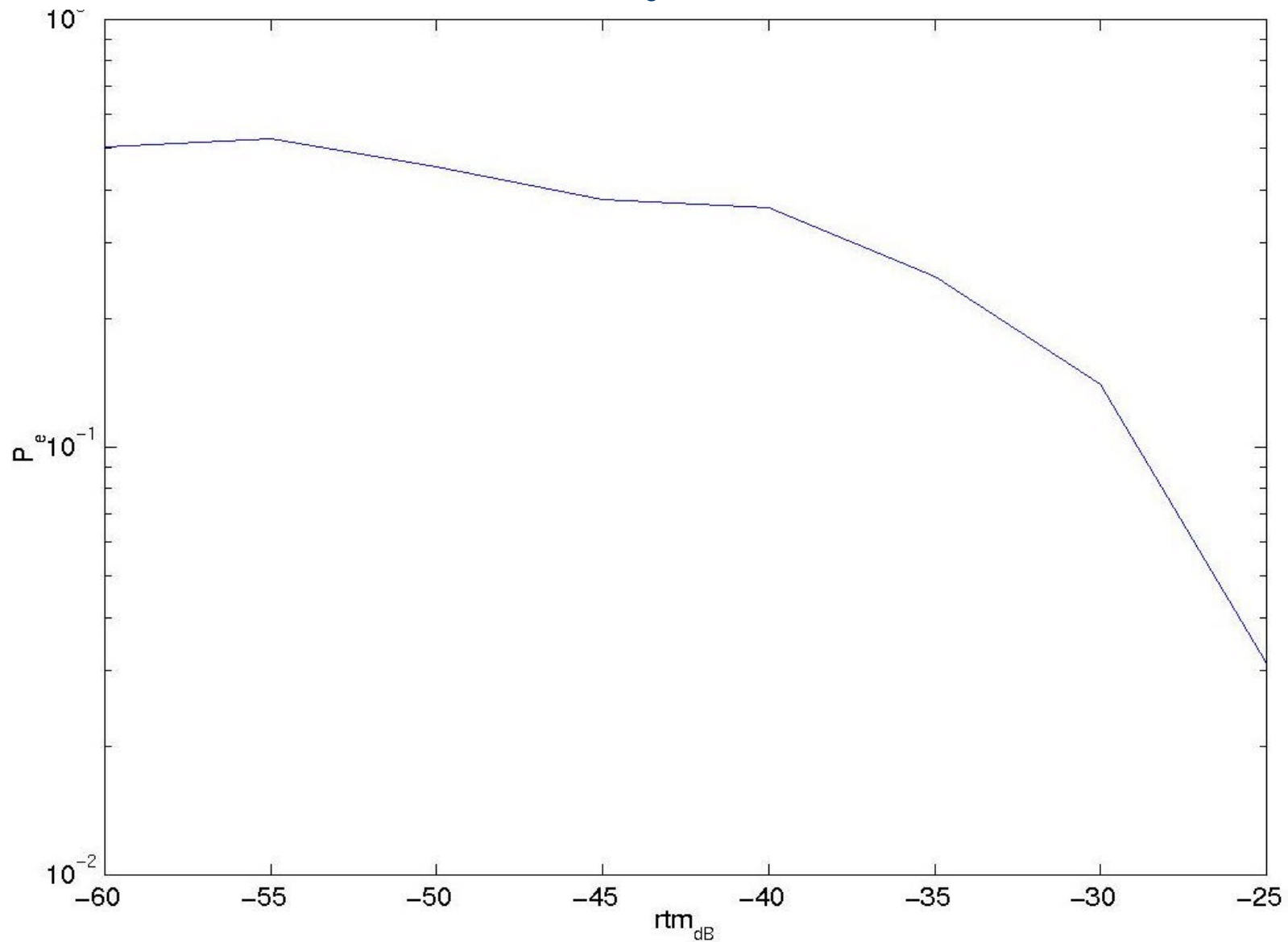
$s(n)$ y $\hat{s}(n)$



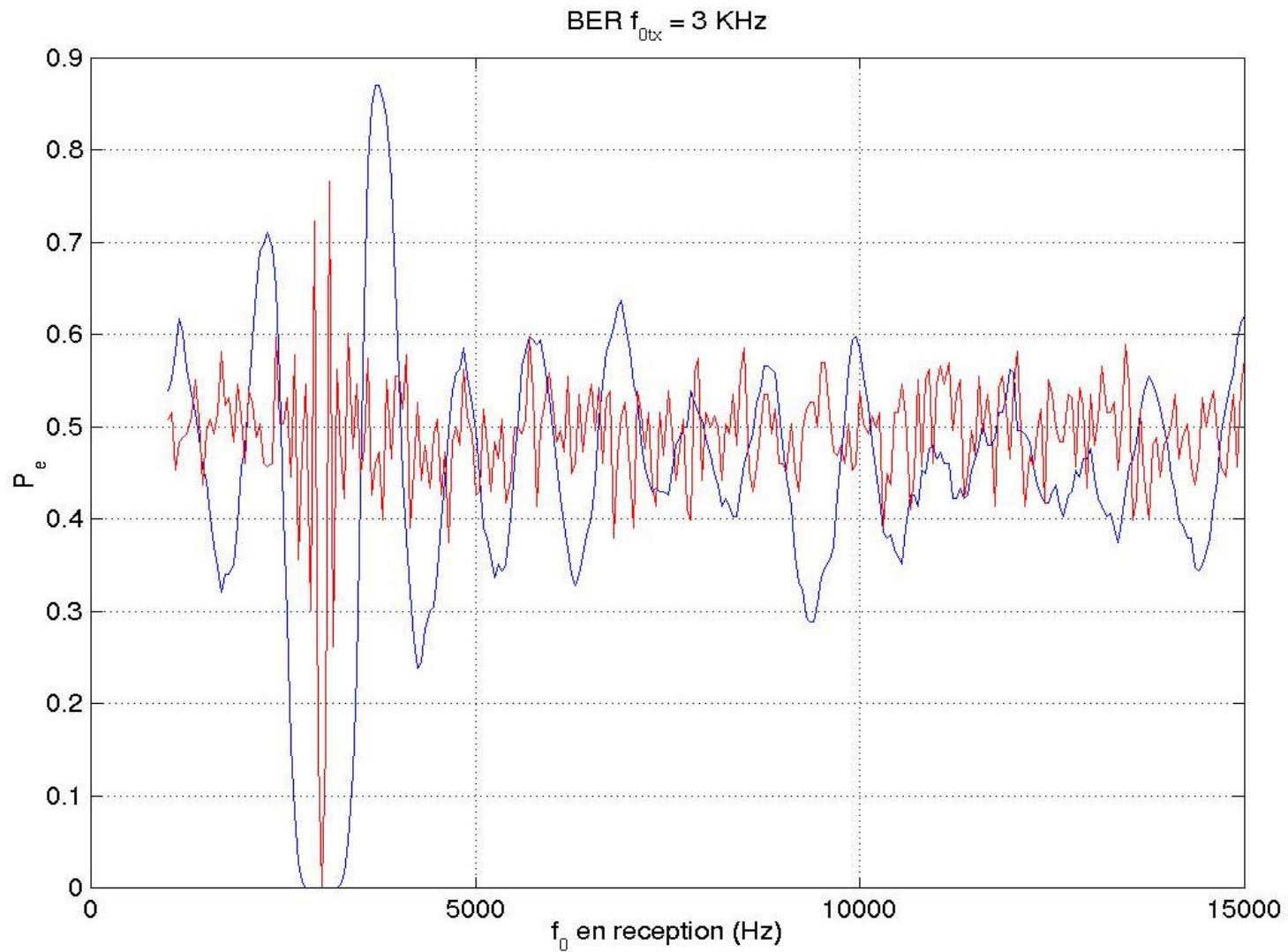
Función de correlación



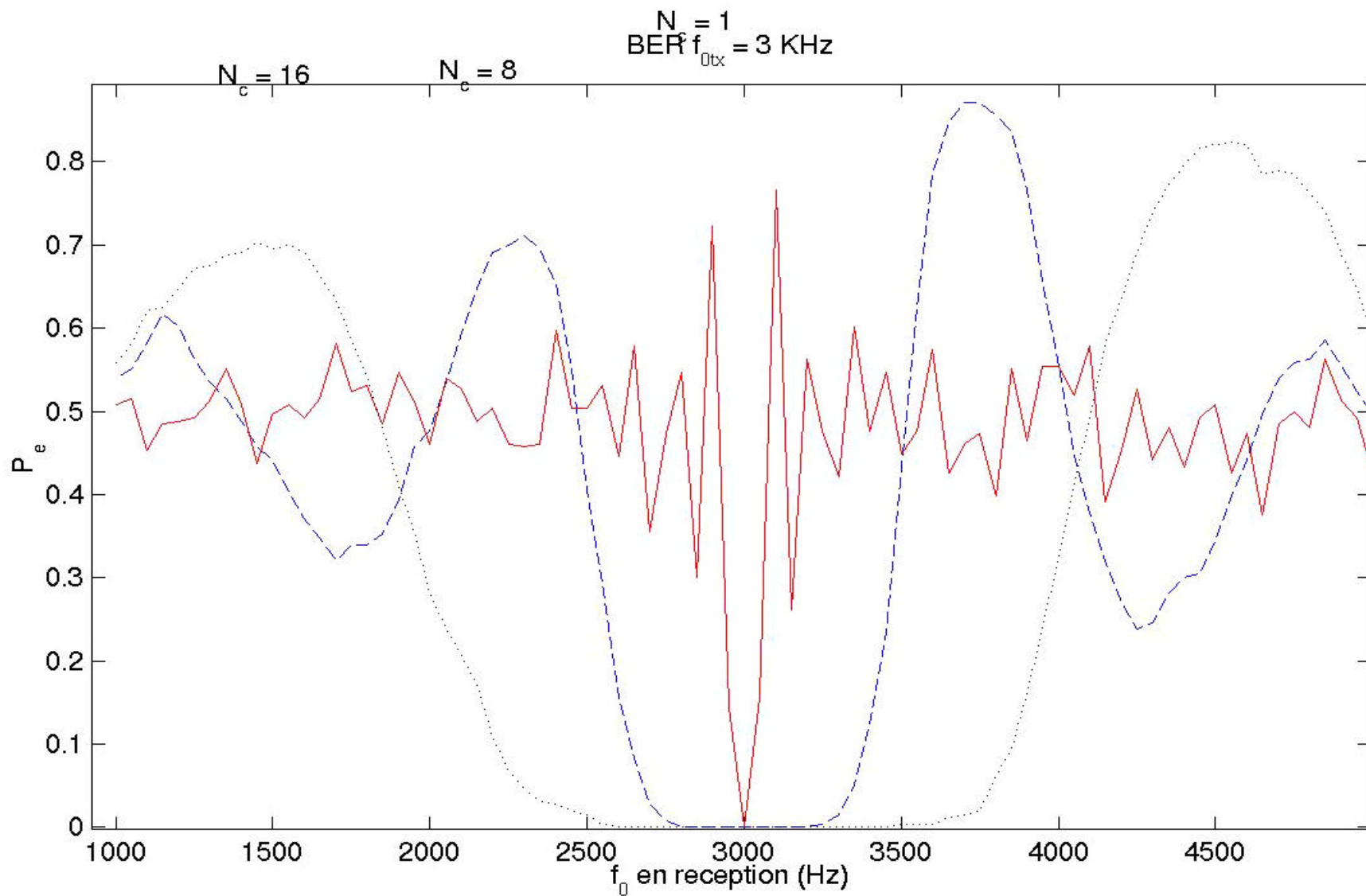
$P_e(\text{RWM})$



Tasa de error para distinta f_{ORX}

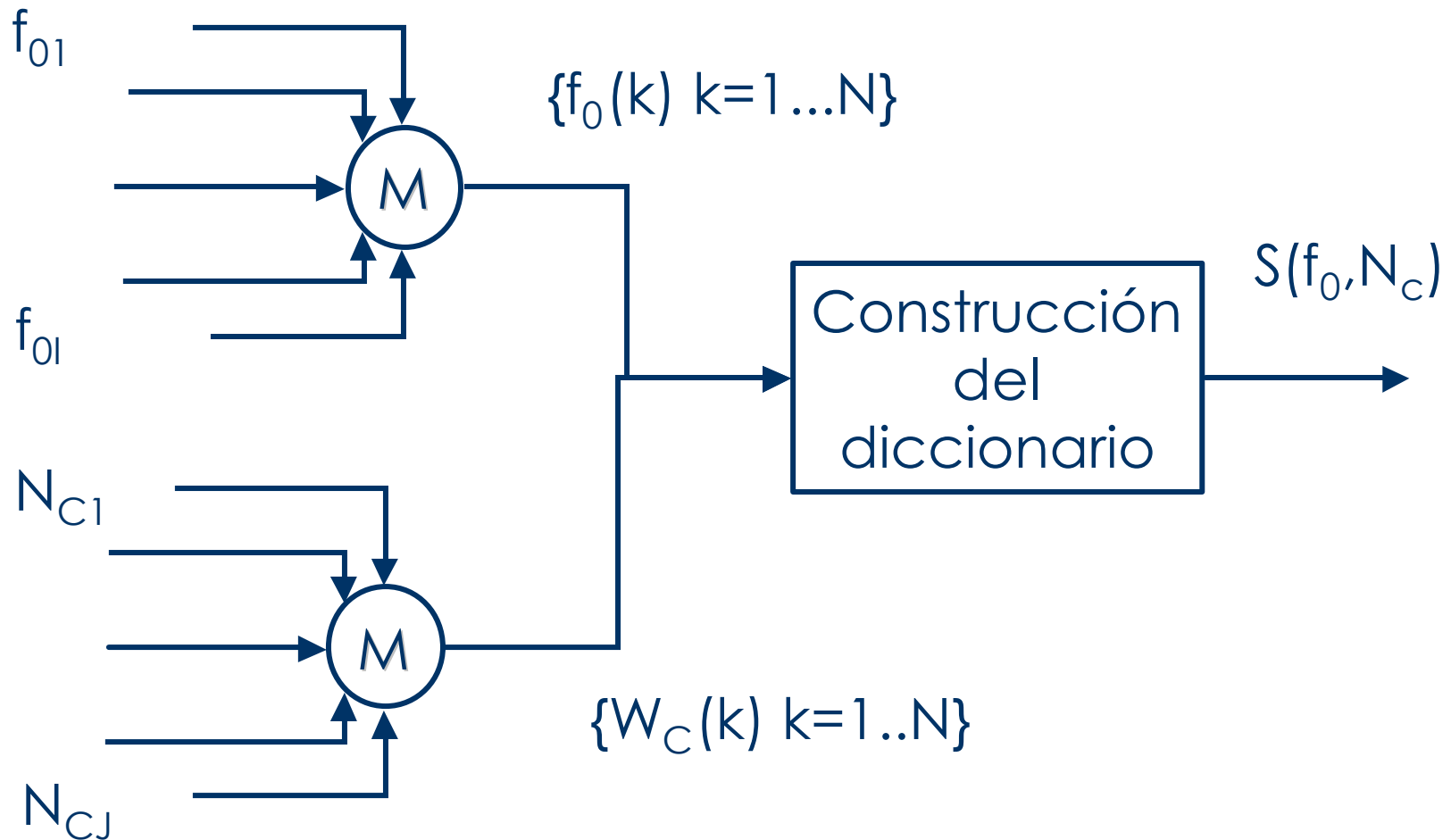


Tasa de error para distinta f0 con diferente Nc

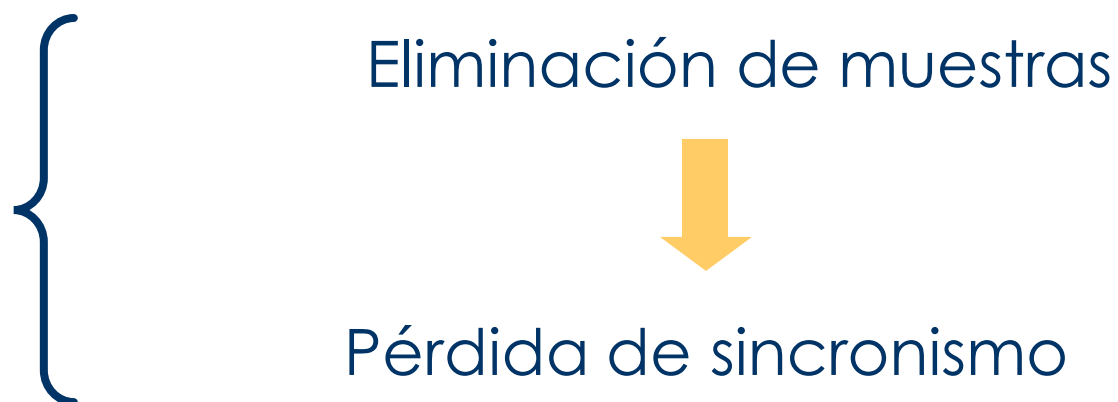


Canales de datos

Diccionario utilizado $S(f_0, N_C)$

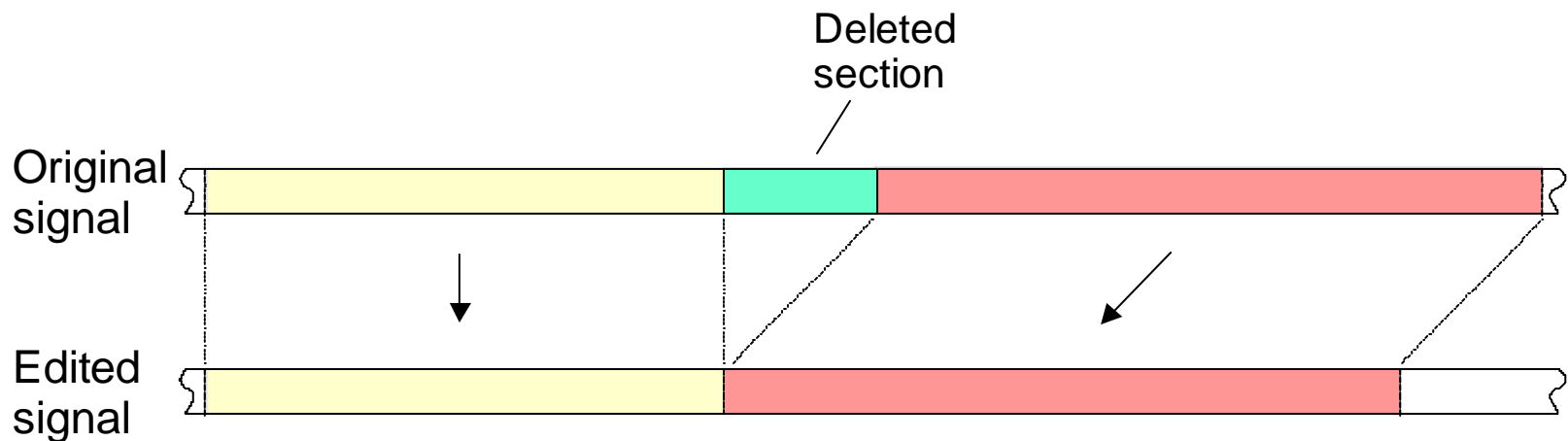


Ataques



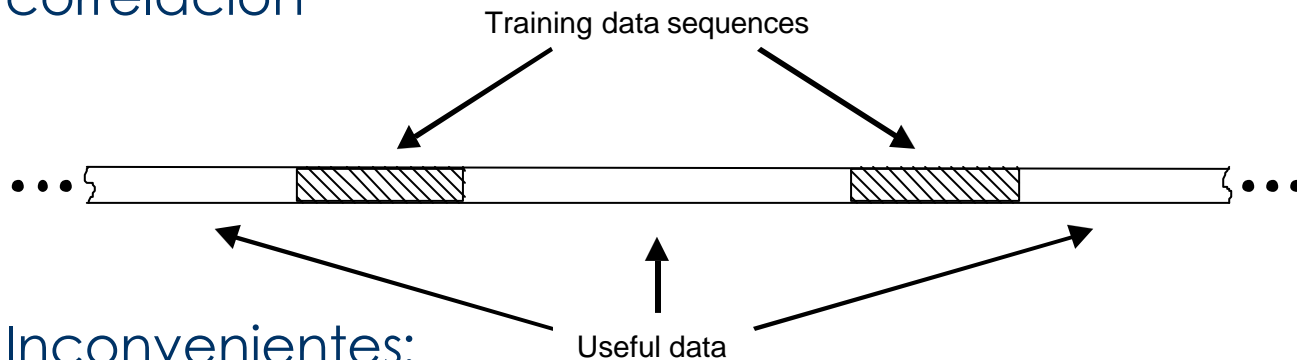
Pérdida de sincronismo

- ❖ Razones estándar: retrasos introducidos por
 - filtrado
 - Compresión MPEG
 - Propagación del sonido
- ❖ Otras razones
 - ataques: filtro paso-todo, adición/supresión de muestras
 - modificación de la escala temporal (time stretching)



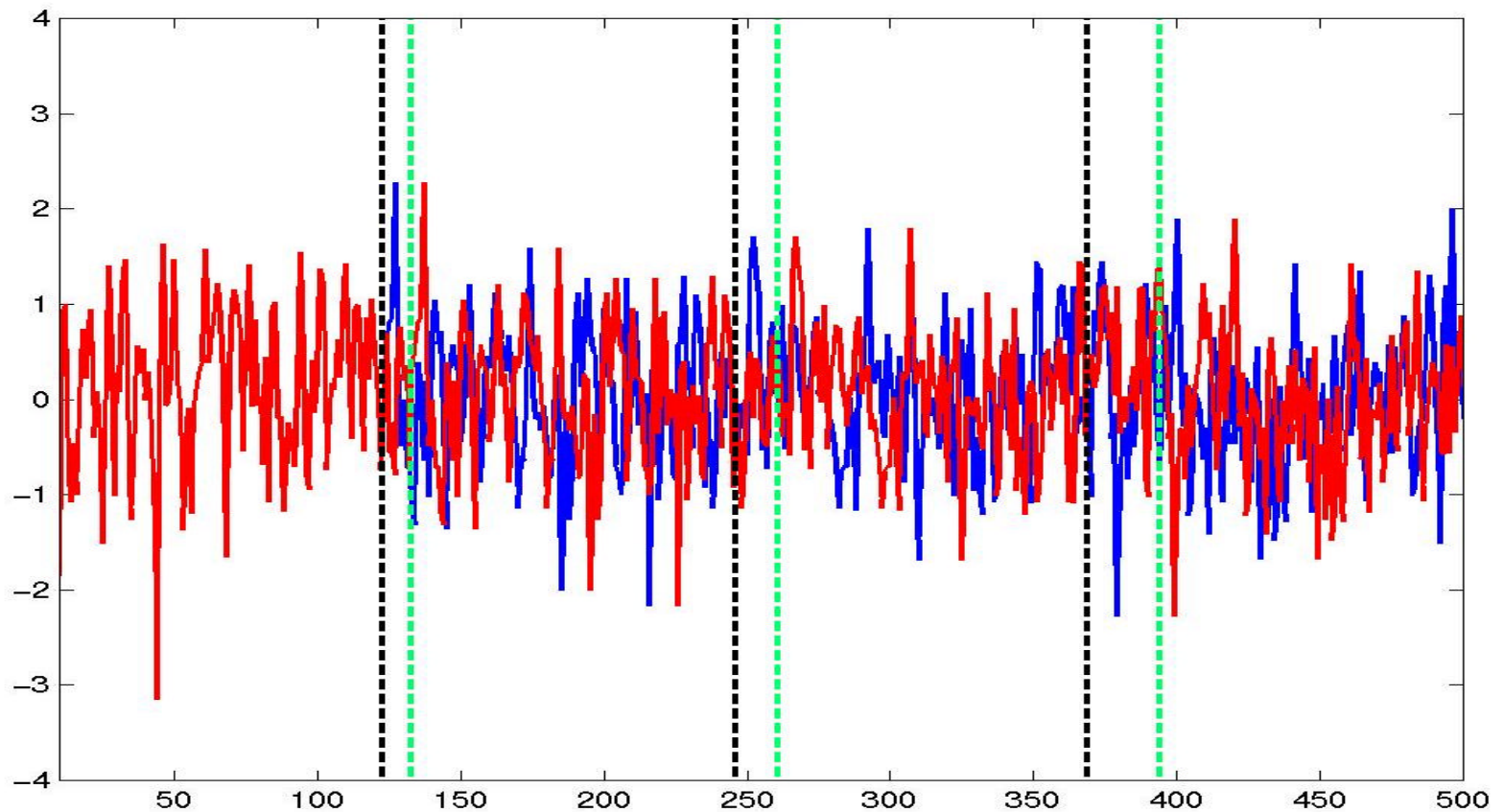
Solución

- Insertar una secuencia de bits conocida (*training sequence* o secuencia de entrenamiento) de vez en cuando
- Utilizar ventanas deslizantes para buscar picos de correlación



- Inconvenientes:
 - Reducción de la tasa de bits
 - Frágil ante ataques

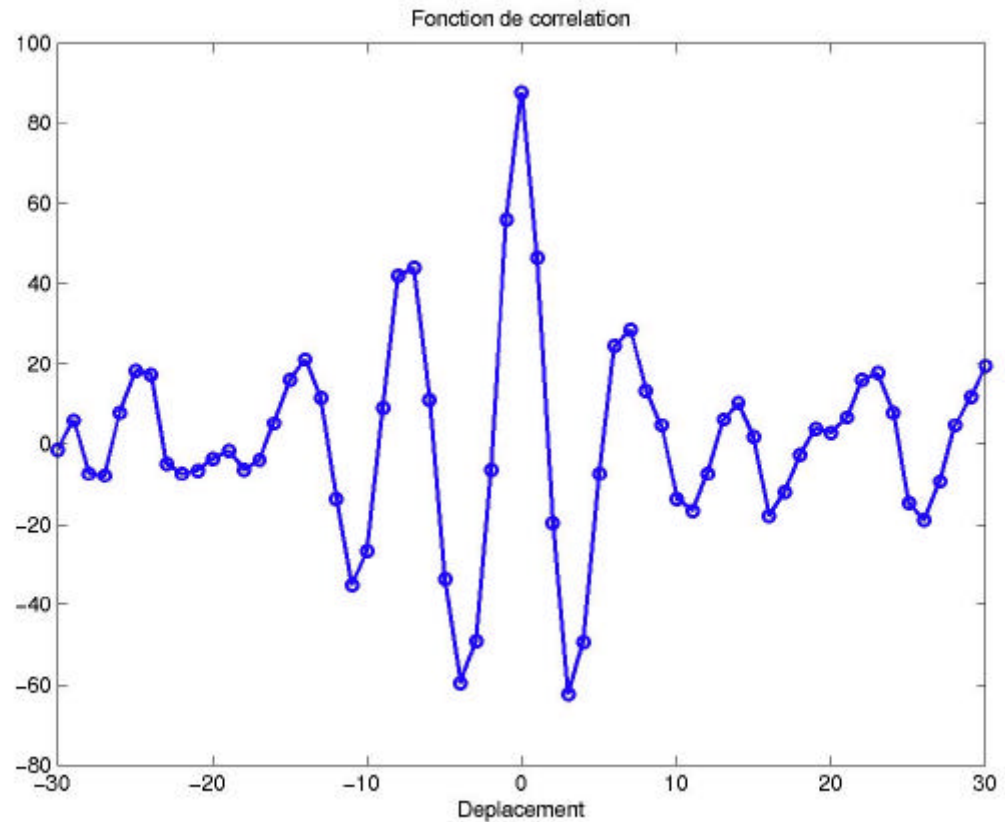
Pérdida de muestras



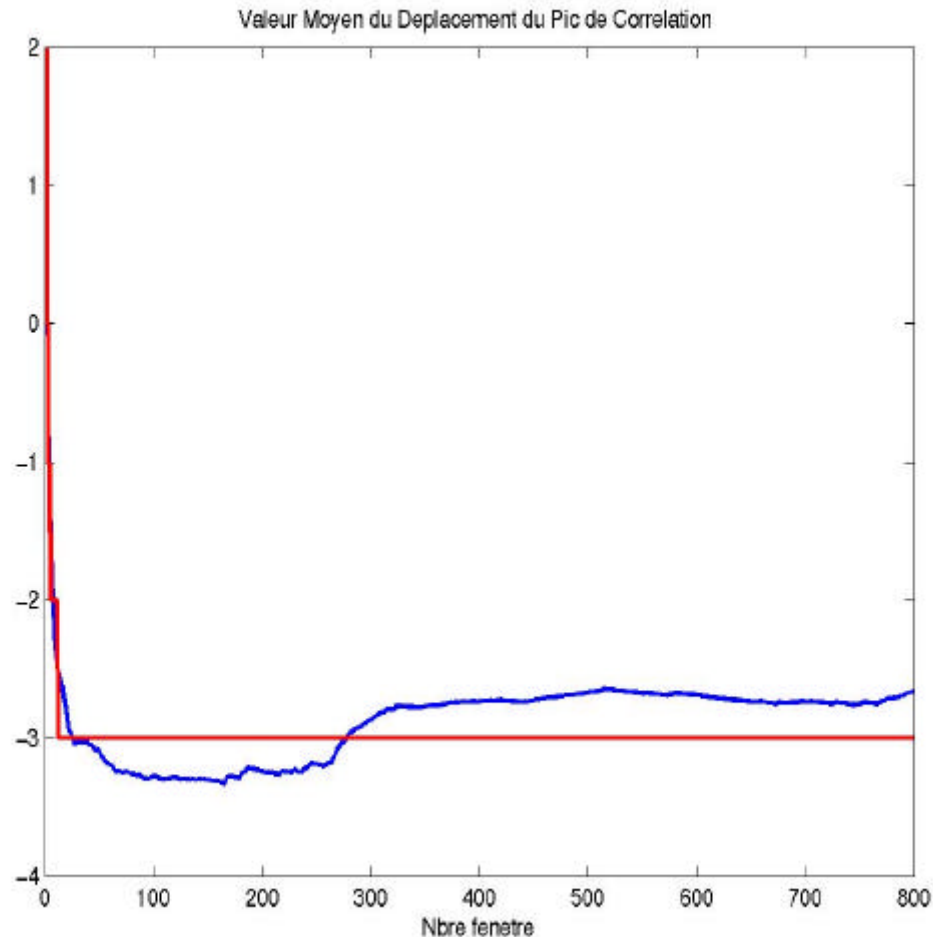
- Utilización de una ventana deslizando: $k \in [-K, K]$
- Búsqueda de la referencia de símbolo

Función de correlación

- Frecuencia de la portadora f_0 : separación entre máximos de la función de correlación
- Secuencia utilizada por el ensanchamiento de espectro W_c de longitud N_c : envolvente de los máximos
- Desplazamiento de la ventana deslizante K

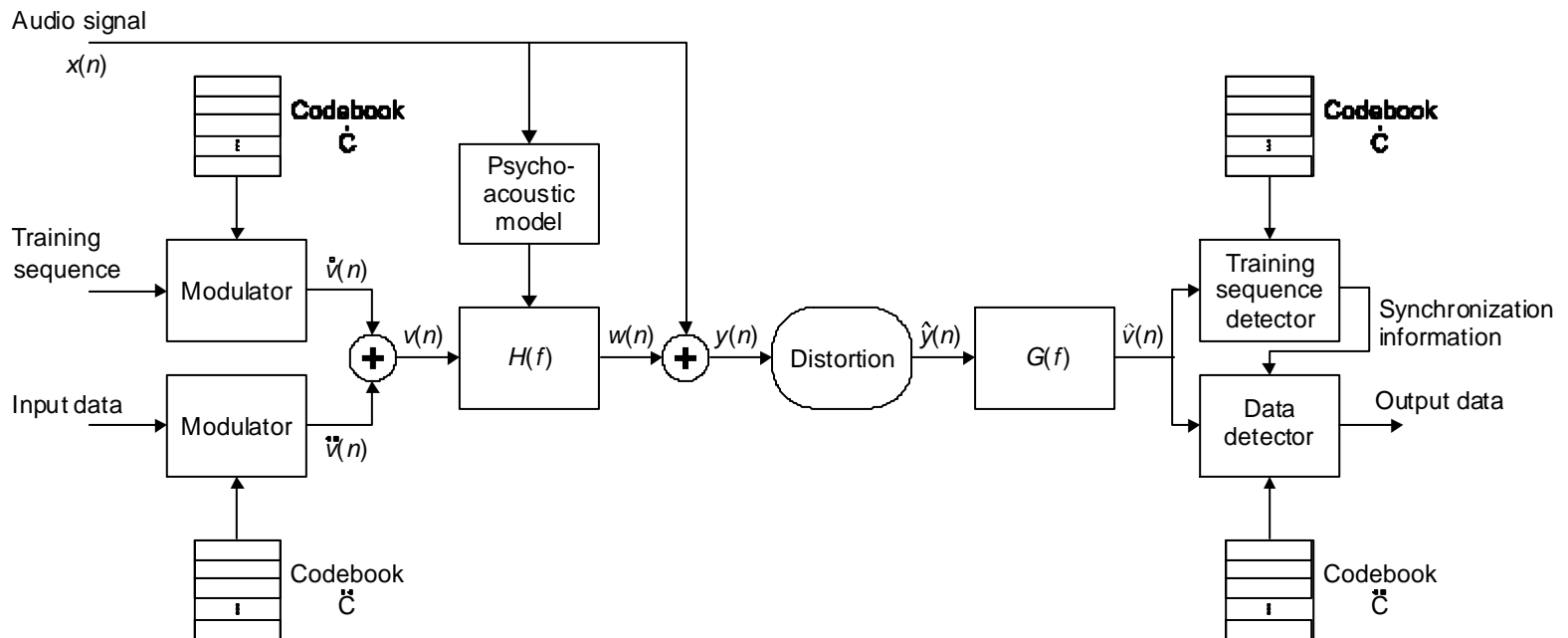


Desplazamiento del máximo de la función de autocorrelación



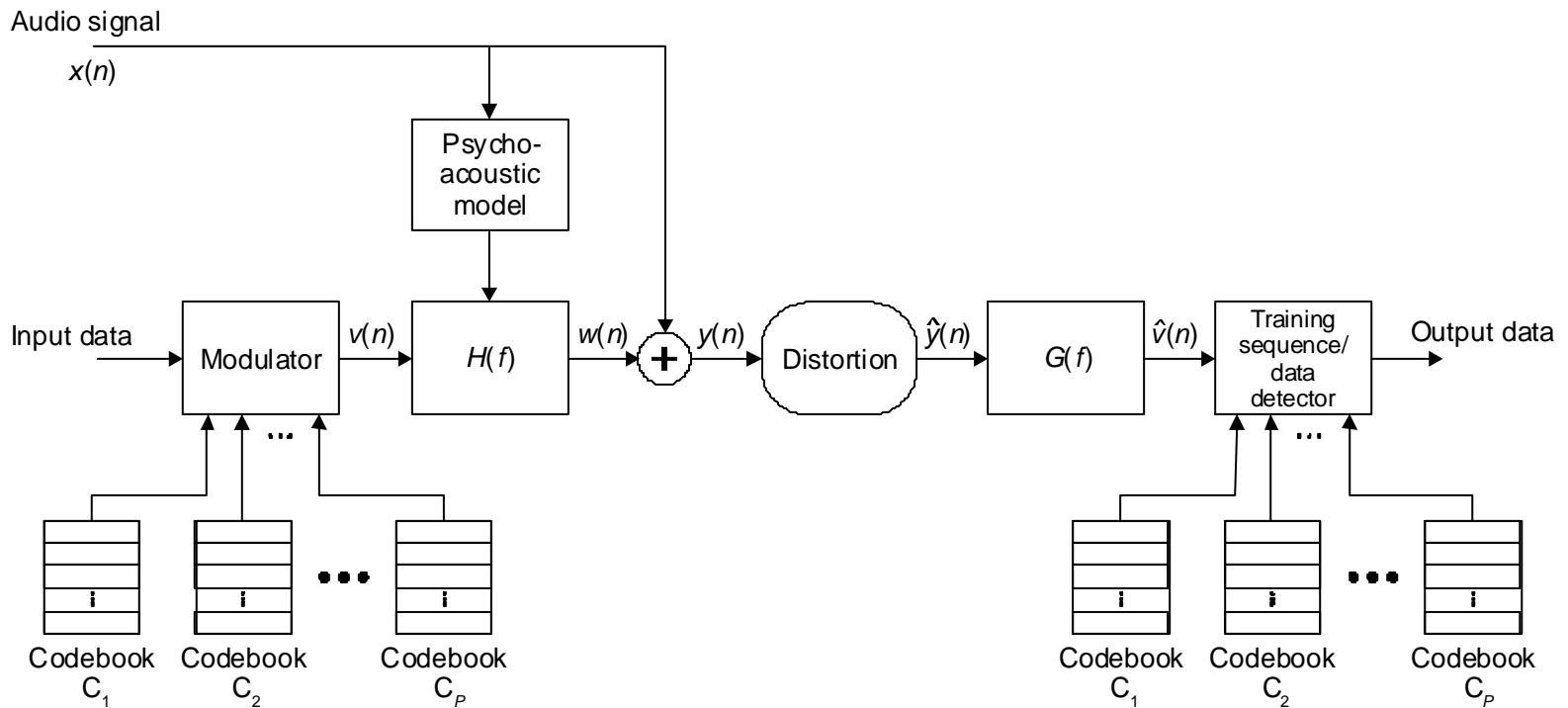
Solución

- Solución propuesta: repartir secuencia de entrenamiento a lo largo de toda la secuencia de bits
- **Primer método:** un segundo watermark que se utiliza exclusivamente para sincronización



Solución II

- **Segundo método:** utilizar diversos diccionarios para codificar la información



Solución III

- Para cada M símbolos consecutivos, se realiza la detección para todas sus N posibles localizaciones
- Se obtiene una matriz $M \times N$ con los resultados de detección
- Se utiliza un algoritmo de programación dinámica para seleccionar el camino más adecuado en esta matriz (Viterbi).
- La función de costo tiene en cuenta los coeficientes de intercorrelación y la secuencia de símbolos de sincronización

		Symbols														
		1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th	13th	14th	15th
Possible detection results		4	4	1	1	1	4	2	1	2	2	4	1	2	1	3
		3	1	3	1	2	1	3	4	1	2	1	3	1	3	3
		1	2	3	3	1	4	3	1	1	3	1	3	1	3	1
		4	4	2	4	1	2	1	3	4	1	3	4	1	4	2
		2	1	4	3	2	3	1	4	4	4	1	1	1	2	3
		2	2	1	2	4	1	2	3	2	1	2	3	1	2	1

Resultados de simulaciones con pérdida y recuperación de sincronismo

- Desincronización global entre transmisor y receptor (*translation in time*)
- Ataques:
 - adición or supresión de una media de 1/2500 muestras
 - Filtro paso-todo (*all-pass filtering*)

Bit-rate = 125 bit/s \wedge error rate \gg 0.05

[Sound_Examples.html](#)

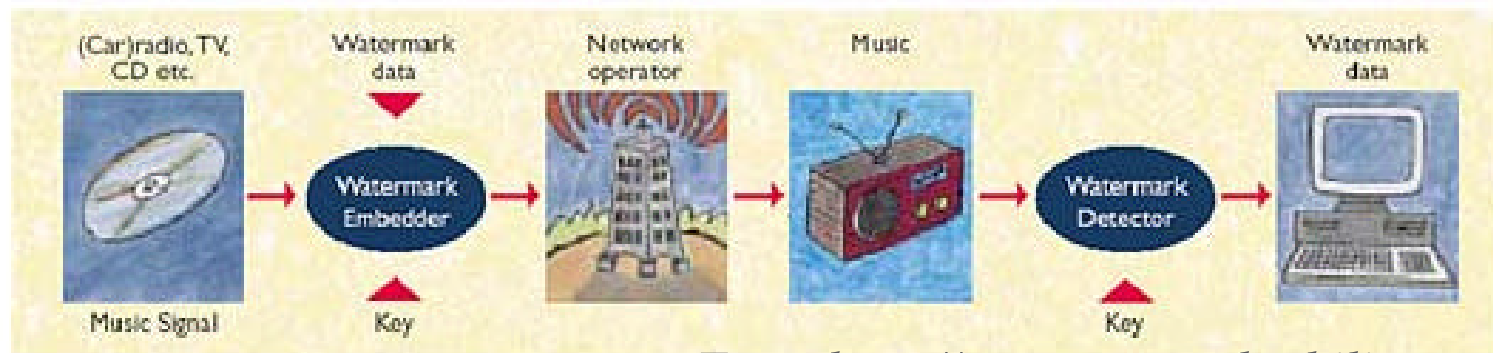
Aplicaciones

1. Aplicaciones relacionadas con la gestión de derechos de autor
(*Copyright-related applications*)
2. Servicios de valor añadido
(*Added-value services*)
3. Aplicaciones de verificación de integridad
(*Integrity verification applications*)

1. © - related

- Prueba de propiedad (*proof of ownership*):
 - Ataques para hacerla indetectable
 - Ataques de ambigüedad
- Monitorización en el punto de consumo:
reproductores MP3, DVD, etc. *Enforcement of Usage Policy*
 - Violan el Principio de Kerckhoff's 1883
 - *Detector mismatch attacks*

- **Monitorización** en el punto de **distribución**: canales de TV, distribuidores Web: Napster y similares, CD Plants
- **Monitorización, identificación** en canales de **broadcast**, cable y otras redes (internet)
- **Seguimiento** del origen de copias ilícitas
 - *Collusion attack*
- Determinación del origen de copias ilícitas



From <http://www.research.philips.com>

Video and Audio Watermarking



New, powerful tool for video and audio rights protection

- Can't be erased or overwritten
- Robust and completely unaffected by common audio or video processing operations
- Survives broadcast chains and over-the-air transmission
- Open system with unique 'secret key' mechanism
- Combines enormous versatility with ease of installation, integration and operation
- Wide range of applications, including copyright control and broadcast monitoring
- Commercially deployed successfully in various markets

MASTER DE LA GRABACIÓN

Una vez la obra se ha digitalizado y se ha insertado la Marca de Agua, sólo queda su fabricación, distribución y venta.

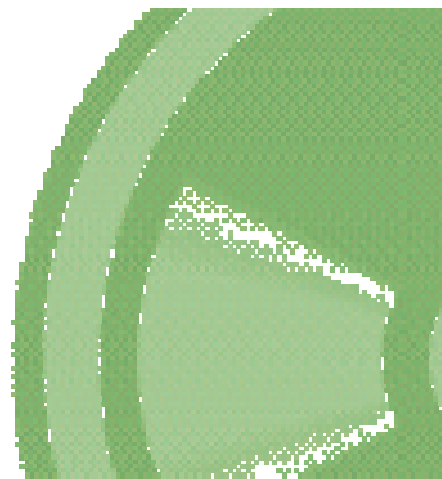
Para poder realizar la distribución es necesaria la fabricación de las copias a distribuir, para lo cual es necesario realizar el Master de la grabación. Es precisamente en este punto donde la Marca de Agua alcanza su punto más importante.

Gracias a haber realizado la Marca de Agua al generar el Master permite una gran ventaja ya que cualquier copia posterior de la obra obtenida tendrá ya inserta la Marca de Agua, lo cual cualquier copia distribuida podrá ser rastreada por la SGAE si se emite en cualquier medio, sea autorizado o no, con lo cual se puede realizar una liquidación de los derechos de autor de la obra de una manera más justa y más



SGAE

WaterMarking



2. Servicios de valor-añadido

- Relativos al contenido
 - Transporte de información de contenido: letras, etc.
- Transporte de información de propósito general:
 - Noticias, anuncios

3. Integrity verification

- Verificación de la integridad de una grabación. Ej: de un testimonio, conversación telefónica, etc.

Empresas

Alpha Tec Ltd, Greece, <http://www.alphatecltd.com>

eWatermark, USA , <http://www.ewatermark.com>

BlueSpike, USA, <http://www.bluespike.com>

MediaSec, USA, <http://www.mediasec.com>

Sealtronic, Korea, <http://www.sealtronic.com>

Signum Technologies, UK, <http://www.signumtech.com>

SureSign Audio SDK (Librería C++), VeriData SDK

The Dice Company, USA

Verance, USA, CONFIRMEDIA. Sistema de monitorización de radio y televisión, **SGAE** <http://codec.sdae.net/>

Digimarc <http://www.digimarc.com/>

Philip's

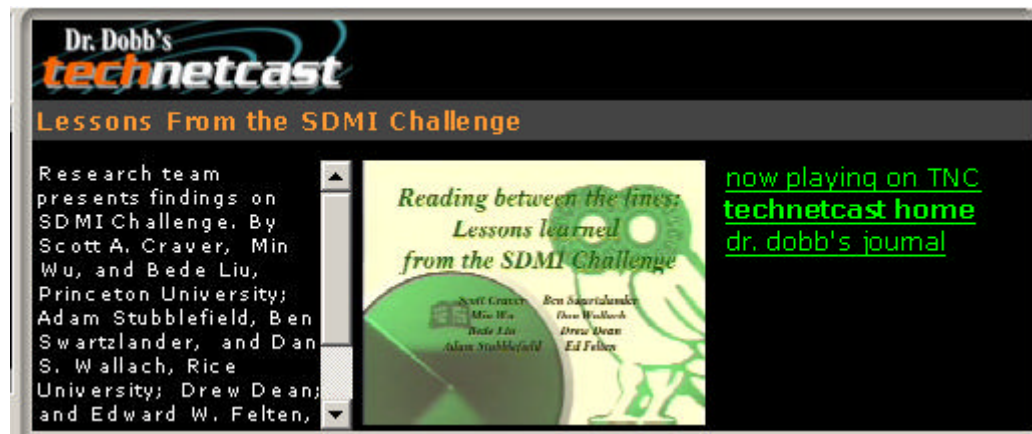
<http://www.research.philips.com/InformationCenter/Global/FArticleSummary.asp?lNodeld=985>

SDMI Challenge

- **Secure Digital Music Initiative:** «proteger la reproducción, almacenamiento y la distribución de la música digital» <http://www.sdmi.org>
- Sistema de protección
- 6 de Septiembre 2000: «An open letter to the Digital Community»
- 4 sistemas de marcado
- *Princeton University, Rice University: Reading between the lines: Lessons from the SDMI Challenge, Proceedings of the 10th USENIX Security Symposium*

SDMI Challenge II

- <http://www.cs.princeton.edu/sip/sdmi>
- **SDMI**, RIAA, Verance Corporation.
- 2nd challenge



<http://www.technetcast.com/sdmi-challenge.html>

Qué se puede conseguir?

- **Limitaciones:** incapacidad de « cualquier cosa » para evitar copias.
- *Bruce Schneier*: propiedad inherente al formato digital.
- SDMI: « *keep honest people honest* »
 - *Blue Spike*

Fingerprinting

- Watermarking de un código único
- **Código que identifica** a una obra: fingerprint (*huella digital*)
- Se **almacenan** todos los códigos en una base de datos
- El código está relacionado con la señal de audio, se extrae de la misma.

Ventajas

- Hacen posibles monitorizar y detectar qué está sonando

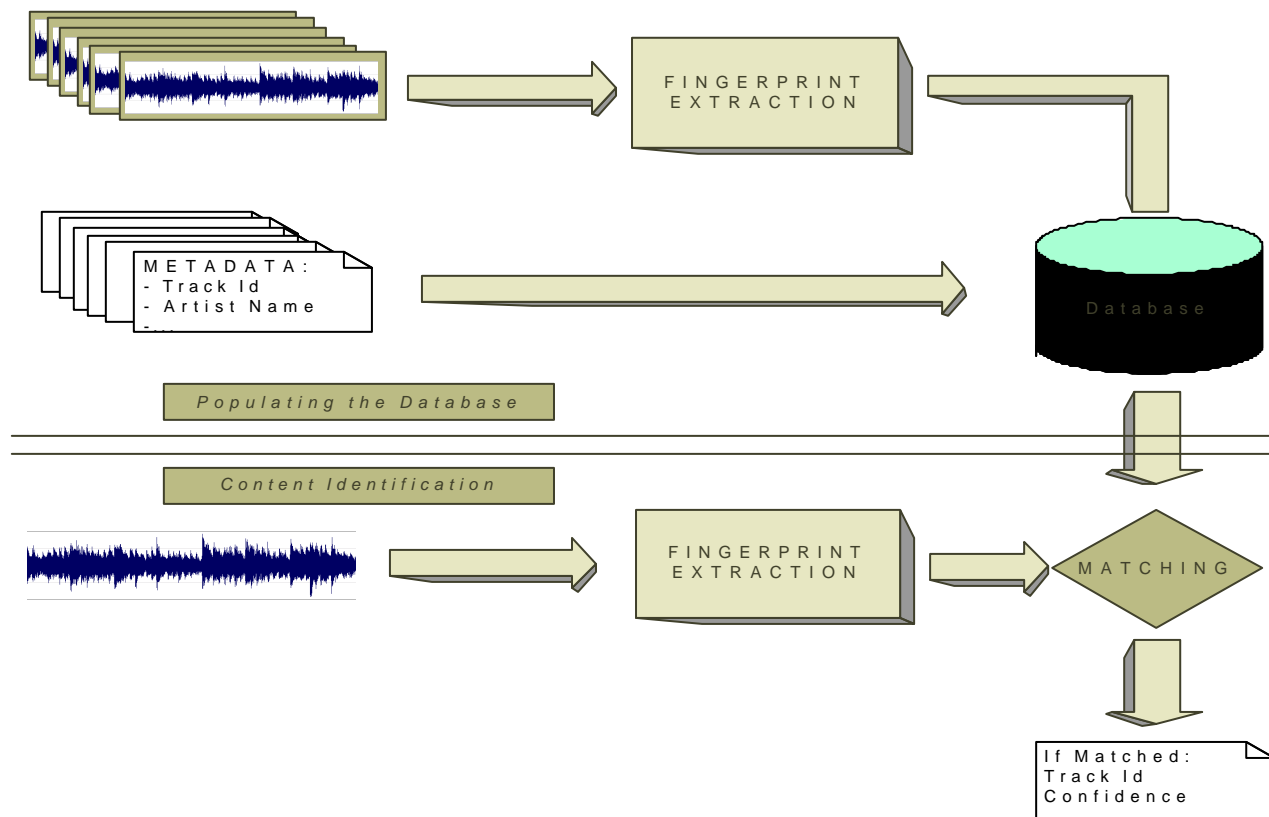


Figure 7: Fingerprinting overall functionality

	Watermarking	Audio Fingerprint
Tasa de errores	Baja P_e	Baja P_e , falsos positivos
Robustez	Robusto	Más robusto (> SNR & basado en el contenido)
Seguridad	No hay un sistema perfecto	Per se más seguro
Imperceptibilidad	Compromiso	Sin diferencia
Versatilidad	Audio ya en circulación	Más versátil
Escalabilidad	Perfectamente escalable	Menos
Complejidad	Menor	Mayor (necesidad de una base de datos)
Dependencia	Independiente de la señal	Relativo al contenido
emilia.gomez@iug.unf.es		

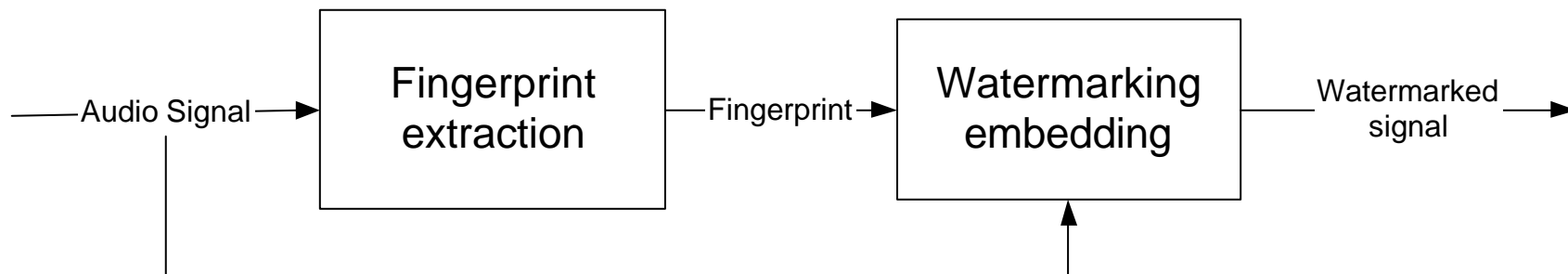
Comparación

Watermarking	Fingerprinting
<ul style="list-style-type: none"> 👤 Posibilidad de discriminar entre copias idénticas 👤 Aplicaciones donde la información es independiente de la señal de audio 👤 No lo suficientemente seguro 👤 Material sin marcar 	<ul style="list-style-type: none"> 👤 Teóricamente robusto a transformaciones que preserven el contenido 👤 Extensión a medidas de similitud 👤 Se necesita una base de datos 👤 Alta complejidad que se incrementa con la talla de la base de datos 👤 <i>Mismatch attack</i> vs diferenciar entre versiones

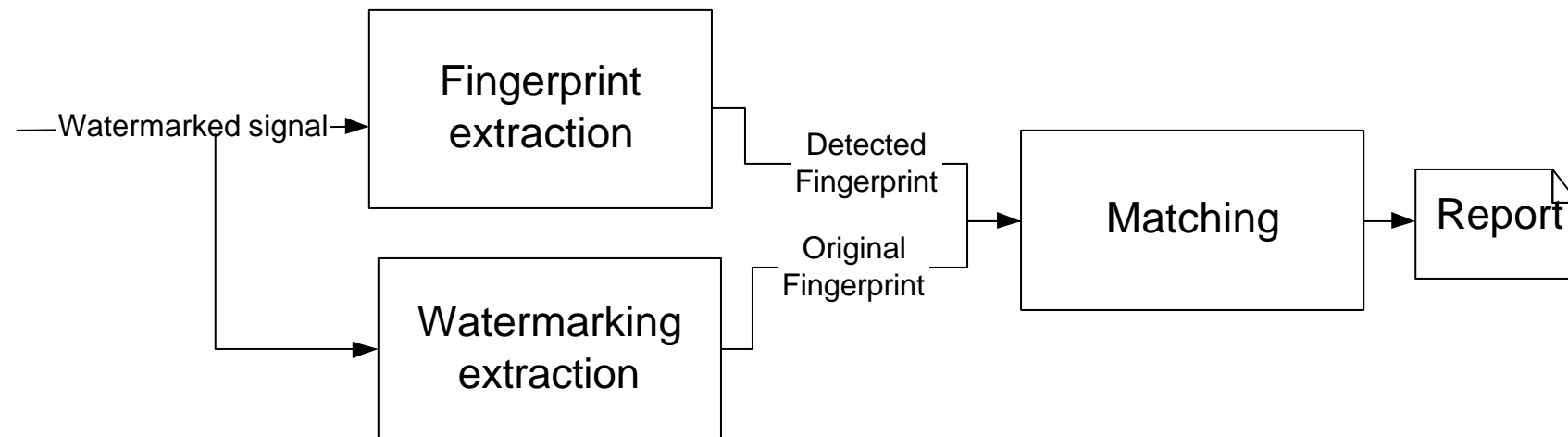
Integrity-verification

- Verificar si los datos han sufrido manipulaciones
 - VeriData <http://www.signumtech.com/>
- 2 soluciones:
 - *Fragile watermarks*
 - No robustos a modificaciones de cambio de contenido.
 - *Content-based watermarks: marcas basadas en el contenido*
 - Robustos a manipulaciones que preserven el contenido
 - Que codifiquen el contenido

Encoding



Decoding



Requerimientos

1. *Fingerprint robusto* a content-preserving transformations (transmisión, equalization) & watermark.
2. *Watermarking* también *robusto* a estas transformaciones
3. Régimen binario del sistema de marcas suficiente para codificar el fingerprint (100 bps)
4. Definir un método de codificación eficiente

Manipulaciones detectables

- Manipulaciones estructurales
- Adición de señales
- Modificaciones de la escala temporal
- ...

Ventajas

- *vs fragile-watermark:*
 - Se almacena información de contenido.
Conocimiento sobre la manipulación realizada.
- *vs robust watermark:*
 - Rango de modificación más amplio
 - no se necesita una base de datos
- *vs fingerprint:*
 - Está en el audio: se conoce el **match**

Referencias watermarking

- Stefan Katzenbeisser, Fabien A.P. Petitcolas editors, *Information Hiding Techniques for steganography and digital watermark*, Artech House, Computer Security Series, Boston, London, 2000.
- Craver S.A., Wu M., Liu B., *What can we reasonable expect from watermarks?*, IEEE Workshop on Applications of Signal Processing to Audio and Acoustics, New Paltz, New York, October 2001.
- Craver S.A., Wu M., Liu B., Stubblefield A., Swartzlander B., Wallch D.S., Dean D., Felten E.W., *Reading between the lines: Lessons from the SDMI Challenge*, Proceedings of the 10th USENIX Security Symposium, Washington, D.C., August 2001.
- <http://www.watermarkingworld.org/>
- <http://www.iis.fhg.de/amm/techinf/water/>