“Seguridad de la información, utilizando marcado de agua y códigos correctores de errores para imágenes digitales”

Francisco Javier García-Ugalde
Facultad de Ingeniería, UNAM

fgarciau@unam.mx

Marzo-2023

Contenido de la presentación:

- Justificación del marcado de agua digital

  -Marca de agua digital

  -Tipos de marca de agua

  -Algunas aplicaciones de la marca de agua digital
- Objetivos
- Metodología
- Hipótesis
- Sistemas de marca de agua desarrollados
- Resultados

Justificación del marcado de agua digital:

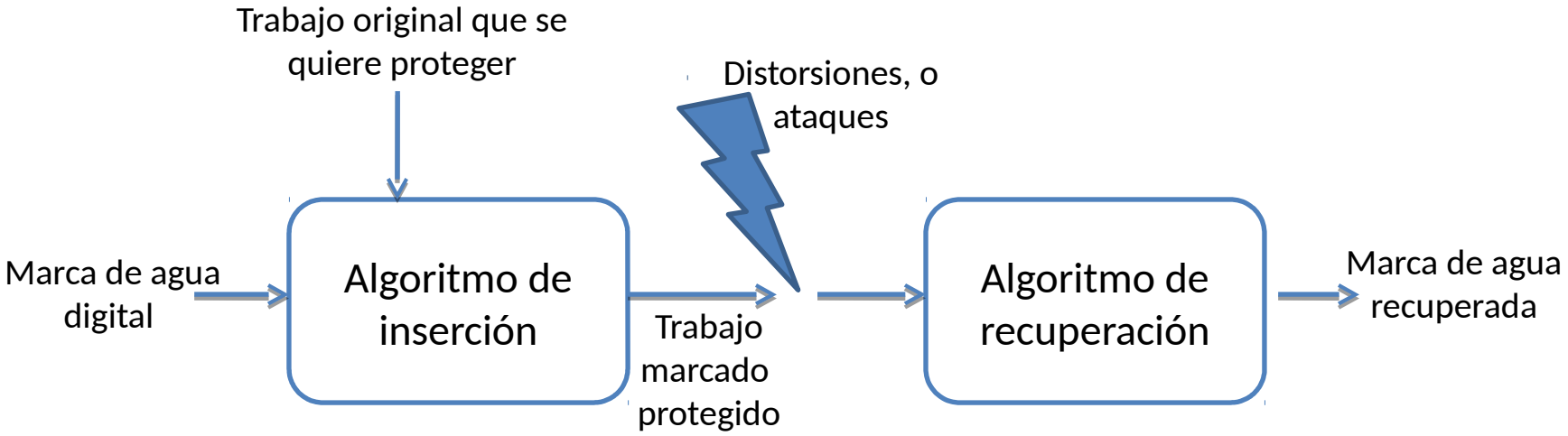
- Las TI facilitan el intercambio de documentos, imágenes, audio y video digital.
- El contenido digital pertenece a un propietario.
- Es necesario proteger la información para evitar falsificaciones, fraudes, copias sin permiso y violaciones al derecho de copia.
- Existen técnicas para proteger la información.

Marca de agua digital

- Inserción de cierta información oculta, o irremovible, en una señal portadora, o huesped.
- La información debe de poder recuperarse, o detectarse.

Marca de agua digital

- Se puede requerir de dos algoritmos:



Tipos de marca de agua

Se clasifican de acuerdo a su:

- **Robustez contra la mayoría de los ataques reportados en la literatura “benchmarking”: compresión, recorte, cambio de escala, rotación, desplazamiento, impresión-escaneo, ruido, etc.**
- Perceptibilidad: visible, invisible, camuflado
- Dominio de inserción: espacial, alguna transformada lineal
- Técnica de detección: coeficiente de correlación, cambio de contraste

Tipos de marca de agua

Se clasifican de acuerdo a su:

- Robustez
- **Perceptibilidad**
- Dominio de inserción
- Técnica de detección

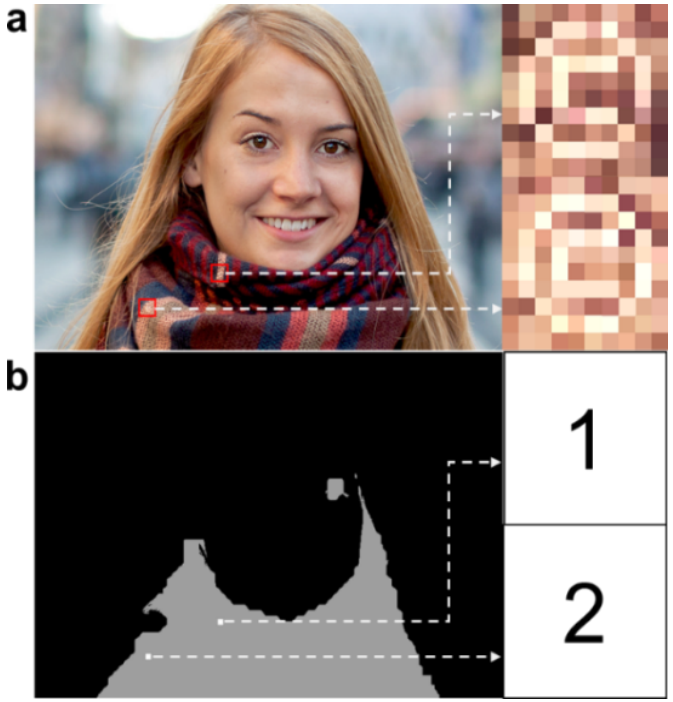
invisible, visible

Ejemplo de marca de agua invisible y visible

Perceptibilidad: camuflada [3]

A la derecha, version con marca de agua de la imagen #20 incluyendo un “zoom” de la marca de agua de la region R, en el ángulo inferior derecho. A la izquierda, la region de marca de agua *R* para cada caso, donde la imagen marcada se reduce a: (a) 50%, (b) 30%, (c) tamaño “digest”, 5½ x 8¼ inches, (d) 17%, y (e) 10%.

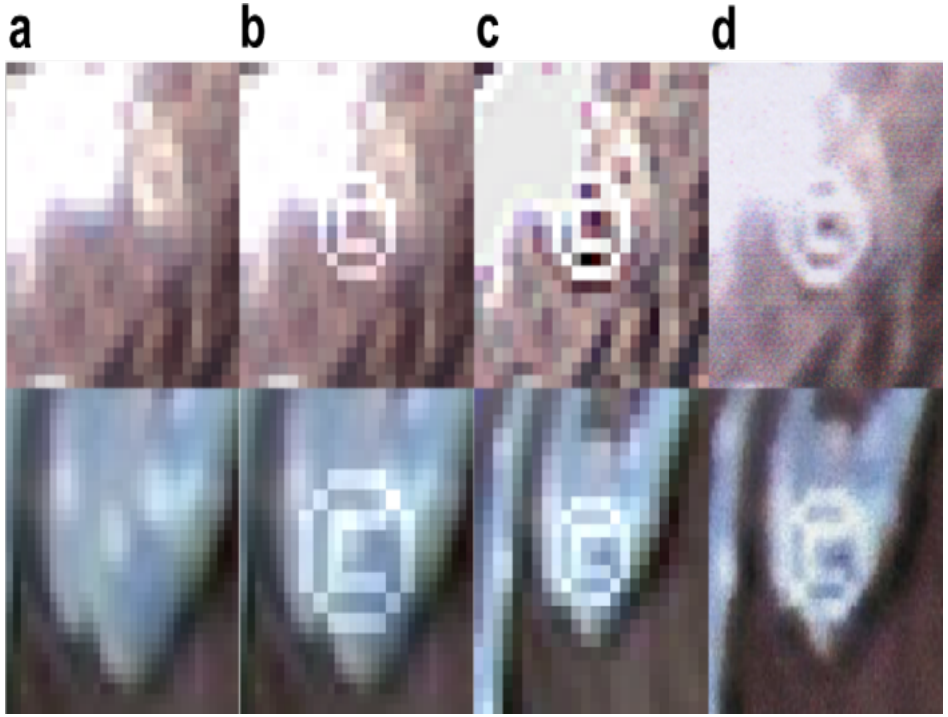
Perceptibilidad: camuflada [3]



Región O_2

Imagen donde la marca de agua se incrustó dos veces: (a) imagen marcada, y (b) region O_2 para incrustar la marca de agua visual, en gris, y los mejores bloques escogidos (que estén cerca de la región de interés ROI, y con ciertas propiedades de luminosidad y textura), en blanco.

Perceptibilidad: camuflada [3]



“Zoom” de las representaciones de las dos regiones R de la marca de agua, en diferentes etapas de un proceso: (a) antes del marcado de agua, (b) region de la marca de agua, antes de los ataques, (c) region de la marca de agua, después de un proceso de edición, y (d) region de la marca de agua, después de un proceso de impresión-escaneo.

Perceptibilidad: camuflada “imperceptible visible” (IVW) [4]

Imagen HDR de color marcada (high dynamic range: por lo menos 10 bits/pixel/componente de color). La base de datos fue proporcionada por la Universidad de Stuttgart.

Perceptibilidad: camuflada (IVW) [4]

Revelado de la marca en la imagen HDR

Tipos de marca de agua

Se clasifican de acuerdo a su:

- Robustez
- Perceptibilidad
- **Dominio de inserción**
- Técnica de detección

espacial,
transformada de Fourier, u otra.

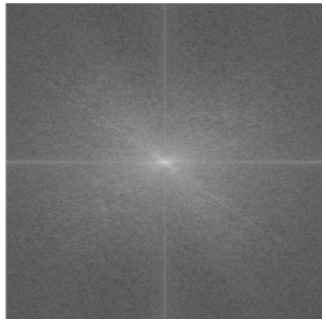


Imagen “lena” y su transformada discreta de Fourier 2D

Tipos de marca de agua

Se clasifican de acuerdo a su:

- Robustez
- Perceptibilidad
- Dominio de inserción
- **Técnica de detección, por ejemplo: teoría de la decisión, coeficiente de correlación, o cambio de las condiciones de despliegue en términos de luminancia**

Propiedades de otro sistema de marca de agua desarrollado

- Robusto
- Invisible
- Dominio transformado, por ejemplo: Fourier, DCT, *"contourlet"*
- No informado: no requiere de la imagen original.

Aplicaciones de la marca de agua digital

- Protección a los derechos de autor
- Autenticación

Objetivos

- Implementar un algoritmo para imágenes digitales monocromáticas (8bits/pixel), o color RGB, de inserción y recuperación de una marca de agua binaria. Por ejemplo: en el dominio de la transformada *contourlet*.

- Mejorar la robustez de la marca de agua utilizando la teoría de la decisión, y la codificación de canal.

Objetivos

- Comparar los resultados utilizando codificación de canal, respecto a los resultados obtenidos sin usar codificación de canal.
- Comparar los resultados utilizando decisión dura “hard-decision”, y decisión suave “soft-decision” en la decodificación.
- Comparar los resultados utilizando dispersión de espectro “spread-spectrum”, para la marca de agua codificada.
- Evaluar la calidad de la imagen marcada, usando un índice de similaridad estructural, SSIM.

Metodología propuesta

- Implementar los algoritmos de inserción y recuperación de la marca de agua.

- Implementar la codificación de la marca de agua utilizando un código convolucional, o un código de bloque.

- Hacer la dispersión de espectro de la marca de agua codificada, usando la técnica de “secuencia directa”.

Metodología propuesta

- Utilizar la teoría de la decisión en la detección de la marca de agua.

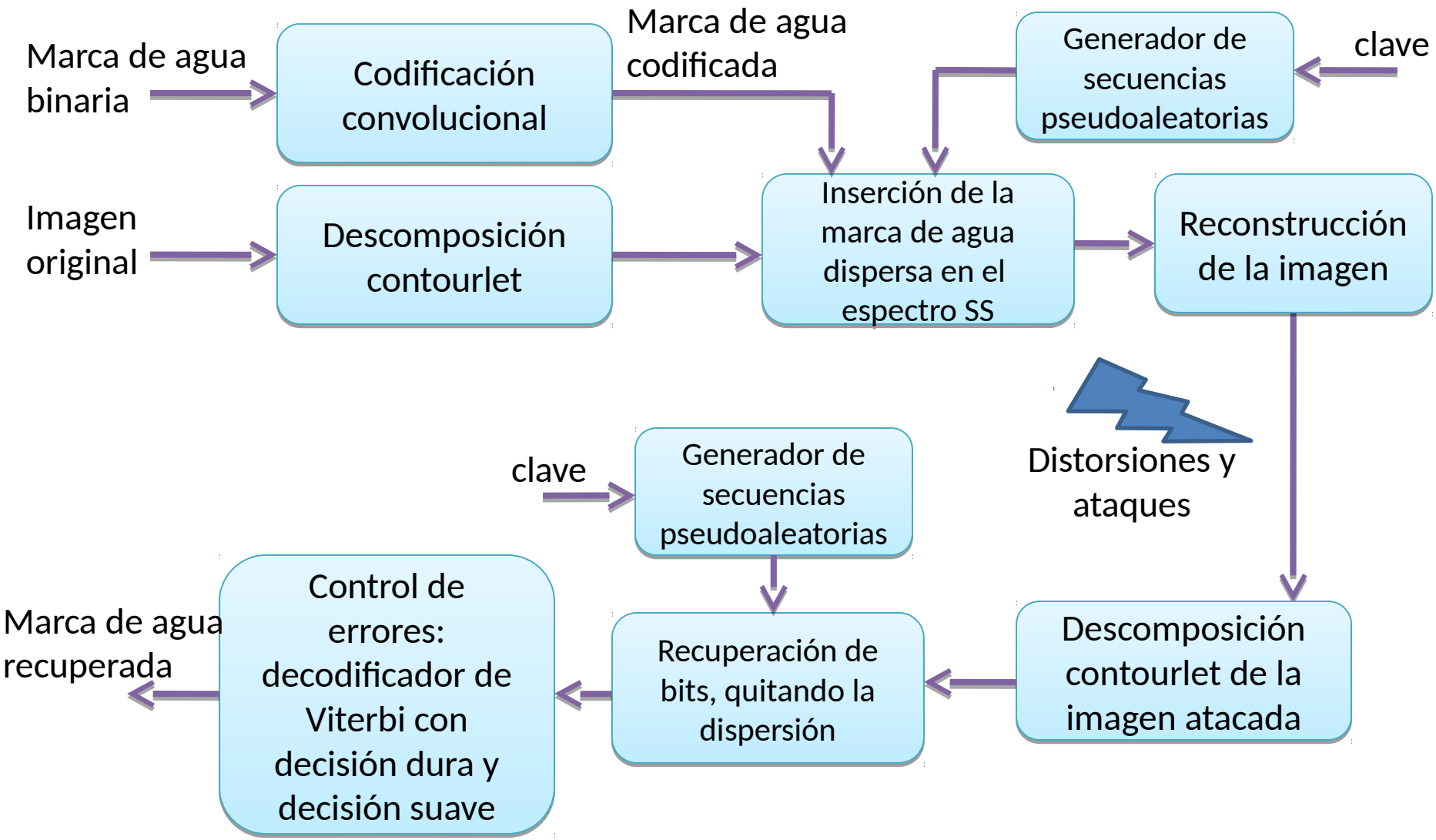
- Para medir la degradación, utilizar el índice de similaridad estructural SSIM, entre la imagen marcada y la imagen original.

- Evaluar la robustez del sistema de marcado de agua, realizando a la imagen marcada varios “ataques”, que aparecen comúnmente en los sistemas de transmisión de información digital.

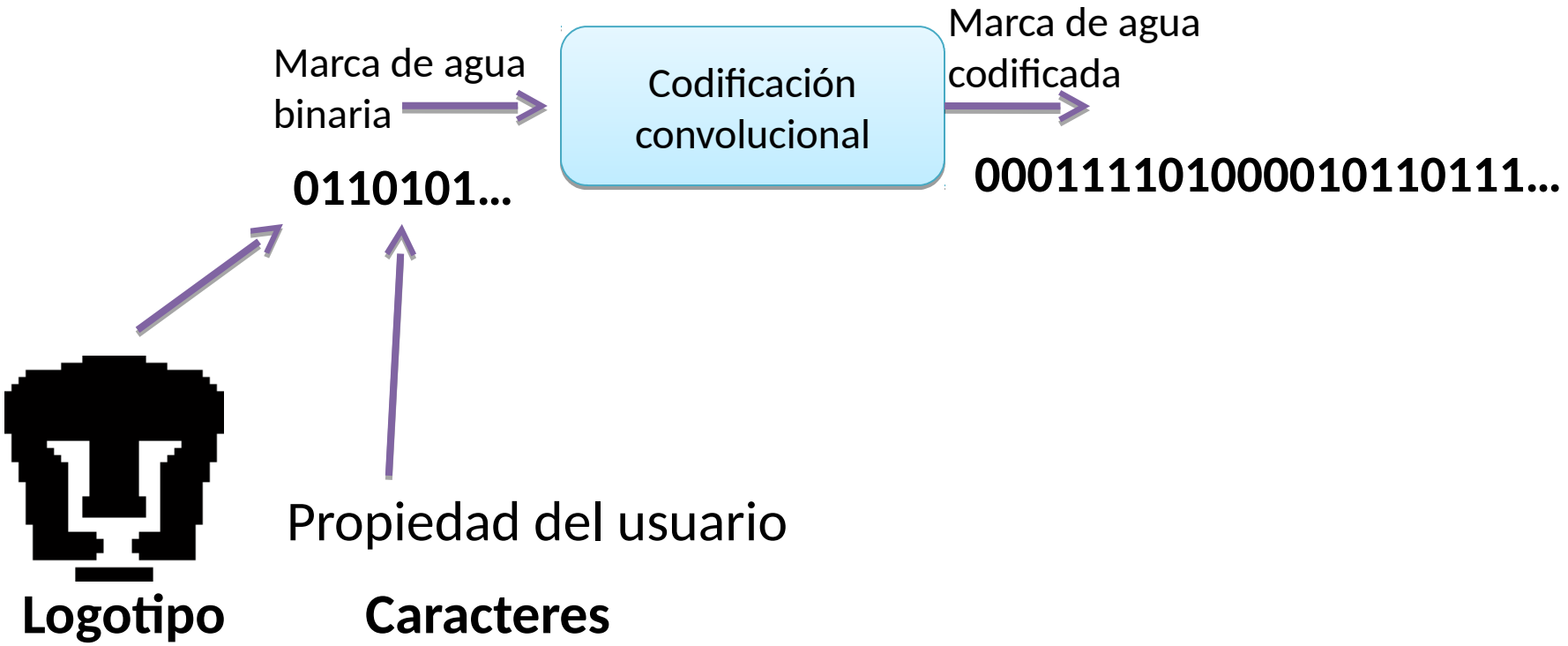
Hipótesis de diseño

- La codificación de canal de la marca de agua aumentará su robustez.
- Utilizando decisión suave (*soft-decision*) en el decodificador de Viterbi, la marca de agua recuperada tendrá menos errores respecto al caso del uso de decisión dura (*hard-decision*).
- Para aumentar aún más la robustez, se utilizará también una técnica de espectro disperso.
- La medida de similitud estructural (SSIM), permite evaluar la calidad perceptual de la imagen marcada.

Algoritmo de marcado de agua propuesto [1], [2]



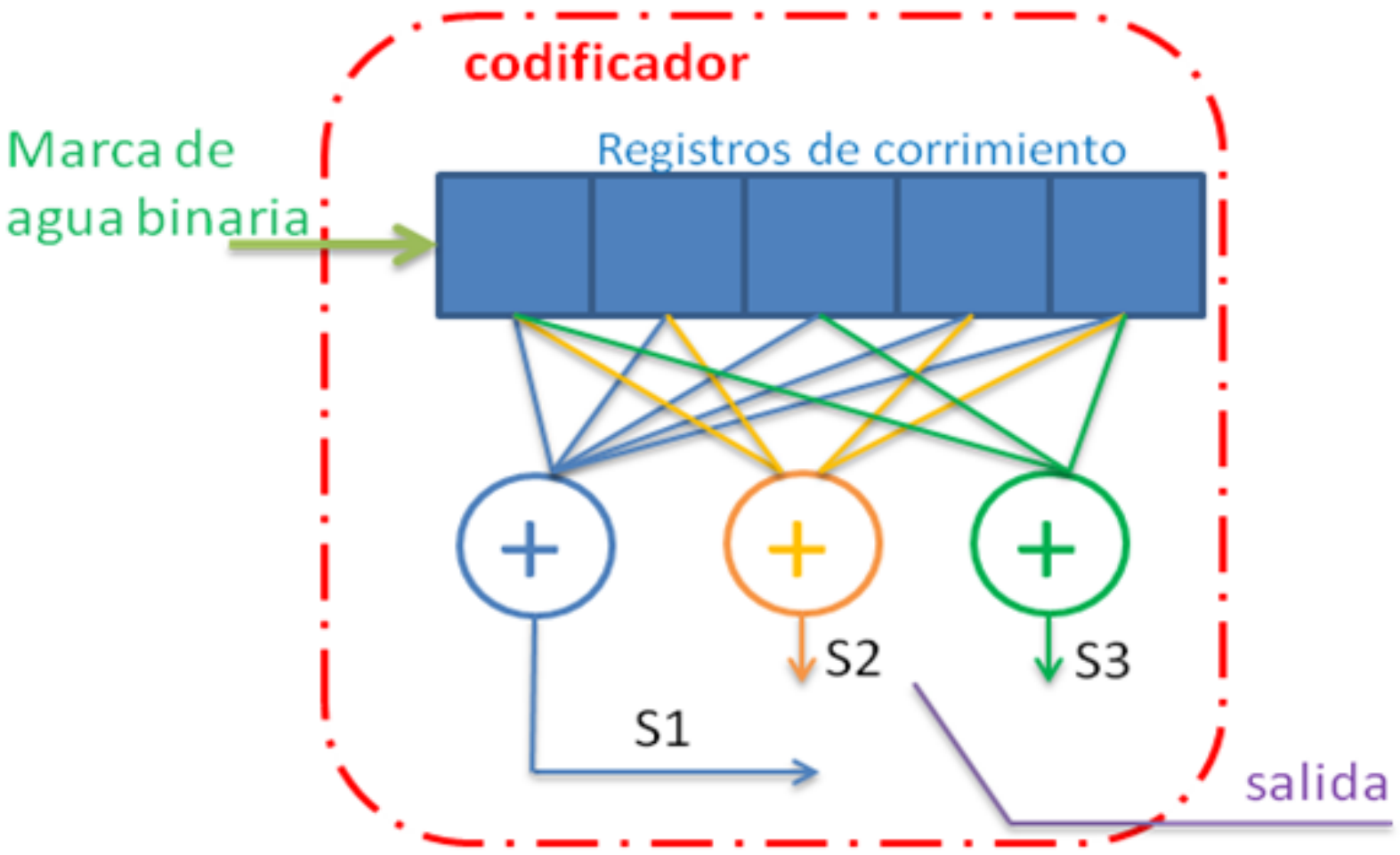
Codificación convolucional



Codificación convolucional

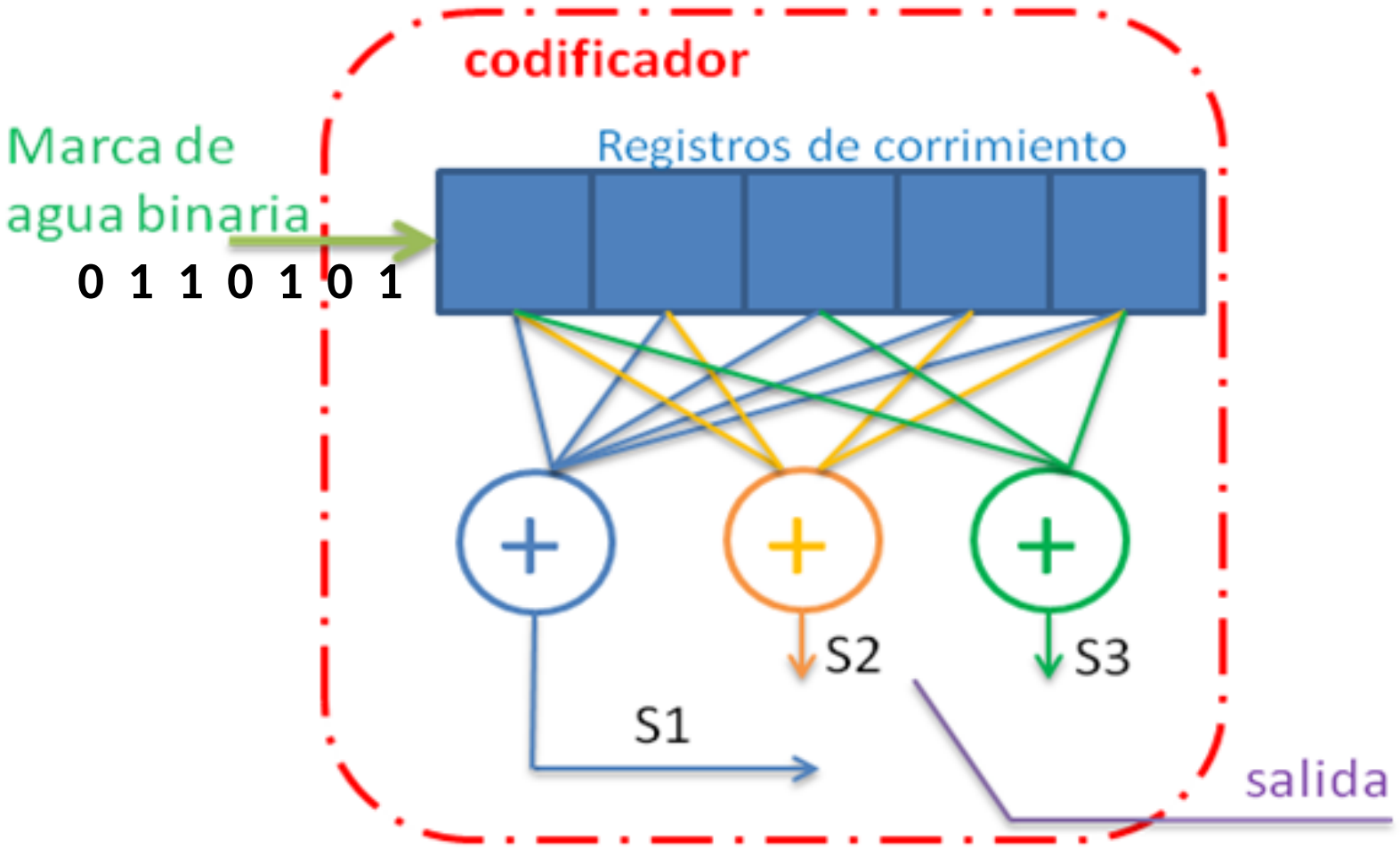
- En función de la aplicación, se optó por una codificación de canal convolucional.
- Mapea la señal a transmitir de un espacio vectorial de menor dimensión, a otro de mayor dimensión, de tal forma que sea menos susceptible a sufrir alteraciones en el canal de comunicaciones.
- Modo de corrección de errores: *Forward Error Correction* (FEC).
- Se compara el desempeño entre la decisión dura (*hard decision*), y la decisión suave (*soft decision*).

Codificación convolucional



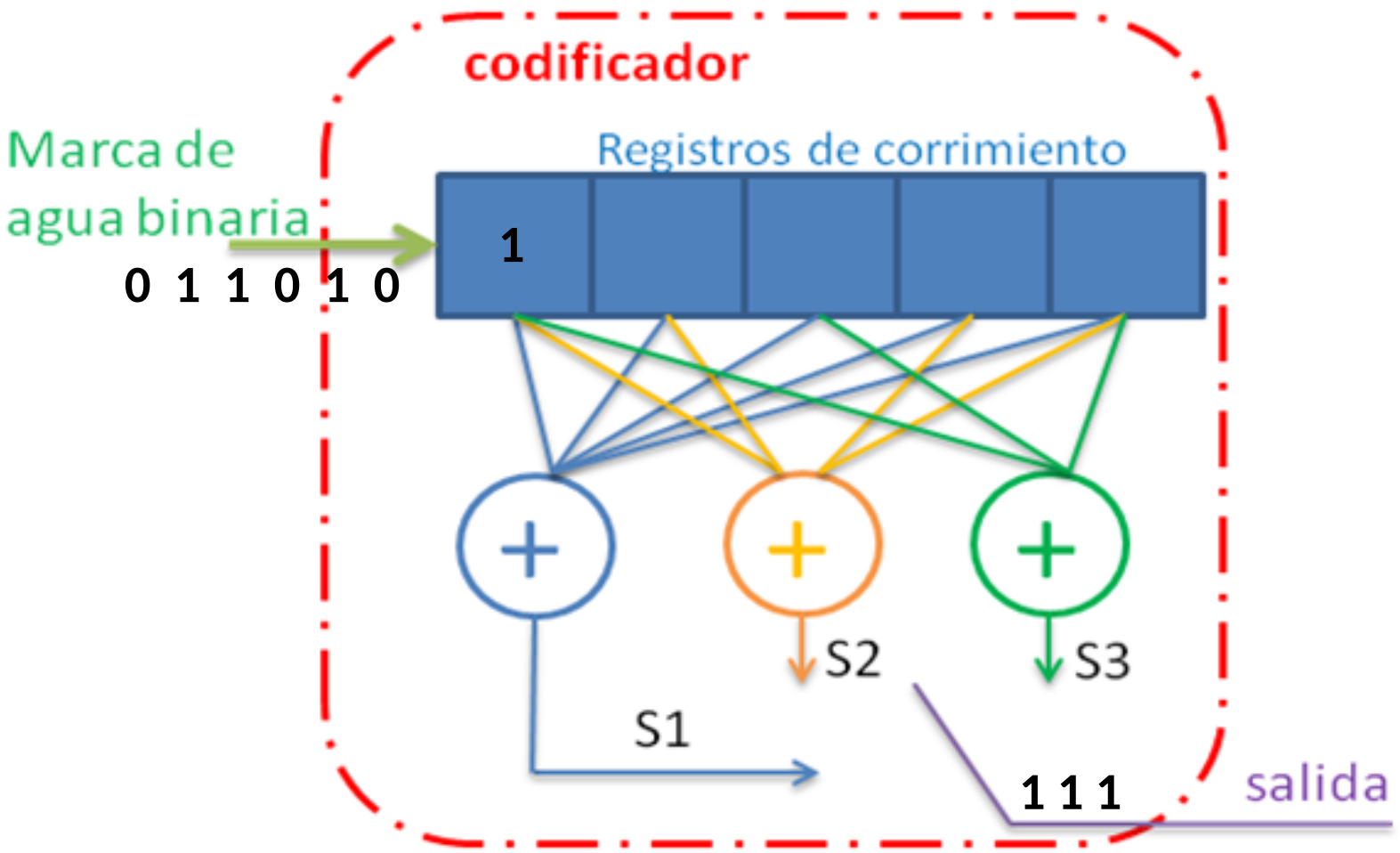
Codificador convolucional

Codificación convolucional



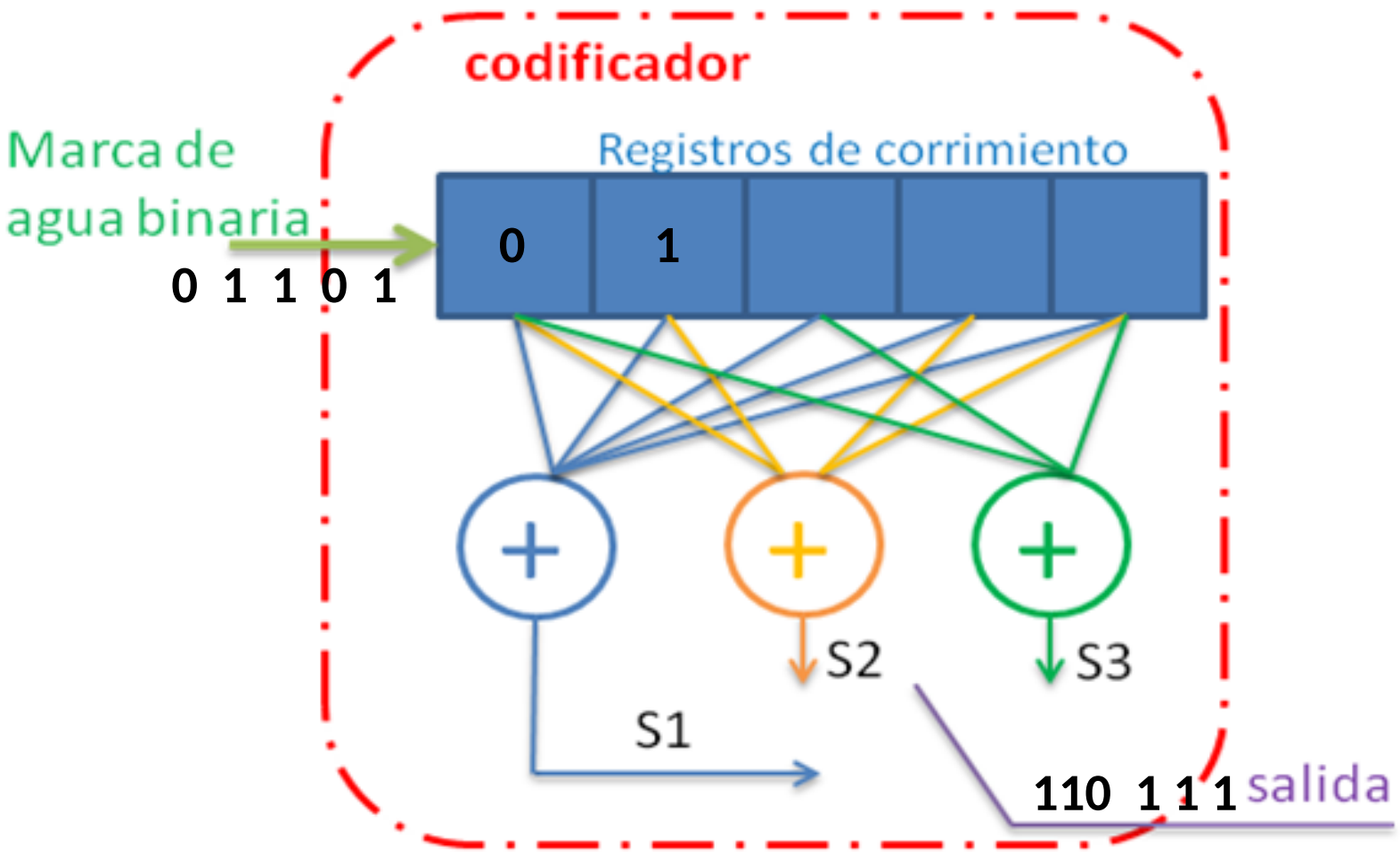
Codificador convolucional

Codificación convolucional



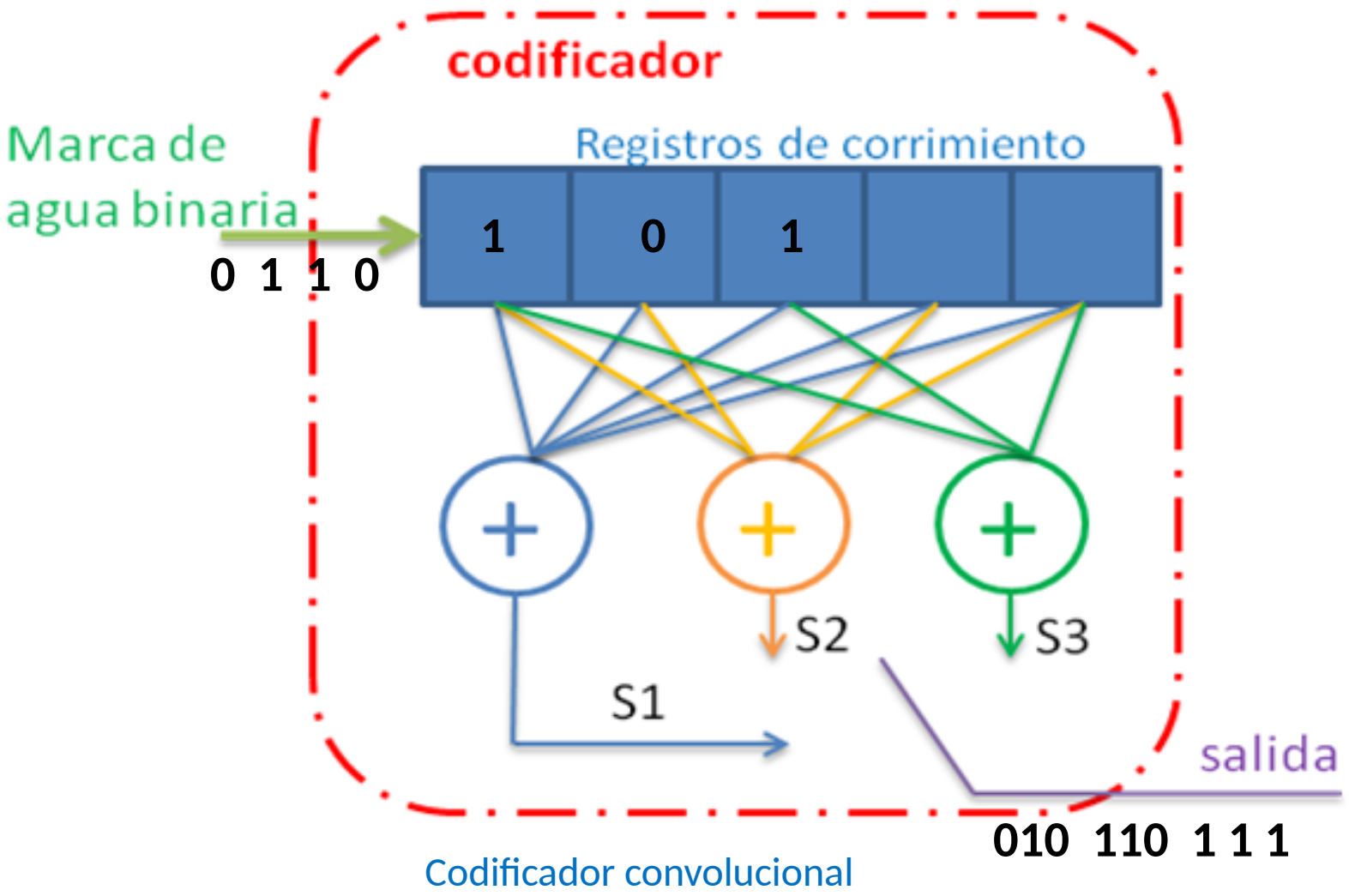
Codificador convolucional

Codificación convolucional



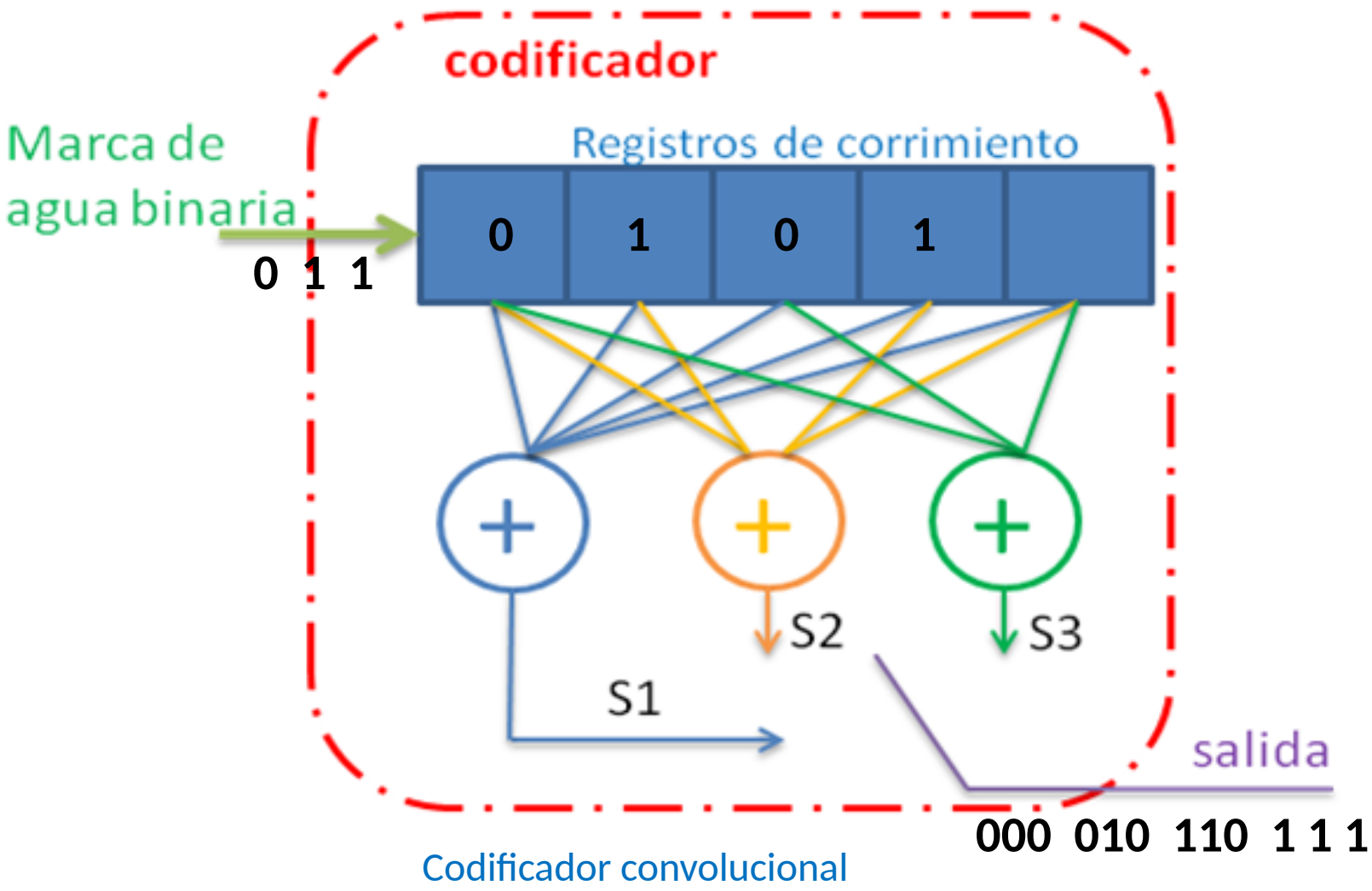
Codificador convolucional

Codificación convolucional



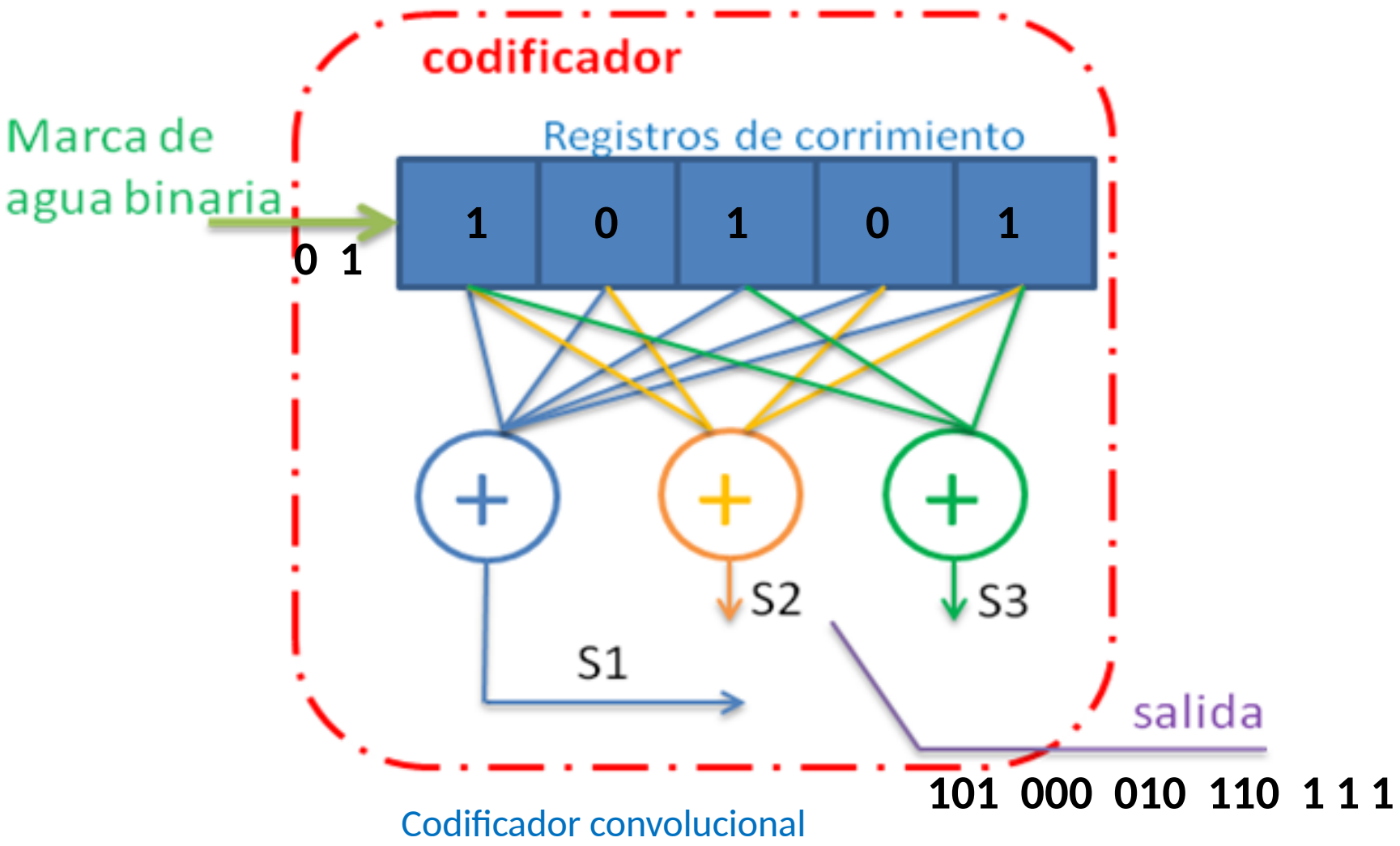
Codificador convolucional

Codificación convolucional



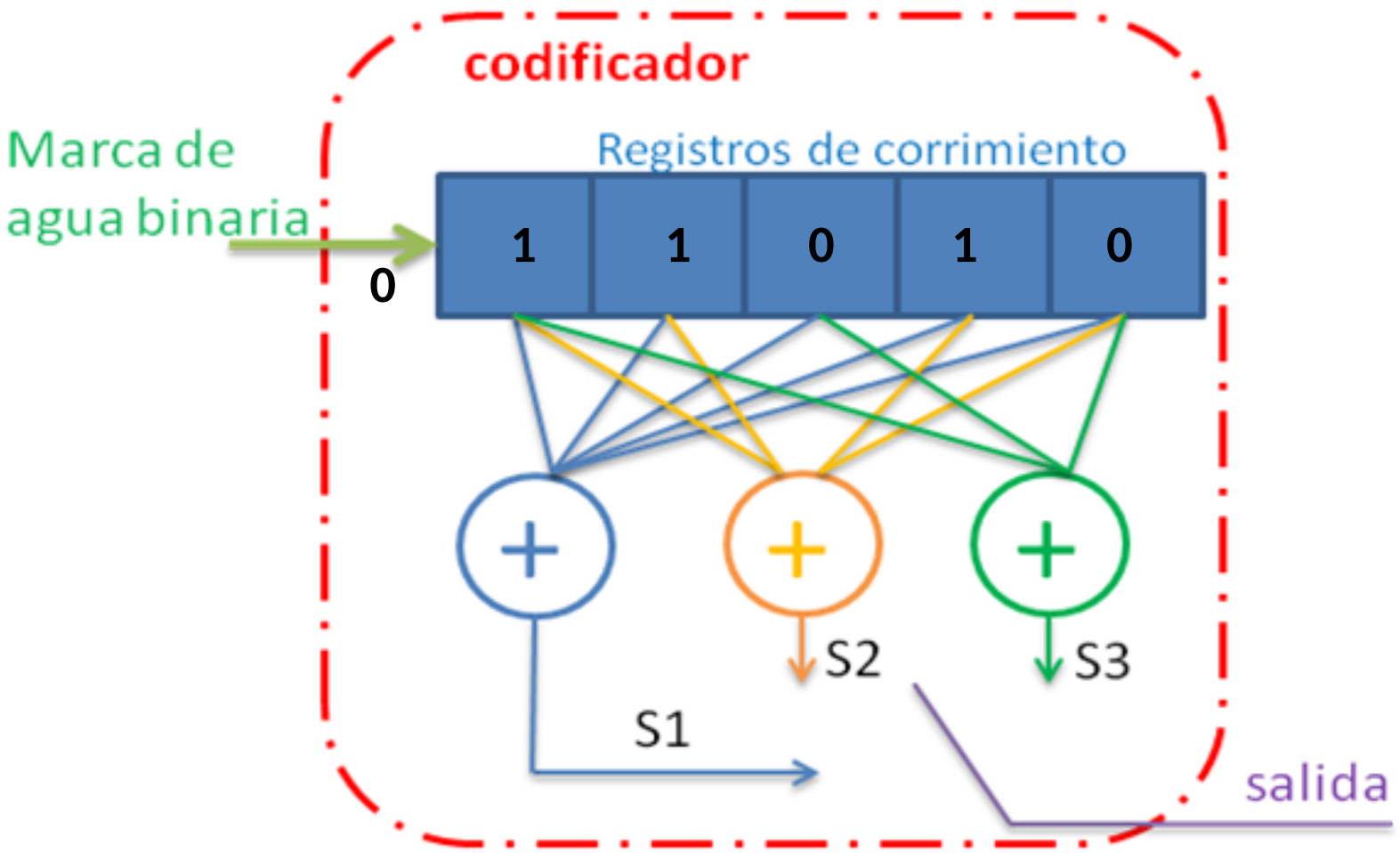
Codificador convolucional

Codificación convolucional



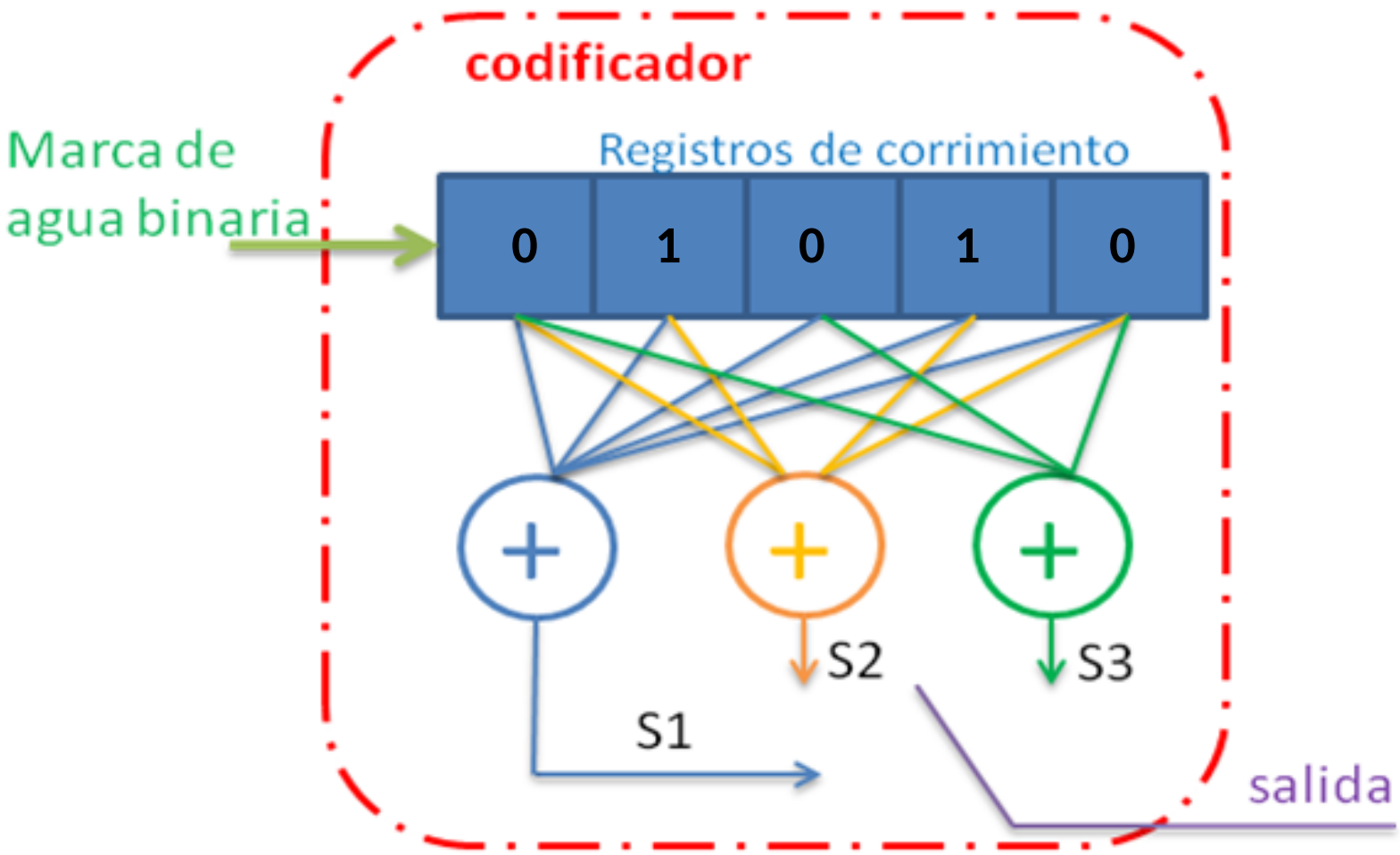
Codificador convolucional

Codificación convolucional



Codificador convolucional

Codificación convolucional



Codificador convolucional

000 111 101 000 010 110 1 1 1

Para una realización se tienen los parámetros de la codificación convolucional

- Tasa del código = 1/3.
- Longitud de restricción: $K=5$.
- Polinomios generadores:

$$g_1 = [1\ 1\ 1\ 1\ 1],\quad g_2 = [1\ 1\ 0\ 1\ 1]\ \text{y}\ g_3 = [1\ 0\ 1\ 0\ 1]$$

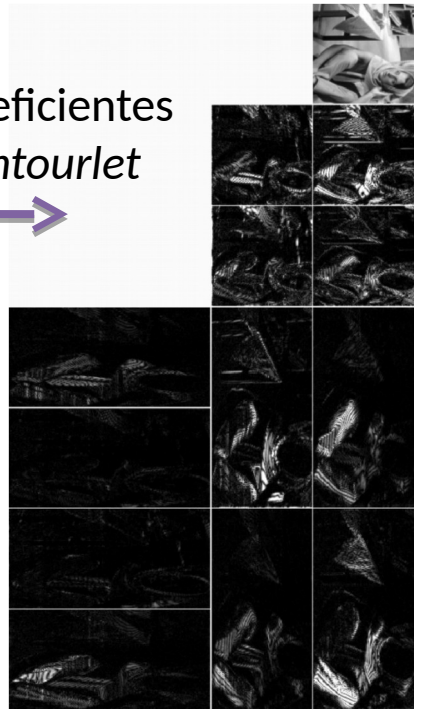
- Distancia libre = $d_{free} \geq 2t+1$
- Corrige hasta t=5 errores para secuencias de longitud, entre 3 K y 5 K. La longitud exacta depende del patrón de errores.

Descomposición *Contourlet*, con filtros direccionales

Imagen original

Descomposición contourlet de 2 niveles

Coeficientes *Contourlet*



Transformada *Contourlet*

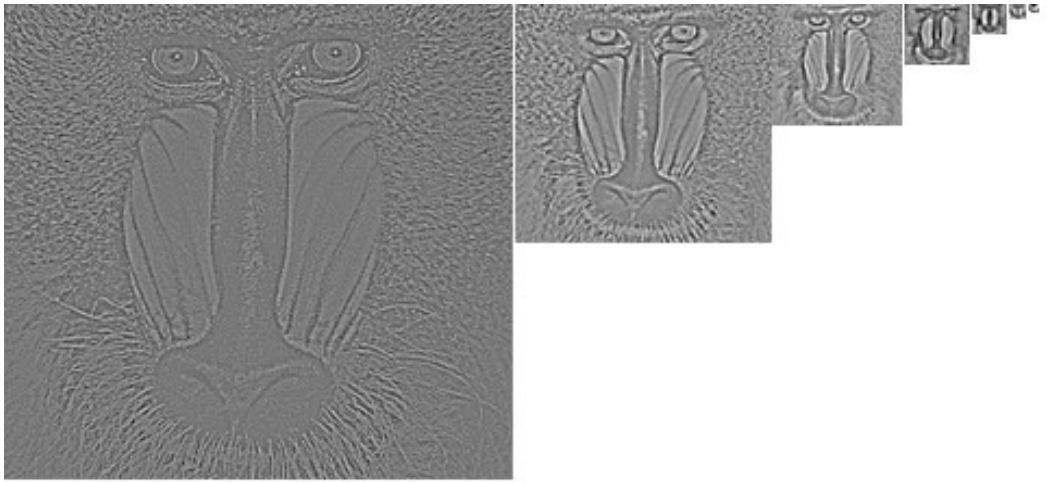
- Realiza una descomposición multiescala y multidireccional de las imágenes.

- Multiresolución: Se consiguen diferentes niveles de resolución utilizando una pirámide Laplaciana (procesamiento digital de imágenes).

Transformada *Contourlet*

- Realiza una descomposición multiescala y multidireccional de las imágenes.

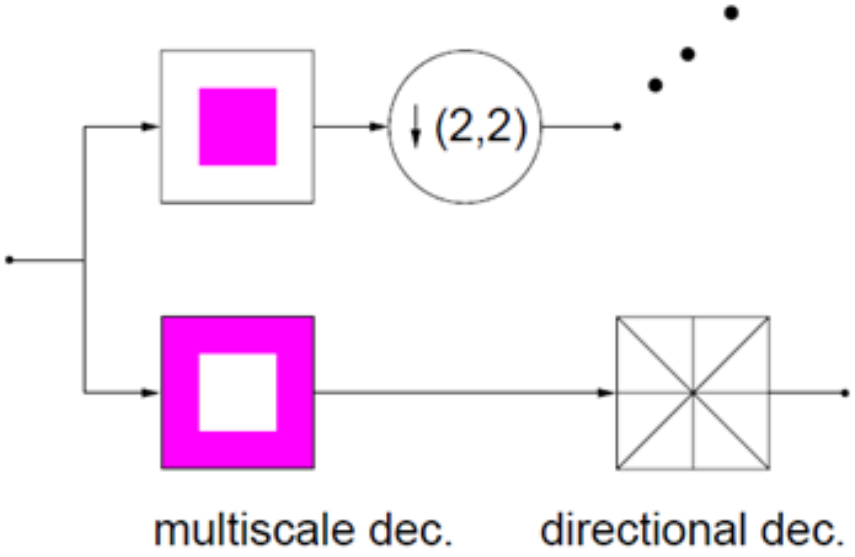
- Multiresolución: Se obtienen diferentes niveles de resolución utilizando la pirámide Laplaciana.

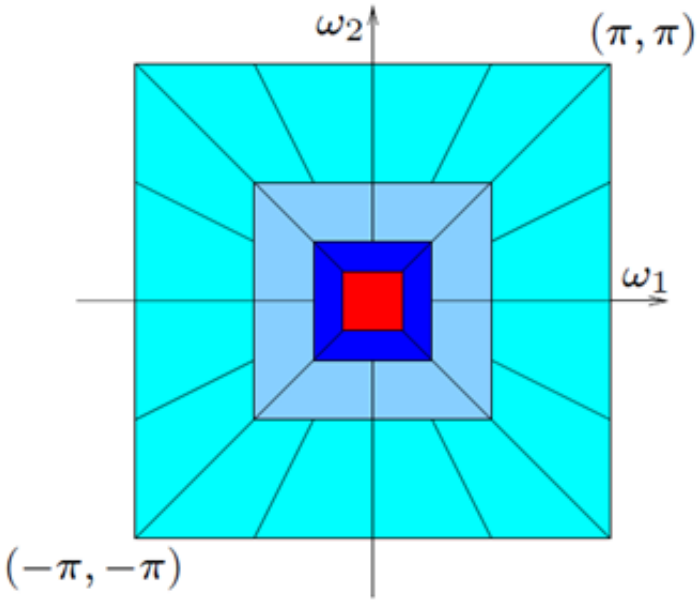


La pirámide Laplaciana de 6 niveles.

Fuente: http://www.prip.tuwien.ac.at/research/research-areas/image-pyramids/laplacian-pyramids

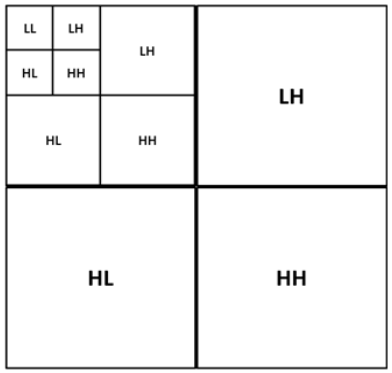
- Realizando la descomposición direccional en el “canal paso-banda” de la pirámide Laplaciana se logra la descomposición multiresolución multidireccional. Aquí se muestran 3 niveles de descomposición:



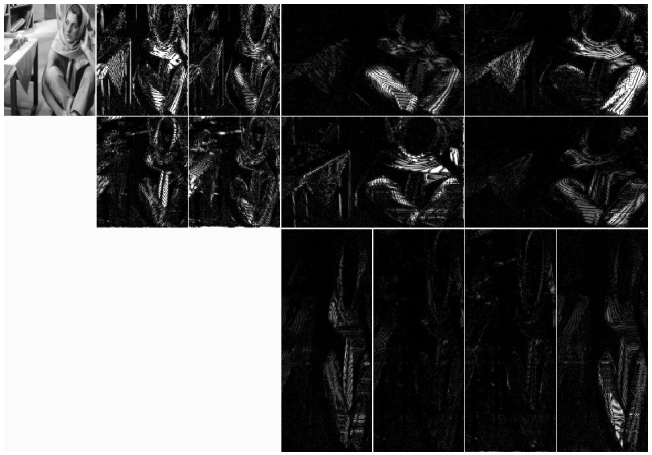


Fuente: Minh N. Do, *Directional Multiresolution Image Representations*, Ph.D. Thesis, October 23, 2001.

- La transformada *contourlet* captura altas frecuencias en diferentes direcciones; detalles y contornos en diferentes orientaciones. A manera de comparación, se tiene la transformada *wavelet*, que solo tiene tres direcciones por nivel de descomposición: HL, LH, HH.



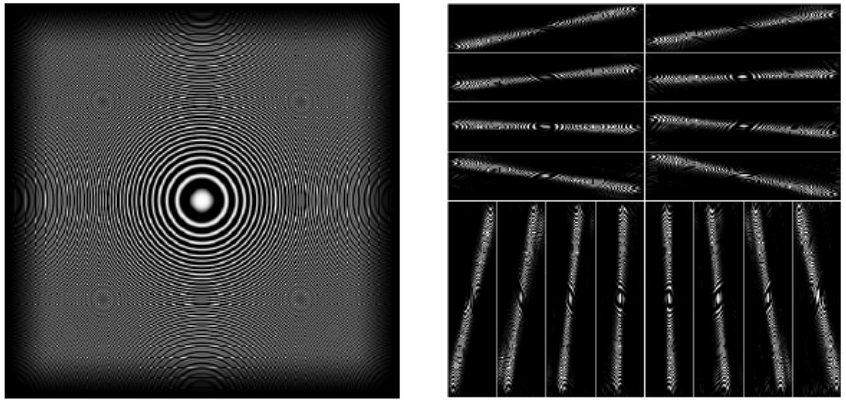
Transformada discreta *wavelet* en 2D de 3 niveles



Transformada *contourlet* de 2 niveles

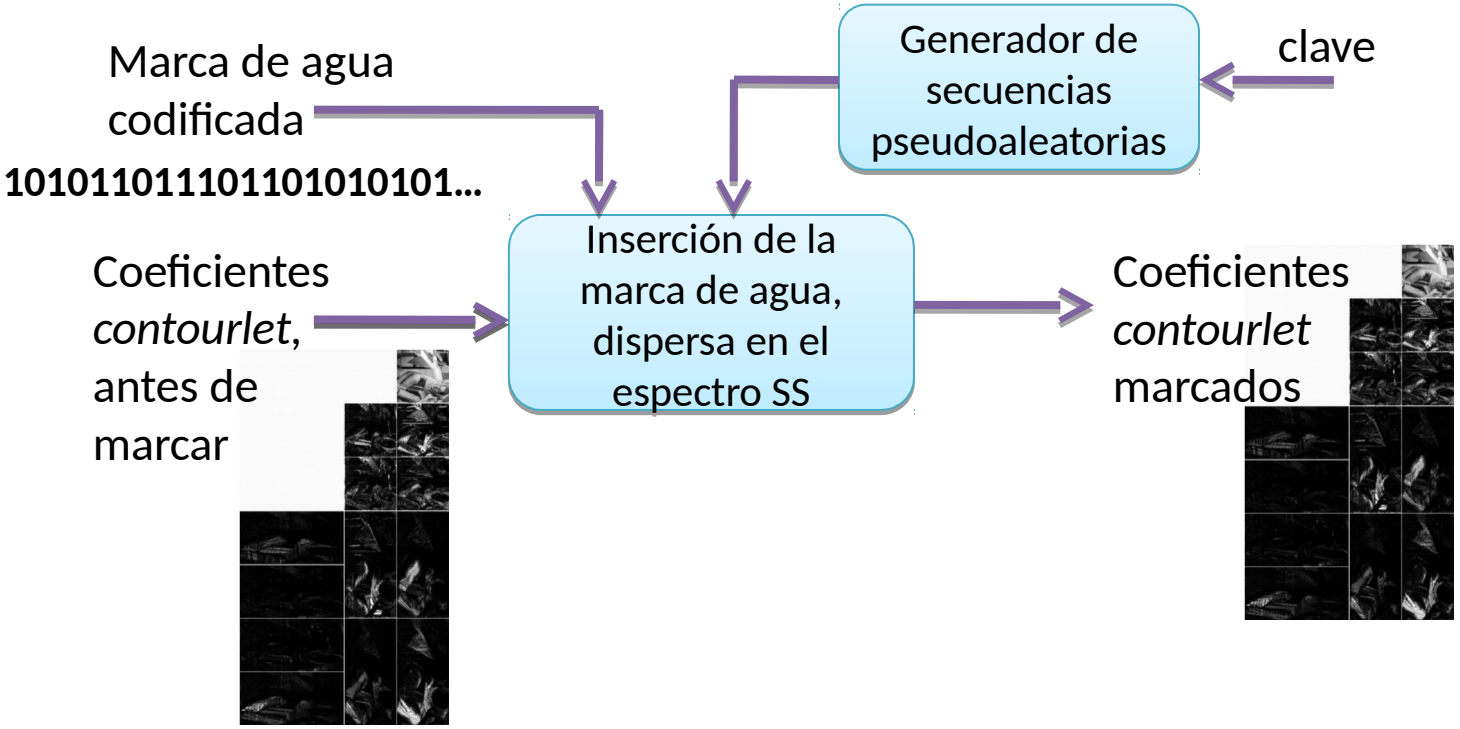
Transformada *Contourlet*

- Descomposición multidireccional: Utilizando un banco de filtros direccionales, se descompone el espectro de la imagen en diferentes direcciones. Aquí se muestra el 3er nivel de una descomposición, con 16 filtros direccionales.



Fuente: Minh N. Do, *Directional Multiresolution Image Representations*, Ph.D. Thesis, October 23, 2001.

Inserción de la marca de agua, con dispersión de espectro, SS (spread spectrum)

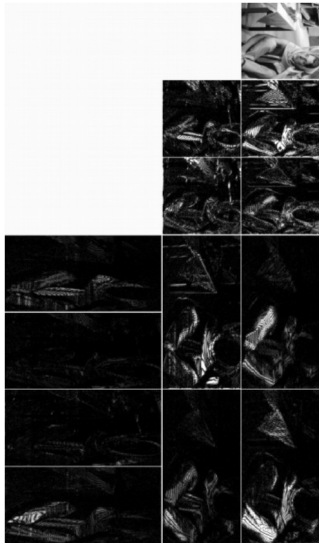


Inserción de la marca de agua dispersa en el espectro, SS

- Técnicas de espectro disperso (utilizadas por diversos sistemas de telecomunicaciones):
- Espectro disperso, método de secuencia directa.
- Cada bit se expande con una secuencia pseodualeatoria generada por una clave.
- El producto [(bit) · (secuencia)] se adiciona a la banda *contourlet*. Generando la banda marcada:

$$Y' = Y + \gamma \sum_{i=1}^{h} w_i P_i$$

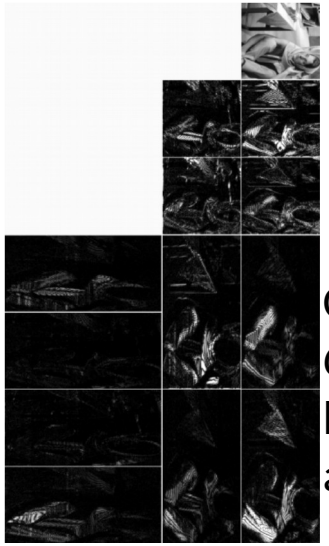
- Donde: w_i es el vector binario de marca de agua de dimensión *h*, modulado en fase: {-1,+1}.
- p_i son matrices no correlacionadas entre sí, de dimensiones *mxm*, que contienen los *"chips"* de secuencias binarias pseudoaleatorias.
- γ (gamma) es un parámetro para controlar la intensidad de la marca de agua.
- *W* es una matriz de *mxm* correspondiente a la banda de la contourlet antes del marcado.
- *W'* es la matriz de *mxm* correspondiente a la banda marcada.



Coeficientes *contourlet* marcados

Reconstrucción de la imagen

Distorsiones y ataques



Coeficientes *Contourlet* de la imagen atacada

Descomposición contourlet

Recuperación de los bits incrustados:

La banda de la contourlet marcada, recibida con ruido N (producto de ataques):

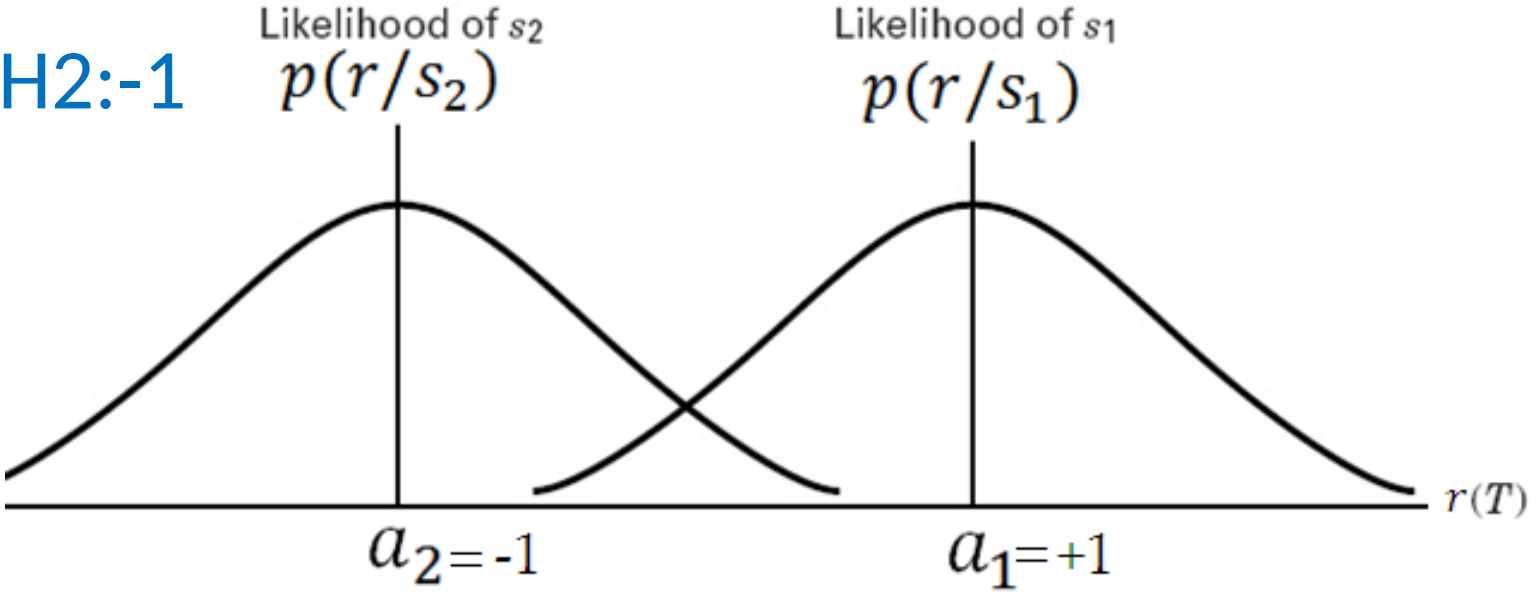
$$R = Y' + N = Y + (\gamma W - \lambda y) \cdot P + N$$

Detección de señales con ruido: la proyección normalizada de *R* en *Pi* es:

$$r_i = \frac{\langle R, P_i \rangle}{\langle P_i, P_i \rangle}$$

Teoría de la decisión para la recuperación con decisión dura de los bits incrustados

- De acuerdo a la teoría de la detección, la salida del correlador es una v.a. Gaussiana continua con media +1 ó -1 : $r_i = w_{i,s} + n_i$
- H1:+1
- H2:-1

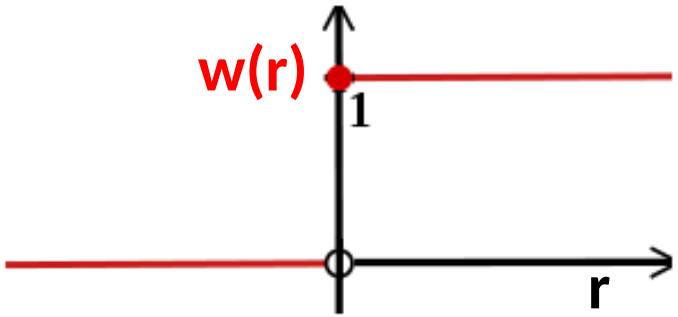


La salida del correlador

Teoría de la decisión para la recuperación con decisión dura de los bits incrustados

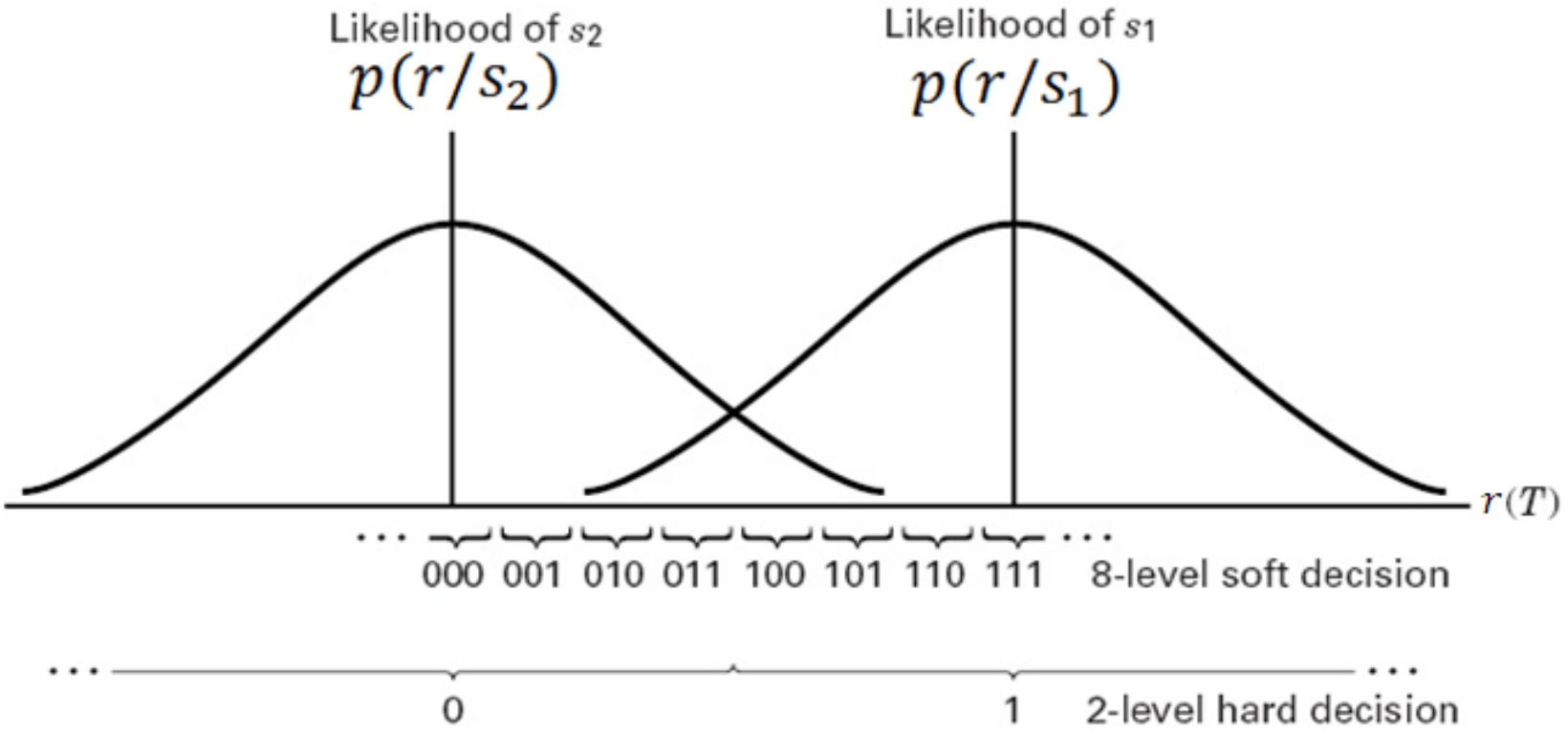
- Utilizando decisión dura, cada bit recuperado *w* es:

$$w = \begin{cases} 1, & si\ r \geq 0 \\ 0, & si\ r < 0 \end{cases}$$



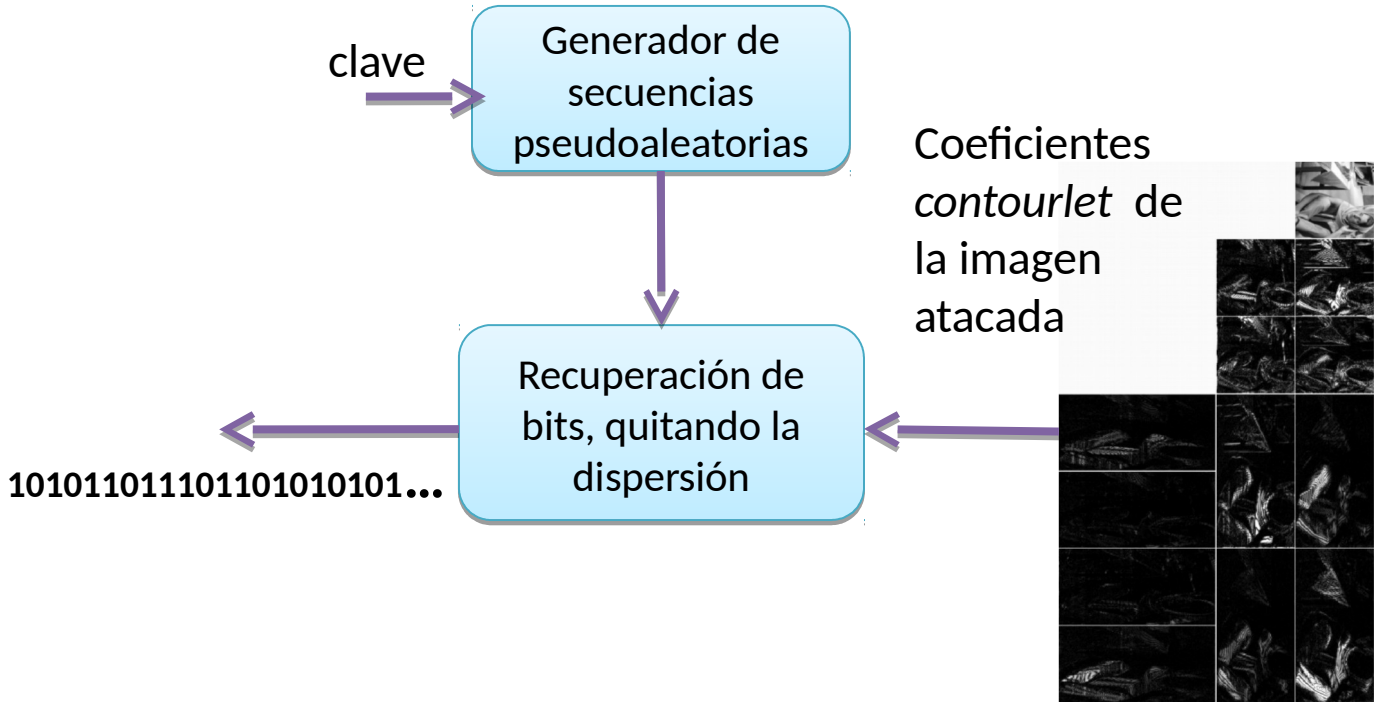
Gráfica de la función que determina cada bit recuperado, con decisión dura.

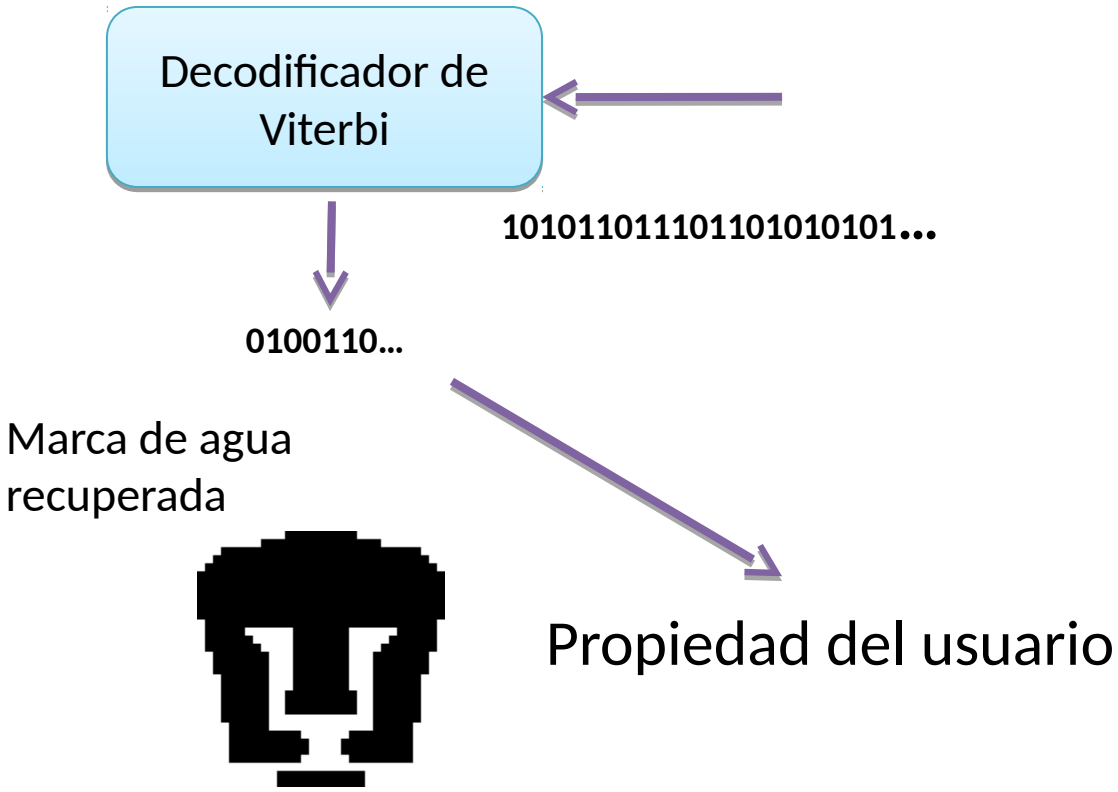
- En comparación aquí se utiliza la decisión suave para la detección de los bits incrustados, con Q=8 niveles de decisión, la salida del correlador puede contener 8 valores cuantizados diferentes, los cuales se envían como vectores al decodificador de Viterbi.



Comparación entre decisión dura y decisión suave.
Fuente: Bernard Sklar, *Digital Communications: Fundamentals and Applications*

Recuperación de los bits de la marca de agua, quitando la dispersión de espectro:




Decodificador de Viterbi
10101101110110101010101...
0100110...
Marca de agua recuperada
Propiedad del usuario

Medición de la calidad de la imagen marcada, para la imperceptibilidad

- **Peak Signal to Noise Ratio: PSNR**

$$PSNR = 10log_{10}\left(\frac{{I_{max}}^2}{MSE}\right)$$

$$MSE = \sum_{m=1}^{M}\sum_{n=1}^{N}\frac{[I_1(m,n)-I_2(m,n)]^2}{M\times N}$$

Otra medición de la calidad de la imagen marcada

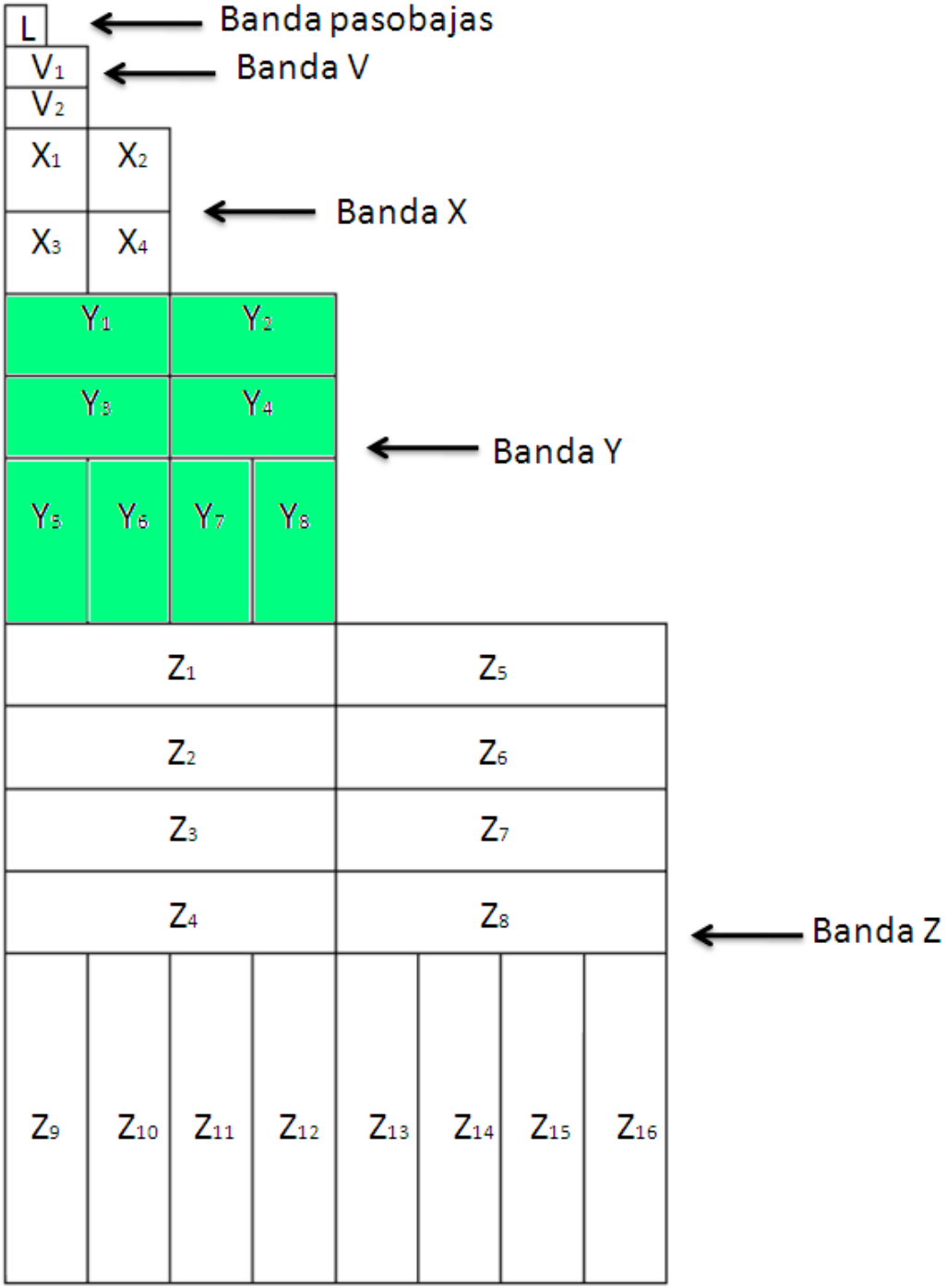
- Se adoptó un **Índice de similaridad estructural (SSIM)** para medir la calidad perceptual.

- Considera 3 características: *luminancia*, *contraste* y *estructura*.

$$SSIM(X,Y) \propto f(l(X,Y), c(X,Y), s(X,Y))$$

Pruebas

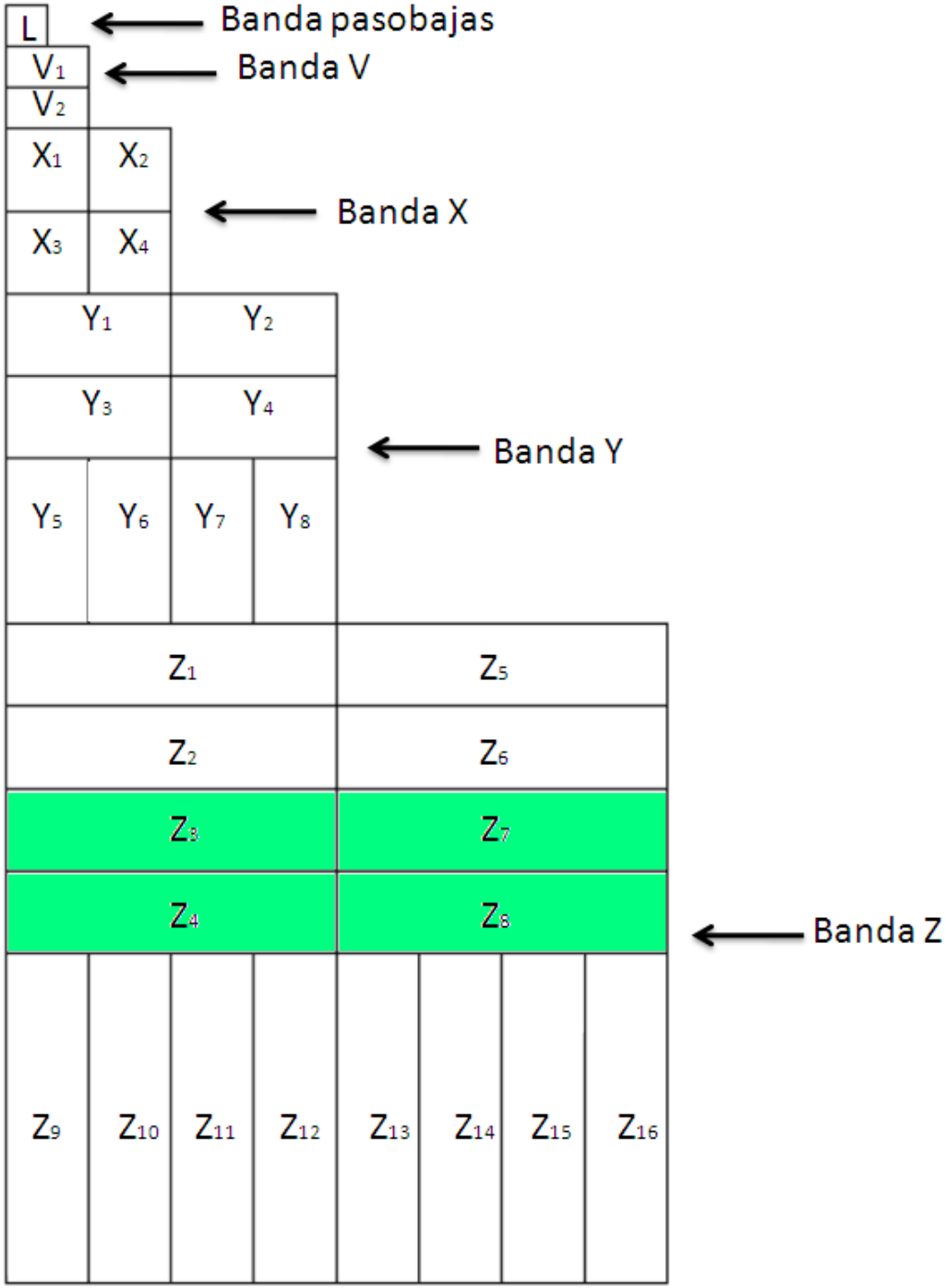
- Se simularon 3 procedimientos:
- ***Procedimiento 1***: Banda Y, del segundo nivel de descomposición.



Bandas contourlet utilizadas en el proc. 1

Pruebas

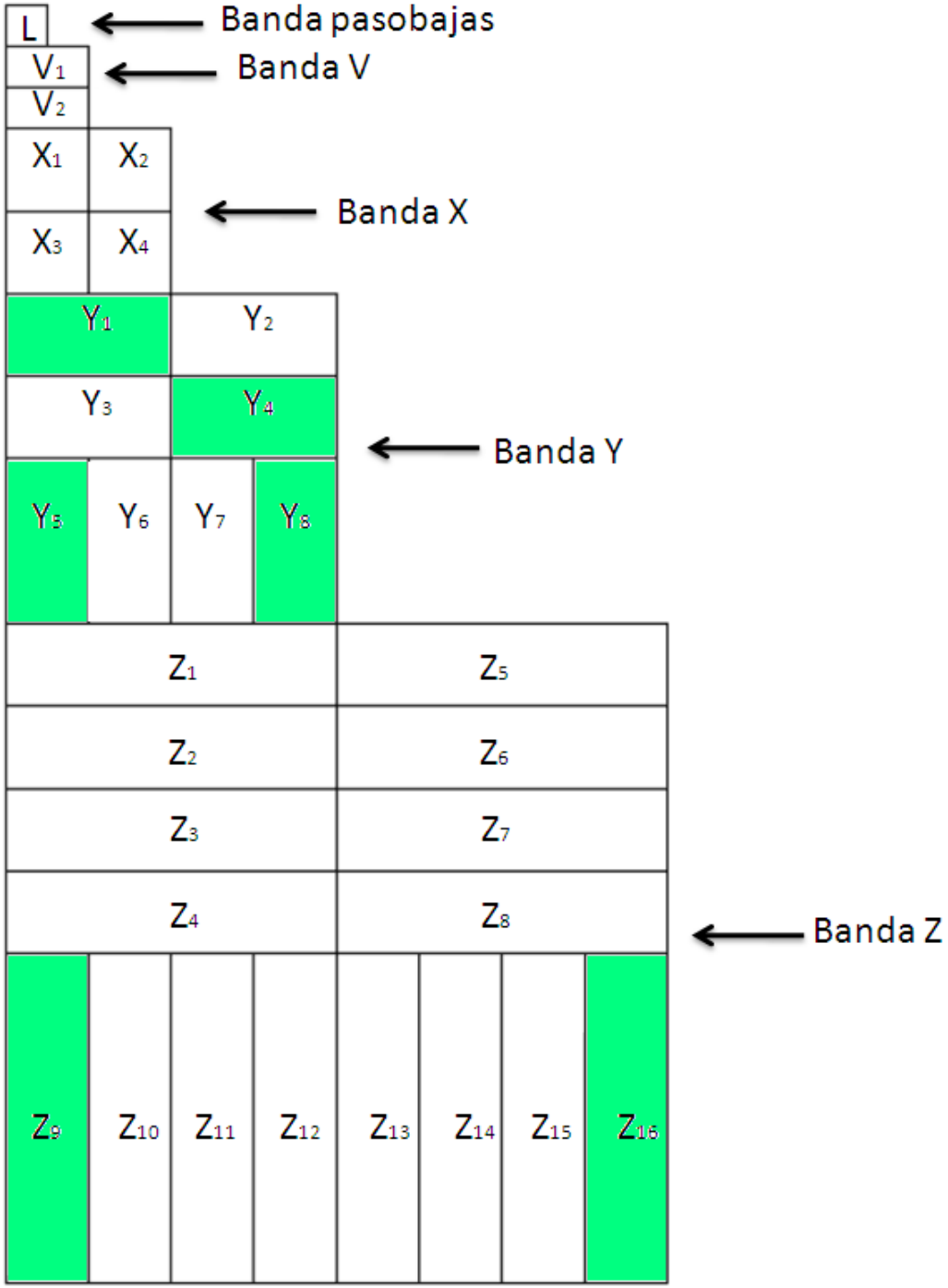
- ***Procedimiento 2***: Subbandas Z3, Z4, Z7 y Z8, del tercer nivel de descomposición.



Bandas contourlet utilizadas en el proc. 2

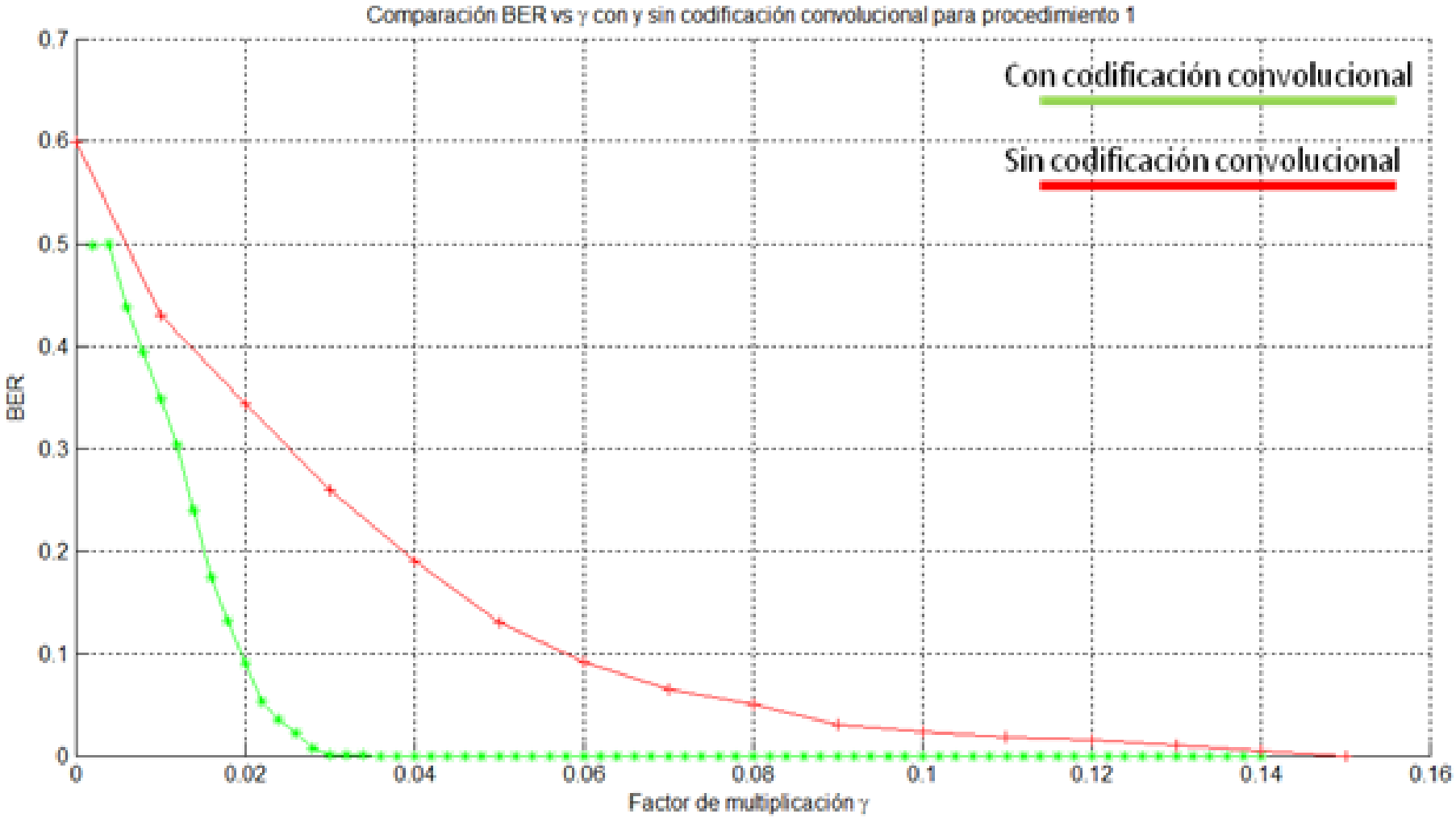
Puebas

- ***Procedimiento 3***: Subbandas Y1, Y4, Y5, Y8, Z9 y Z16, se combinan los niveles de descomposición 2 y 3.



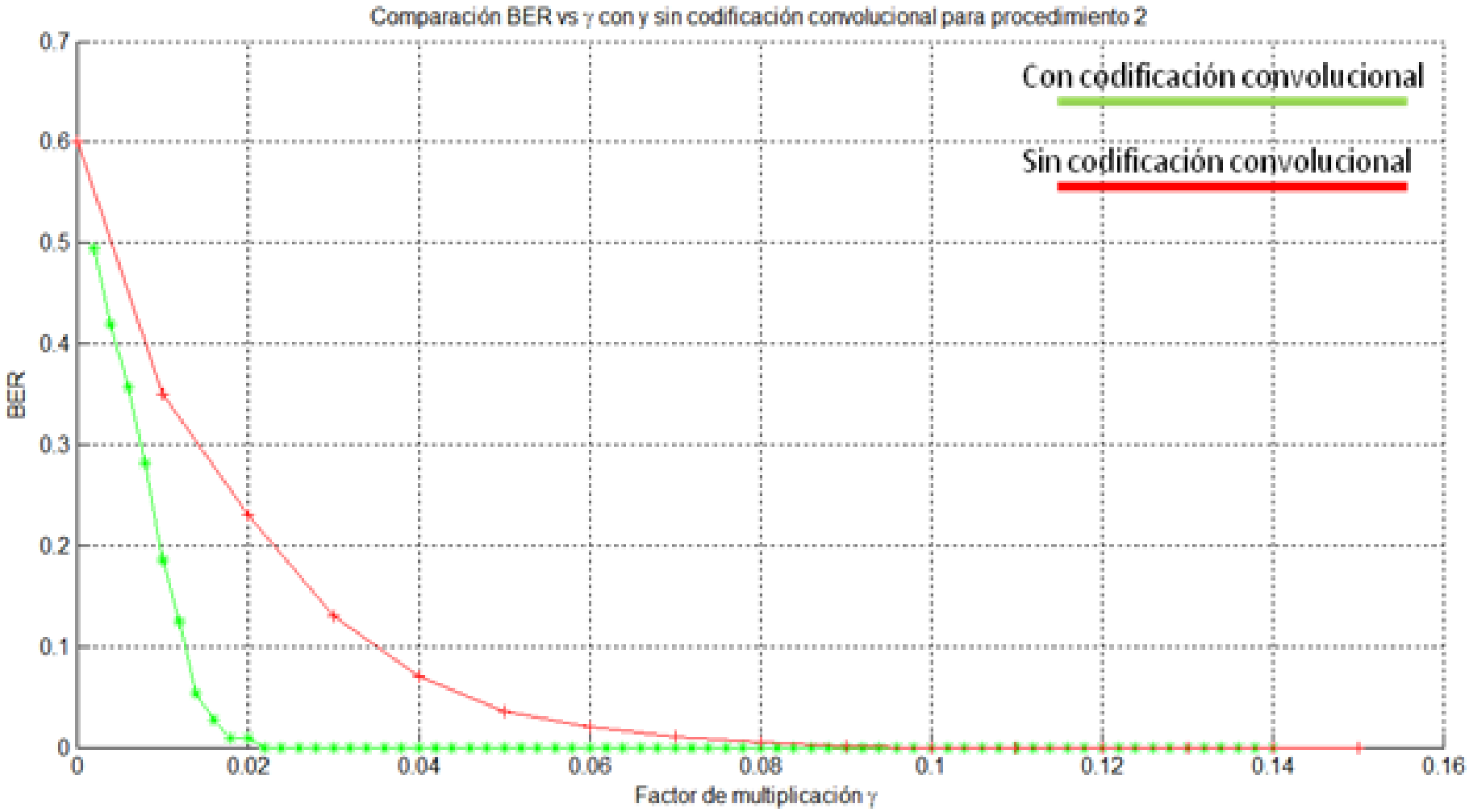
Bandas contourlet utilizadas en el proc. 3

Resultados



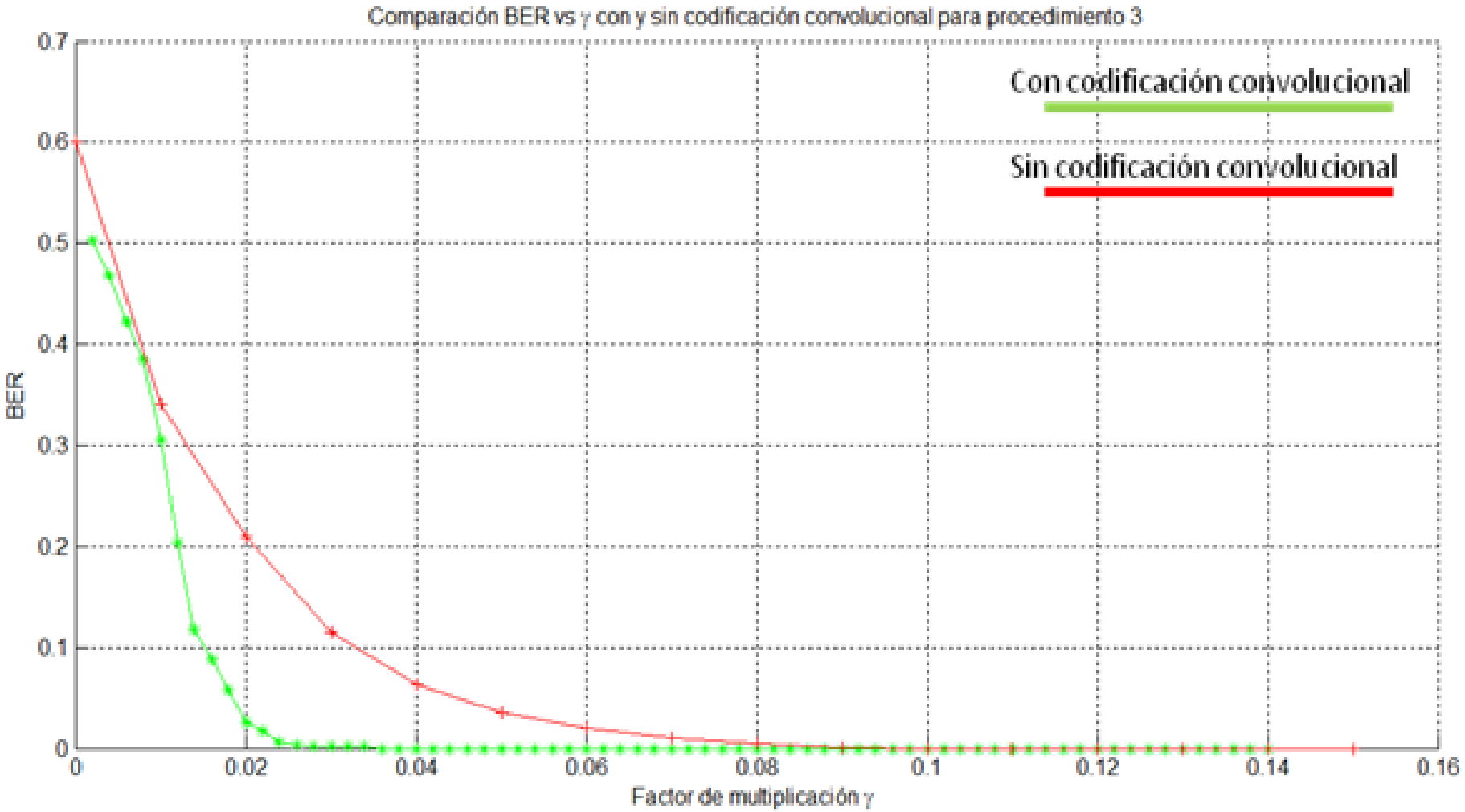
Comparación de la tasa de bits en error en la marca de agua recuperada usando el procedimiento 1. Se incrustó una marca de agua de 2048 bits.

Resultados



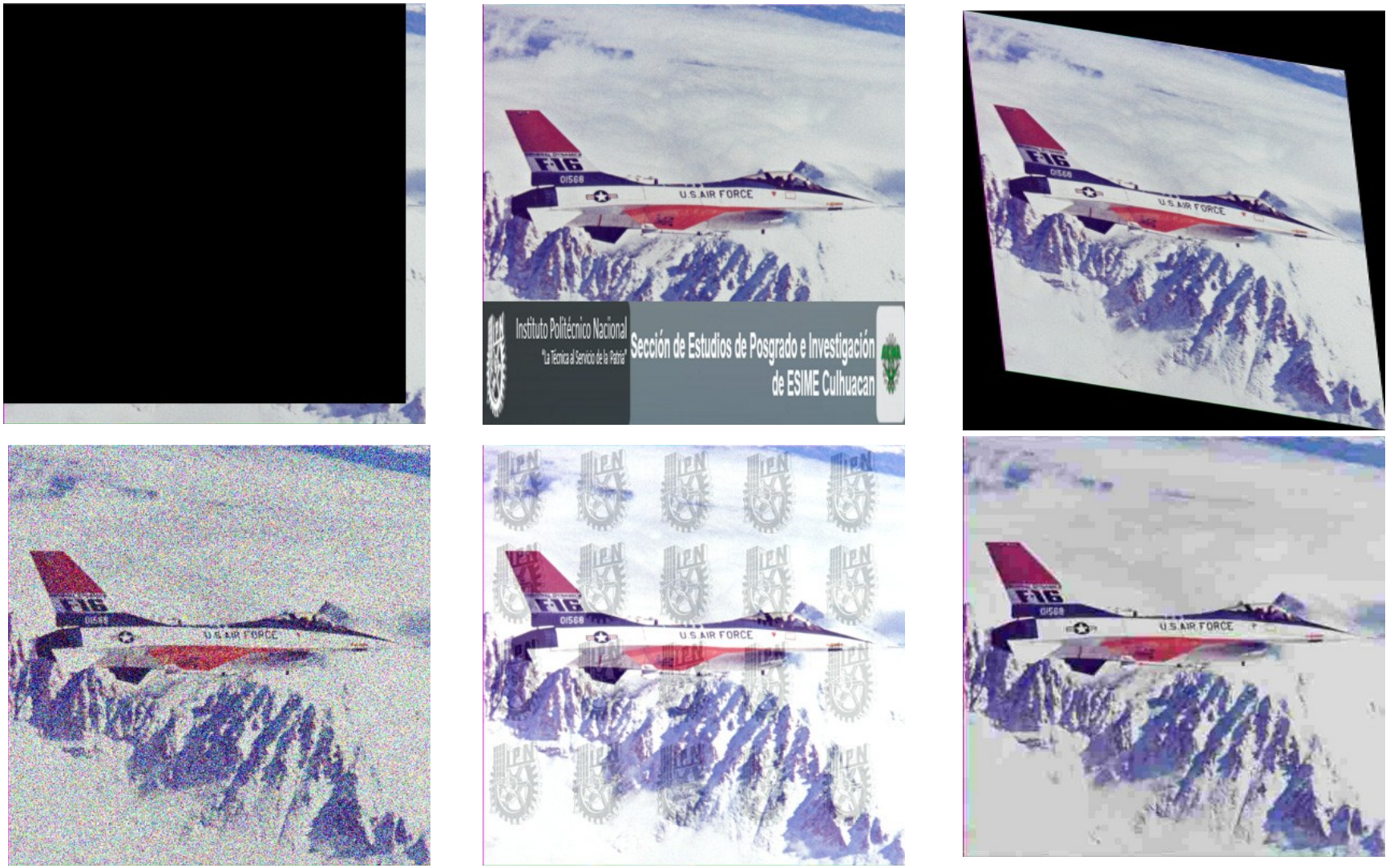
Comparación de la tasa de bits en error en la marca de agua recuperada usando el procedimiento 2. Se incrustó una marca de agua de 2048 bits.

Resultados



Comparación de la tasa de bits en error en la marca de agua recuperada usando el procedimiento 3. Se incrustó una marca de agua de 2048 bits.

[5] Original (a), (c), (e), Watermarked versions (b), (d), (f).



[5] Aggressive geometric and signal processing distortions in Airplane watermarked image. (a) Cropping with 95%. (b) Image replacement. (c) Affine transformation. (d) Gaussian noise (0,0.07). (e) Visual watermark added. (f) JPEG with QF = 10.

Conclusiones

- La codificación de canal y la dispersión de espectro de la marca de agua, aumentó su robustez.
- Utilizando decisión suave en la decodificación se tiene una menor tasa de errores BER en la marca de agua recuperada respecto al uso de decisión dura.
- Para compresión JPEG y filtrado pasobajas el procedimiento más robusto fue el 1.
- Para ruido Gaussiano, ruido "*sal y pimienta*", y recortes los procedimientos más robustos son el 2 y 3.

Conclusiones

- Con el sistema propuesto, se tiene una marca de agua robusta, con un factor de fuerza gamma $\gamma \geq .15$ y usando una marca de agua de 2048 bits, respecto a 2097152 bits (payload $= 9.765625 \times 10^{-4}$).
- El índice SSIM permite medir la calidad perceptual de la imagen marcada.

Referencias:

Solicitud de patente nacional:

- [1] PEREZ-DANIEL, K., GARCIA-UGALDE, F., and SANCHEZ, V., “Método de inserción de marca de agua visible imperceptible como firma digital para la protección de imágenes digitales HDR”, solicitud de patente presentada ante el Instituto Mexicano de la Propiedad Industrial (IMPI), MX/a/2021/010302, folio MX/E/2021/060918, identificador 89657, Ciudad de México 26 de agosto de 2021.

Publicaciones:

- [1] JIMÉNEZ-SALINAS, M., and GARCIA-UGALDE, F., “Improved spread spectrum image watermarking in contourlet domain”, 23rd International Conference Image and Vision Computing New Zealand (ICIVCNZ 2008), 26-28 November 2008, Lincoln University, Christchurch, New Zealand, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4762090,
- [2] GARCIA-UGALDE, F., CEDILLO-HERNÁNDEZ, M., MORALES-DELGADO, E., AND PŠENIČKA, B., “Robust encoded spread spectrum image watermarking in contourlet domain”, 6th International Conference on Signal Processing and Communication Systems, ICSPCS 2012, IEEE Communications Society, 12-14 December 2012, Gold Coast, Australia, DOI: 10.1109/ICSPCS.2012.6508010, 978-1-4673-2393-2/12/$31.00 ©2012 IEEE, pp. 1-5,
- [3] CEDILLO-HERNÁNDEZ, A., CEDILLO-HERNÁNDEZ, M., GARCIA-UGALDE, F., NAKANO-MIYATAKE, M., AND PÉREZ-MEANA, H., “A visible watermarking with automated location technique for copyright protection of portrait images”, Letter of the IEICE Trans. Inf. And Syst., The Institute of Electronics, Information and Communication Engineers, DOI: 10.1587/transinf.2015EDP7412, online ISSN: 1745-1361, Volume and Number: Vol.E99-D, No.6, June 2016, pp. 1541-1552,

- [4] PEREZ-DANIEL, K., GARCIA-UGALDE, F., SANCHEZ, V., “Scene-based Imperceptible-visible Watermarking for HDR Video Content”, 7th IAPR/IEEE International Workshop on Biometrics and Forensics, IWBF-2019, 2-3 May 2019, Cancun. Mexico, INSPEC Accession Number: 18776151, DOI: 10.1109/IWBF.2019.8739184 ©2019 IEEE, pp. 1-6,
- [5] CEDILLO-HERNÁNDEZ, M., CEDILLO-HERNÁNDEZ, A., GARCIA-UGALDE, F., NAKANO-MIYATAKE, M., AND PÉREZ-MEANA, H., “Digital color images ownership authentication via efficient and robust watermarking in a hybrid domain”, Radioengineering, Proceedings of Czech and Slovak Technical Universities and Joint URSI Committee, ISSN 1210-2512, DOI: 10.13164/re.2017.0536, Vol. 26, No. 2, June 2017, pp. 536-551,
- [6] JUAREZ-SANDOVAL, O., GARCIA-UGALDE, F., CEDILLO-HERNANDEZ, M., RAMIREZ-HERNANDEZ, J., and HERNANDEZ-GONZALEZ, L., “Imperceptible-Visible Watermarking to Information Security Tasks in Color Imaging”, in Mathematics 2021, MDPI Journal, Computer Graphics, Image Processing and Artificial Intelligence, EISSN: 2227-7390, DOI: https://doi.org/10.3390/math9192374, Vol. 9, Issue: 19, No. 2374, published on 24 September 2021, pp. 1-23,
- [7] JUAREZ-SANDOVAL, O., REYES-RUIZ, L., GARCIA-UGALDE, F., CEDILLO- HERNANDEZ, M., RAMIREZ-HERNANDEZ, J., and MORELOS-ZARAGOZA, R., “Additional Information Delivery to Image Content via Improved Unseen-Visible Watermarking”, Electronics 2021, MDPI Journal, Special Issue Theory and Applications in Digital Signal Processing, EISSN: 2079-9292, DOI: https://doi.org/10.3390/electronics10182186, Vol. 10, Issue: 18, No. 2186, published on 7 September 2021, pp. 1-23,

¡Muchas Gracias!