UNIVERSIDAD AUTÓNOMA DE SAN LUIS POTOSÍ

FACULTAD DE CIENCIAS

PROCESAMIENTO DE SEÑALES Y SOLUCIÓN DE PROBLEMAS CON LA TRANSFORMADA WAVELET

TESIS

QUE PARA OBTENER EL GRADO DE

DOCTORA EN CIENCIAS APLICADAS

PRESENTA:

CECILIA VARGAS OLMOS

ASESOR:

DR. JOSÉ SALOMÉ MURGUÍA IBARRA

SAN LUIS POTOSÍ, SLP. JULIO DE 2017

A las personas más importantes en mi vida.

De las cuales parto y a las cuales les agradezco su valioso e invaluable esfuerzo y todas sus enseñanzas.

Mis padres:

Ma. Leonor Olmos Flores
Tiburcio C. Vargas Raya.

A las que les tocó acompañarme en la niñez y adolescencia y las que aún hoy, a pesar de la distancia, siguen estando y tengo la certeza de que estarán.

Mis hermanos:

Rebeca, Leonor, Sara y Daniel.

Y a sus respectivos retoños por su alegría y espontaneidad.

Mis sobrinos:

Yael, Dafne y Anaís.

Al que me acompaña, comprende, entiende, apoya y comparte conmigo tanto tristezas como alegrías desde hace 13 años y al cual admiro y amo profundamente.

Mi esposo:

Carlos Francisco Leura González.

Al que llevé en mí, he cuidado, visto crecer y ha iluminado mi vida.

Mi hijo:

Francisco Tonatiuh *(Gracias por el brillo en tus ojos y tu sonrisa al verme).*

A esa nueva vida que ha estado en mí, por toda esa luz que irradia.

Mi bebé:

Yaotl *(Gracias por darme las más hermosas, espontáneas y reconfortantes sonrisas).*

Agradezco:

A mi asesor, el *Dr. José Salomé Murguía Ibarra*, quien fue imprescindible para la realización y buen término de este proyecto y quien con verdadera calidez humana me otorgó toda la confianza, ánimo, tiempo, consejos, y sobretodo paciencia y apoyo en el transcurso de todos estos años de mi formación académica.

Al *Dr. Alexander Vergara* **(**†**)** por su muy valiosa y apreciada contribución y colaboración en la primera parte de este trabajo.

A la *Dra. Marcela Mejía Carlos* y al *Dr. Marco Tulio Ramírez Torres* por su aportación para llevar a cabo la segunda parte de esta disertación.

A mis revisores de tesis, por todas sus observaciones, útiles sugerencias y críticas constructivas que hicieron para que este trabajo se concluyera de mejor manera.

A todas las personas que forman parte del IICO, quienes día a día hacen posible este posgrado, por todo el apoyo concedido.

Al *CONACyT*, por el apoyo económico que me entregó y sin el cual no hubiera iniciado ni concluido el doctorado.

A la *Facultad de Ciencias de la UASLP* por el estímulo económico que me proporcionó durante tres meses para finalizar un artículo más como parte de este documento.

Al FAI 2015, por medio del cual se me otorgó un incentivo económico para concluir un artículo más relacionado con esta tesis.

Resumen

Este trabajo representa uno de los muchos marcos de colaboración entre diversas áreas que actualmente se forman en el ámbito de la investigación académica, en él se procesaron señales provenientes de dos disciplinas científicas muy distintas y las cuales no parecerían tener algo en común. En esta tesis se enlazaron por un lado la quimiometría con el análisis *wavelet* y el reconocimiento de patrones y, por otro lado, se logró observar cómo el análisis *wavelet* junto con el análisis fractal, pueden ser de gran utilidad a la criptografía. Así, después de presentar de manera concisa los fundamentos teóricos de la transformada *wavelet*, se plantearon dos cuestiones muy interesantes que fueron abordadas en dos diferentes capítulos. La primera de ellas tuvo como finalidad conseguir una exitosa discriminación y clasificación de señales obtenidas a partir de dos sensores ópticos de gas, químicamente modificados, expuestos de manera independiente a cada una de las concentraciones elegidas de seis gases diferentes; meta que se alcanzó implementando un novedoso sistema de extracción de características basado en la transformada *wavelet* discreta bidimensional y haciendo uso de un clasificador llamado máquina de soporte vectorial. Posteriormente, en el segundo planteamiento, se propuso realizar un análisis fractal a las matrices de cifrado de un sistema de encriptación así como a un conjunto de imágenes cifradas y, en base a los resultados obtenidos mediante el cálculo del exponente de escala determinado a partir del análisis de fluctuaciones sin tendencia, se logró determinar el comportamiento multifractal de las matrices del esquema de cifrado analizado y además se logró establecer una correspondencia entre la seguridad perceptual de las imágenes cifradas y su exponente de escala.

Índice general

Índice de figuras

Índice de tablas

1

Introducción

En el mundo actual es común encontrar retos y problemas que surgen en un área específica de la ciencia, los cuales, debido a su complejidad o a su interrelación con otras disciplinas suelen ser resueltos de manera conjunta por un equipo interdisciplinario en el que cada miembro participa y colabora aportando su conocimiento, experiencia e ideas a fin de resolver y encontrar la mejor solución a dichas cuestiones. Lo anterior sucede en el día a día del quehacer científico e independientemente de muchos otros retos o problemas que sin lugar a dudas se presentan de forma particular en cada área especializada de las ciencias (sean sociales, naturales, de la ingeniería, etc.) existe uno que es común a todas y en el cual se centran muchos de los esfuerzos de investigación hoy en día, éste es el de procesar acertadamente las señales o los datos que han sido obtenidos en cada aplicación ya que dicho procesamiento puede ser la tarea principal o una etapa crucial de una tarea más compleja. Así pues, con el paso del tiempo el campo de acción del procesamiento de señales se ha ido extendiendo y actualmente, debido al gran desarrollo de la tecnología y a la rapidez de operación de las computadoras, logra aportar información concreta incluso en tiempo real permitiendo delegar acciones como el monitoreo, la interpretación y la decisión a una máquina por lo cual ha contribuido al desarrollo a la vez que forma parte de diversas disciplinas tales como el control, el análisis de imágenes, la minería de datos, la inteligencia artificial y el reconocimiento de patrones, por citar sólo algunas. Para conseguir extraer tal información, en el procesamiento de señales se hace uso de herramientas matemáticas implementadas por medio de algoritmos ya sea en un dispositivo específico o en una computadora, dichas herramientas abarcan desde operaciones básicas hasta otras más sofisticadas que suelen encargarse, por ejemplo, de minimizar o eliminar el ruido, de reducir el volumen de los datos, de extraer la información más representativa, de transformar las señales a otro dominio, etc.

Perteneciendo esta tesis al campo de acción del procesamiento de señales, a lo largo de ella se presentan y utilizan herramientas actuales de análisis como son las máquinas de soporte vectorial y el análisis de fluctuaciones sin tendencia, pero también y principalmente la transformada *wavelet*.

1.1 Justificación

Siendo muy grande así como diverso el número de aplicaciones en las que se involucra el procesamiento de señales y disponiendo de una gran variedad de técnicas y herramientas a implementar según sea el caso, esta tesis resalta la importancia y versatilidad de una de las herramientas matemáticas que ha sido explotada en los últimos treinta años y la cual seguramente seguirá utilizándose por mucho tiempo más, a saber: el análisis *wavelet*. Este análisis, de manera similar al análisis de Fourier, se caracteriza por descomponer una señal en una suma de ciertos coeficientes, llamados coeficientes *wavelet*, algunos de los cuales concentran la información más significativa de la señal, dicha característica ha sido aprovechada, entre otras cosas, para eliminar o reducir el ruido, comprimir datos, detectar bordes, reducir la dimensionalidad de los datos o para detectar la información que posiblemente no había sido captada por otros métodos.

Además de resaltar la importancia y versatilidad del análisis *wavelet*, en esta tesis se muestra cómo dicho análisis puede complementarse junto a técnicas del reconocimiento de patrones o geometría fractal para dar solución a dos problemas muy distintos y los cuales son una pequeña muestra del sinfín de problemas que pueden abordarse por medio de una metodología similar. En el primero de ellos se aborda un problema de análisis y caracterización de señales provenientes de quimiosensores, tema reciente y de creciente interés pues el monitoreo continuo del ambiente así como la identificación exacta de especies químicas, son altamente deseables en muchas aplicaciones, incluyendo el diagnóstico médico, el deterioro de alimentos y el control de calidad en hábitats humanos. Específicamente, el problema planteado aquí consiste en implementar un algoritmo que permita discriminar y clasificar seis diferentes tipos de gases expuestos, de manera aleatoria y a distintas concentraciones, a dos modelos de sensores ópticos presentes independientemente en una misma cámara. Dicha clasificación multivariable se logró resolver gracias a la implementación de un extractor de características basado en la transformada *wavelet* bidimensional y a un clasificador denominado máquina de soporte vectorial. En el segundo problema la transformada *wavelet* es utilizada

como un medio para calcular la tendencia de ciertas señales en lugar de usar una clásica estimación por regresión, esto con el fin de implementar el análisis de fluctuaciones sin tendencia (DFA, por sus siglas en inglés) mediante *wavelets* y calcular el exponente de escala de algunas de las matrices de cifrado de un esquema de encriptación así como el de algunas imágenes cifradas por éste y otros dos sistemas. El interés por develar las propiedades de escala de todo tipo de señales ha estado presente prácticamente desde que existe la geometría fractal y esto ha permitido caracterizarlas. El análisis que se realizó en esta parte de la tesis, permitió determinar que las matrices de cifrado analizadas tienen un comportamiento multifractal y que en el caso de las imágenes cifradas el exponente de escala puede ser utilizado como una medida de la seguridad perceptual de éstas.

1.2 Objetivos

De manera particular se plantea estudiar, implementar y aplicar técnicas de procesamiento de señales, reconocimiento de patrones y geometría fractal para aportar metodologías basadas en la transformada *wavelet* con el fin de lograr la caracterización de información en una y dos dimensiones. Para llevar a cabo lo anterior se pretende:

1. Aplicar la transformada *wavelet* bidimensional a señales provenientes de dos sensores ópticos distintos, los cuales fueron expuestos de manera independiente a cada una de las diversas concentraciones de seis diferentes gases, con el fin de extraer las características más importantes y a partir de éstas lograr una acertada discriminación y así obtener una exitosa clasificación de los mismos.

2. Calcular la tendencia de una señal e implementar el método llamado análisis de fluctuaciones sin tendencia mediante *wavelets*, para estimar y calcular el exponente de escala de la densidad de unos de algunas de las matrices utilizadas en un esquema de cifrado, así como el de algunas imágenes cifradas por éste y otros esquemas.

Mientras el primer objetivo se propone con el fin de solventar uno de los problemas que aún se presentan en los sistemas quimiosensoriales desde que se aplicó y extendió el uso de la instrumentación analítica moderna (allá por los años 80 gracias a la disponibilidad de las computadoras que dieron origen a una nueva

era para la adquisición, procesamiento e interpretación de datos químicos [66]), este es, el de manejar apropiadamente el gran conjunto de datos obtenidos buscando desde disminuir el volumen de los datos para hacer más rápido y viable su análisis hasta conseguir extraer la información más relevante de los mismos; el segundo fue inspirado en algunos estudios realizados con anterioridad donde se buscaba develar propiedades fractales o multifractales de diversas señales [16, 38, 57, 74, 94] y en la referencia ([98]) donde el exponente de Hurst generalizado fue considerado como una medida eficiente de esquemas de encriptación. Más información acerca del estado del arte para cada uno de los objetivos planteados en esta tesis se expone oportunamente en los respectivos capítulos en los que se presenta su desarrollo.

1.3 Organización

En primer lugar, la tesis, en su introducción, ofrece un pequeño pero conciso panorama de lo que se puede encontrar en ella y en seguida, el capítulo 2 presenta los fundamentos teóricos de la transformada *wavelet*, haciendo énfasis en la transformada *wavelet* discreta y el análisis multirresolución; a continuación, el capítulo 3 aborda cómo el hecho de aplicar la transformada *wavelet* discreta bidimensional en la extracción de características de un conjunto de datos obtenidos a partir de sensores ópticos conlleva a la obtención de una exitosa discriminación y clasificación de seis gases distintos; continuando con otro tema, el capítulo 4 muestra el análisis fractal aplicado tanto a matrices utilizadas en un esquema de cifrado, así como el análisis fractal aplicado a un banco de imágenes cifradas y no cifradas con éste y otros esquemas con lo cual se logra establecer la multifractalidad de las matrices de cifrado y una medida de la seguridad perceptual de imágenes cifradas. Finalmente, en el capítulo 5 se pueden observar las conclusiones generales y el planteamiento de futuras líneas de investigación.

2

Fundamentos del análisis wavelet

El origen del análisis *wavelet* se remonta a 1909 cuando Alfred Haar descubrió lo que ahora se considera su precursor, la llamada construcción de Haar, una base ortonormal que consta de funciones escalonadas, aplicable tanto a funciones sobre un intervalo como a funciones en toda la recta real [31]; sin embargo, a principios de los años 80 apareció en la literatura el término *wavelet* y puede decirse que este fue el momento en el que comenzaron a gestarse tanto su fundamento teórico como su novedoso y exitoso desarrollo práctico a los que muchos investigadores desde el punto de vista de diferentes disciplinas han contribuido [12]. Aunque inicialmente el análisis *wavelet* fue presentado como la transformada *wavelet* continua, el interés que despertó hizo que relativamente pronto este tipo de análisis evolucionara y actualmente existe en varias formas estrechamente relacionadas; a saber, la transformada *wavelet* continua (TWC), las series *wavelet* (SW) y la transformada *wavelet* discreta ortonormal, o simplemente, la transformada *wavelet* discreta (TWD); esta última es la que se elige con mayor frecuencia para realizar por medio de ella el análisis (descomposición) y síntesis (reconstrucción) de la señal de interés pues ofrece una gran versatilidad al permitir llevar a cabo los cálculos computacionales a través de su estructura multirresolución de bancos de filtros; dicha forma de aplicar el análisis *wavelet* la convirtó rápidamente en una de las herramientas matemáticas más ampliamente utilizada en el análisis de señales y procesamiento numérico hoy en día. Por medio de ella se han estudiado una gran variedad de temas, entre los cuales están: la compresión de datos, el análisis y compresión de imágenes, el análisis de imágenes biomédicas, la visión por computadora, las comunicaciones digitales, el reconocimiento de patrones, las ecuaciones diferenciales, los sistemas dinámicos y las señales provenientes de sensores. A pesar de existir hace relativamente poco tiempo como una teoría fundamental, las técnicas *wavelet* han demostrado tener un gran potencial así

como su uso ha resultado ser el más pertinente en muchas áreas diferentes de la ciencia e ingeniería, particularmente para esos fenómenos en los cuales los métodos de Fourier clásicos son inefectivos. Teniendo en cuenta lo expuesto anteriormente, las siguientes secciones ofrecen algunos de los aspectos teóricos del análisis *wavelet*, en particular, del proceso de transformar una señal genérica en una base *wavelet* multiescala, es decir, de la transformada *wavelet* discreta, ya que es la herramienta principal en los siguientes capítulos.

2.1 Expansión en series de una señal

Representar una señal o función como una serie de funciones de un conjunto base es una práctica común por las ventajas que suele ofrecer la expansión de la señal o función en una serie de términos, como ejemplos frecuentes están la expansión de una función en una serie de potencias o en una serie de Fourier [21]; generalmente se busca que los coeficientes obtenidos a partir de la expansión proporcionen información más útil de la señal que la que se puede apreciar directamente de ella misma y/o que los valores de algunos de los coeficientes sean muy pequeños o incluso cero para tener una representación dispersa cuya importancia es fundamental en aplicaciones tales como la estimación y detección estadística, la compresión de datos, la reducción de ruido no lineal y en la implementación de algoritmos rápidos [6]. Así pues, la expansión de una señal o función se utiliza frecuentemente con el fin de analizarla, describirla o procesarla convenientemente y, de forma general [90], para cualquier señal o función $f(t)$ de algún espacio S, de dimensión finita o de dimensión infinita, se puede encontrar un conjunto de señales elementales $\{\varphi_k\}_{k\in\mathbb{Z}}$, donde $\mathbb{Z}$ denota el conjunto de los enteros, tal que $f(t)$ sea expresada como la combinación lineal indicada en la ecuación (2.1), la cual es conocida como expansión o serie para $f(t)$.

$$f(t) = \sum_k c_k \varphi_k. \tag{2.1}$$

Se dice que el conjunto $\{\varphi_k\}$ es completo para el espacio S si todas las señales $f \in S$ pueden expandirse como en la expresión (2.1) y es llamado una base para S. En tal caso, también existirá un conjunto dual $\{\tilde{\varphi}_k\}_{k\in\mathbb{Z}}$ tal que los coeficientes c_k de la expansión en la ecuación (2.1) puedan calcularse para señales en tiempo

continuo y para señales en tiempo discreto de la siguiente manera:

$$c_k = \langle f, \varphi_k \rangle = \int f(t)\tilde{\varphi}_k(t)dt, \tag{2.2a}$$

$$c_k = \langle f, \varphi_k \rangle = \sum_n f[n]\tilde{\varphi}_k[n]. \tag{2.2b}$$

Un caso particularmente importante es cuando el conjunto $\{\varphi_k\}$ es ortonormal y completo, ya que entonces se tiene una base ortonormal para S y la base y su dual son iguales, esto es $\varphi_k = \tilde{\varphi}_k$. Entonces:

$$\langle \varphi_i, \varphi_j \rangle = \delta[i-j], \tag{2.3}$$

donde $\delta[m]$ es igual a 1 si $m = 0$ y 0 si no. Cuando el conjunto es completo y los vectores φ_k son linealmente independientes pero no ortonormales se tiene una base biortogonal y la base y su dual satisfacen:

$$\langle \varphi_i, \tilde{\varphi}_j \rangle = \delta[i-j]. \tag{2.4}$$

En caso de que el conjunto sea completo y además redundante (es decir, cuando los φ_k no sean linealmente independientes) no se tiene una base sino una representación sobrecompleta.

Mientras en el análisis de Fourier una señal es representada por medio de funciones sinusoidales (permitiendo una buena aproximación de aquellas señales que sean estacionarias pero sin caracterizarlas localmente en el dominio del tiempo), en el análisis *wavelet* el conjunto base no es único y está formado por funciones llamadas *wavelets*, las cuales son pulsos bien localizados en el dominio del tiempo lo que les permite proporcionar la información espectral correspondiente a posiciones temporales diferentes de una señal. Además, dependiendo del tipo de componente espectral que se desee analizar puede elegirse el ancho de la *wavelet*, así, para analizar componentes de baja frecuencia se utiliza una *wavelet* más ancha que para analizar componentes de altas frecuencias [52].

2.2 Transformada *wavelet*

Como se acaba de mencionar, el conjunto base del análisis *wavelet* no es único y está formado por funciones llamadas *wavelets*, éstas son versiones escaladas y trasladadas (en el dominio del tiempo) de una forma de onda oscilante de longitud finita y rápido decaimiento normalmente referida como *wavelet* madre o *wavelet*

base. Algunos ejemplos de este tipo de funciones se muestran en la figura 2.1; en ella, las *wavelets* presentadas en las subfiguras (a), (b) y (c) tienen una expresión en forma cerrada, mientras la mostrada en la subfigura (d) no puede ser descrita analíticamente y fue obtenida por medio de un procedimiento computacional. La

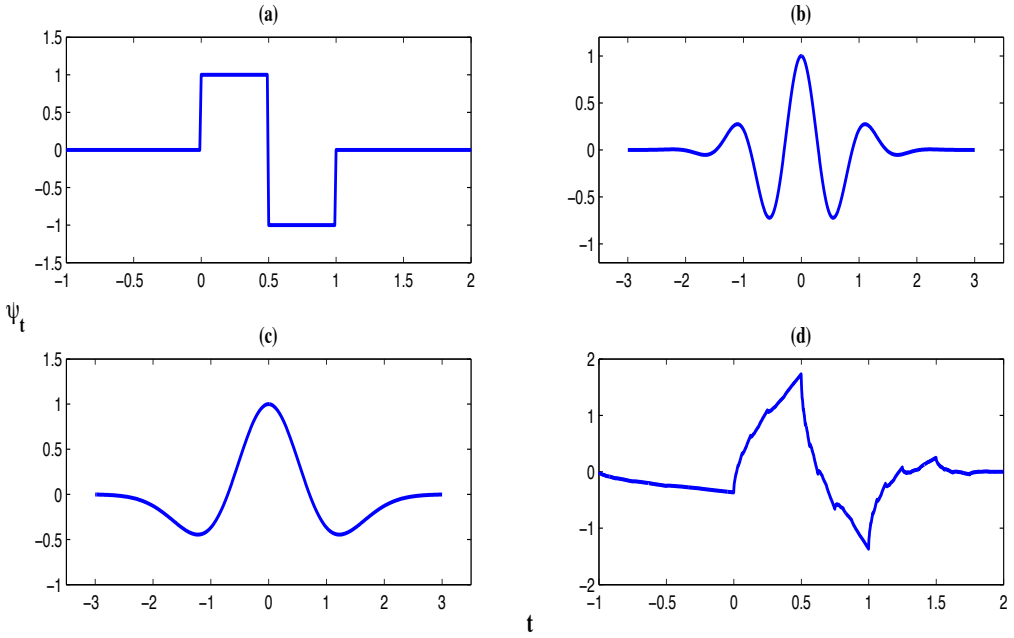


Figura 2.1: Ejemplos de *wavelets* madre: (a) *wavelet* de Haar, (b) *wavelet* de Morlet, (c) *wavelet* Sombrero Mexicano y (d) *wavelet* Daubechies 2.

wavelet madre, denotada en este trabajo por $\psi(t)$, puede ser una función real o compleja y debe satisfacer las siguientes condiciones: tener un promedio cero, ecuación (2.5a), tener energía finita (es decir, pertenecer al conjunto de todas las funciones cuadrado integrables: $\psi(t) \in \mathbf{L}^2(\mathbb{R})$, donde $\mathbb{R}$ denota el conjunto de los números reales), expresión (2.5b), y cumplir con la condición de admisibilidad, expresión (2.5c) donde C_ψ es una constante positiva y $\Psi(\omega)$ es la transformada

de Fourier de $\psi(t)$.

$$\int_{-\infty}^{\infty} \psi(t)dt = 0, \tag{2.5a}$$

$$\int_{-\infty}^{\infty} |\psi(t)|^2 dt < \infty, \tag{2.5b}$$

$$C_\psi = \int_{-\infty}^{\infty} \frac{|\Psi(\omega)|^2}{|\omega|} d\omega < \infty. \tag{2.5c}$$

Las otras *wavelets*, las que son versiones trasladadas y escaladas de la *wavelet* madre, son denotadas por $\psi_{a,b}(t)$ y están definidas por:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{t-b}{a}\right), \tag{2.6}$$

donde a y b son dos números reales arbitrarios que representan los parámetros de escala y traslación respectivamente y el factor $|a|^{-1/2}$ es una constante de normalización considerada para preservar la energía ($\|\psi_{a,b}\| = \|\psi\|$) [2, 22, 53].

Al principio del capítulo se dijo que existen la transformada *wavelet* continua, las series *wavelet* y la transformada *wavelet* discreta; pues bien, la opción a elegir depende del tipo de señal a analizar (continua o discreta) así como también de si los parámetros de escala y traslación se han o no discretizado.

Por definición, la transformada *wavelet* continua de una función $x(t)$ está dada por:

$$TWC(a,b) = \int_{-\infty}^{\infty} x(t)\psi_{a,b}(t)dt, \tag{2.7}$$

donde el mapeo va de una señal continua unidimensional a una función de dos variables reales continuas (a y b), lo cual deriva en una enorme cantidad de cálculos e información redundante, hechos que pueden reducirse si se aplica un muestreo, que comúnmente es diádico para garantizar la eficiencia en la implementación computacional, a los parámetros de escala y traslación, esto es:

$$a = 2^{-m} \qquad \text{y} \qquad b = n2^{-m} \qquad \text{donde} \qquad m, n \in \mathbb{Z}. \tag{2.8}$$

Al sustituir dichos parámetros en la ecuación (2.6) se obtiene la familia de *wavelets* expresada en su forma discreta:

$$\psi_{m,n}(t) = 2^{m/2}\psi(2^m t - n), \tag{2.9}$$

la cual constituye una familia de funciones base ortonormales con m y n denotando los índices de dilatación y traslación respectivamente.

Ahora, sustituyendo la ecuación (2.9) en la fórmula (2.7) se obtiene la expresión (2.10) que permite determinar los coeficientes de la serie *wavelet* para la función continua $x(t)$.

$$d_{m,n} = TWC(2^{-m}, n2^{-m}) = \int_{-\infty}^{\infty} x(t)\psi_{m,n}(t)dt. \tag{2.10}$$

Si el conjunto $\{\psi_{m,n}\}$ forma una base ortonormal, la señal original se recupera a través de los coeficientes discretos $d_{m,n}$ por medio de la expresión:

$$x(t) = \sum_m \sum_n d_{m,n}\psi_{m,n}(t). \tag{2.11}$$

Hasta el momento se ha dado a conocer la expansión en términos de *wavelets* para señales continuas; sin embargo, en la práctica usualmente se manejan señales discretas donde la señal a analizar está definida por una secuencia de números o es una versión muestreada de alguna variable continua, $x_s = x(sT)$, razón por la cual se elige aplicar la transformada *wavelet* discreta, dicha transformada puede implementarse numéricamente y de una forma muy práctica gracias al análisis multirresolución (AMR) y su relación con los bancos de filtros [46]. En el AMR, la TWD es expresada en términos de las versiones trasladadas y dilatadas de la función *wavelet*, $\psi(t)$, así como de su función de escala asociada, $\varphi(t)$, definida por:

$$\varphi_{m,n}(t) = 2^{m/2}\varphi(2^m t - n). \tag{2.12}$$

De acuerdo a lo anterior y considerando que la función *wavelet*, ecuación (2.9), y la función de escala, ecuación (2.12), conforman una base ortonormal, la expansión de $x(t)$ puede escribirse como:

$$x(t) = \sum_n \left(a_{m_0,n}\varphi_{m_0,n}(t) + \sum_{m=m_0}^{M-1} d_{m,n}\psi_{m,n}(t) \right), \tag{2.13}$$

donde los coeficientes de escala o de aproximación, $a_{m,n}$, y los coeficientes *wavelet*, $d_{m,n}$, constituyen la transformada *wavelet* discreta y están definidos de manera respectiva por las expresiones (2.14a) y (2.14b), siendo m el índice de dilatación y n el de traslación.

$$a_{m,n} = \sum_t x(t)\varphi_{m,n}(t), \tag{2.14a}$$

$$d_{m,n} = \sum_t x(t)\psi_{m,n}(t). \tag{2.14b}$$

2.3 Análisis multirresolución

El análisis multirresolución permite calcular los coeficientes $a_{m,n}$ y $d_{m,n}$ de una manera práctica y eficiente, esta técnica fue desarrollada originalmente por Stephane Mallat e Yves Meyer [46] y su fundamento teórico se convirtió en lo que ahora se conoce como la transformada *wavelet* rápida (TWR), un algoritmo que conecta de una manera elegante las *wavelets* y los bancos de filtros. Intuitivamente, en el AMR una señal X se descompone primeramente en una versión de aproximación y en otra de detalles que de manera conjunta generan la señal original; después, a la versión de aproximación se le aplica recursivamente esta descomposición de tal forma que cada aproximación es una versión suavizada de su antecesora; al final, X es representada por una serie de funciones de detalle complementada por una función de aproximación burda.

Matemáticamente, el AMR se define como una secuencia de subespacios cerrados anidados ($\{0\} \subset \ldots \subset V_{-1} \subset V_0 \subset V_1 \subset V_2 \subset \ldots \subset \boldsymbol{L}^2(\mathbb{R})$) los cuales satisfacen las siguientes propiedades:

1. $\bigcup_{m\in Z} V_m$ es denso en $\boldsymbol{L}^2(\mathbb{R})$.
2. $\bigcap_{m\in Z} V_m = 0$.
3. Invariabilidad en escala: para cada $m \in \boldsymbol{L}$, $x(t) \in V_m$ es equivalente a $x(2t) \in V_{m+1}$.
4. Invariabilidad bajo corrimiento: para cada $x(t) \in V_0$ y para cada $n \in Z$, $x(t-n) \in V_0$.
5. Existencia de una base: $\{\varphi(t-n)\}_{n\in Z}$ es una base ortonormal para V_0, donde φ es llamada función de escala.

Para una señal $x(t) \in V_{m+1}$, donde V_{m+1} es algún espacio determinado perteneciente a $\boldsymbol{L}^2(\mathbb{R})$, la función de escala, mediante escalamiento y traslación, genera una base (ecuación (2.12)) para los espacios V_m que permiten representar la información promedio de la señal; mientras que los espacios W_m, cuya base (expresión (2.9)) es generada por la función *wavelet*, proporcionan el resto de la información (los detalles) pues son el complemento ortogonal de los espacios V_m, por consiguiente: $V_{m+1} = V_m \oplus W_m$. Dicha descomposición se ilustra en la figura 2.2 y logra materializarse gracias al punto de vista de bancos de filtros, donde la descomposición de la señal se realiza por medio de filtros en cascada, utilizando

un par de filtros espejo para cada nivel de resolución, en específico, un filtro pasa bajas asociado con la función de escala proporciona las aproximaciones y un filtro pasa altas asociado con la función *wavelet* da los detalles [67]. Como resultado, la representación tiempo-escala de una señal digital es obtenida a través de estas técnicas de filtrado digital aplicadas sucesivamente; este procedimiento ofrece una buena resolución en tiempo a altas frecuencias y una buena resolución en frecuencia a bajas frecuencias, esto sucede porque reduce gradualmente a la mitad el tiempo de resolución de la señal (lo cual significa que solamente la mitad del número de muestras caracteriza iterativamente la señal completa) mientras progresivamente dobla la resolución en frecuencia (ya que la banda de frecuencia de la señal abarca solamente la mitad de la banda de frecuencia previa); de este modo, conforme se avanza en cada nivel de descomposición se reduce efectivamente la frecuencia por la mitad. En la figura 2.3 se ilustra lo explicado anteriormente: en la parte (a) se muestra la manera en que se aplica una descomposición de tres niveles a una señal $x[n]$ por medio de bancos de filtros en cascada, donde los valores de la señal original son considerados como los coeficientes de aproximación del nivel de resolución más alto a partir del cual se comienza el análisis; también se pueden observar los espacios vectoriales a los que pertenecen tanto los coeficientes de detalle como los de escala en cada nivel de resolución consecutivo. En la parte (b) de la misma figura se muestra la división que sufre el ancho de banda de la señal en cada uno de los niveles: en la primera etapa el espectro es dividido en dos partes iguales y en la segunda etapa la mitad de más baja frecuencia es dividida también en dos partes iguales, este procedimiento se repite a su vez en la tercera etapa.

Las expresiones (2.15a) y (2.15b) determinan la TWR calculando los coeficientes de escala y los coeficientes *wavelet* en la escala m a partir de los coeficientes de escala en la próxima escala más fina $m+1$; en tales expresiones, $h[n]$ y $g[n]$ son respectivamente los filtros pasa bajas y pasa altas del banco de filtros de análisis asociado, siendo las señales $a_{m,n}$ y $d_{m,n}$ las respectivas convoluciones de $a_{m+1,n}$ con los filtros $h[n]$ y $g[n]$ seguidos por una reducción de muestreo de factor 2 [46].

$$a_{m,n} = \sum_k h[k-2n]a_{m+1,k}, \tag{2.15a}$$

$$d_{m,n} = \sum_k g[k-2n]a_{m+1,k}. \tag{2.15b}$$

La transformada *wavelet*, como muchas otras transformadas existentes [88], es reversible (es decir, permite ir y venir entre la señal original y las señales procesadas); sin embargo, todavía exhibe alta redundancia en la información,

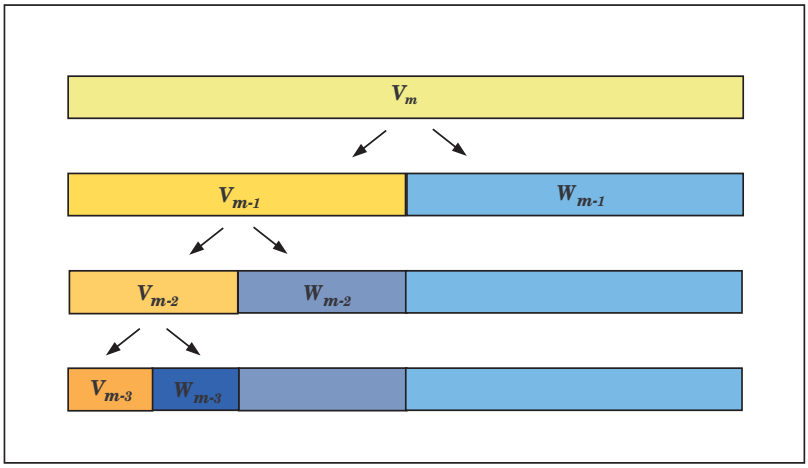


Figura 2.2: Espacios vectoriales del análisis multirresolución: en el AMR una señal $x(t) \in V_m$ se descompone en una versión de promedios (espacios V_{m-1}) y en otra de detalles (espacios W_{m-1}), para calcular el siguiente nivel de resolución a la versión de promedios se le aplica la descomposición y así sucesivamente hasta alcanzar el nivel de resolución deseado.

incrementando significativamente la cantidad de tiempo computacional y recursos requeridos para su procesamiento. No obstante, ya que los filtros utilizados durante la TWR se derivan de funciones base ortonormales, la síntesis o reconstrucción de la señal original puede ser conveniente y fácilmente realizada siguiendo en orden inverso el procedimiento anteriormente mencionado, lo cual reduce significativamente el tiempo de cálculo. En consecuencia, la reconstrucción de los coeficientes de escala originales $a_{m+1,n}$ puede llevarse a cabo a partir de la combinación de los coeficientes de escala y *wavelet* en una escala menor, como se muestra en la ecuación (2.16) que corresponde al banco de filtros de síntesis y representa la inversa de la TWR.

$$a_{m+1,n} = \sum_k \left(h[2k-n]a_{m,k} + g[2k-n]d_{m,k} \right) . \tag{2.16}$$

Esta parte puede ser vista como las convoluciones discretas de la señal sobremuestreada $a_{m,l}$ y los filtros $h[n]$ y $g[n]$. En otras palabras, siguiendo un sobremuestreo de factor 2, las respectivas convoluciones entre la señal sobremuestreada y los filtros $h[n]$ y $g[n]$ son calculadas, lo cual esencialmente

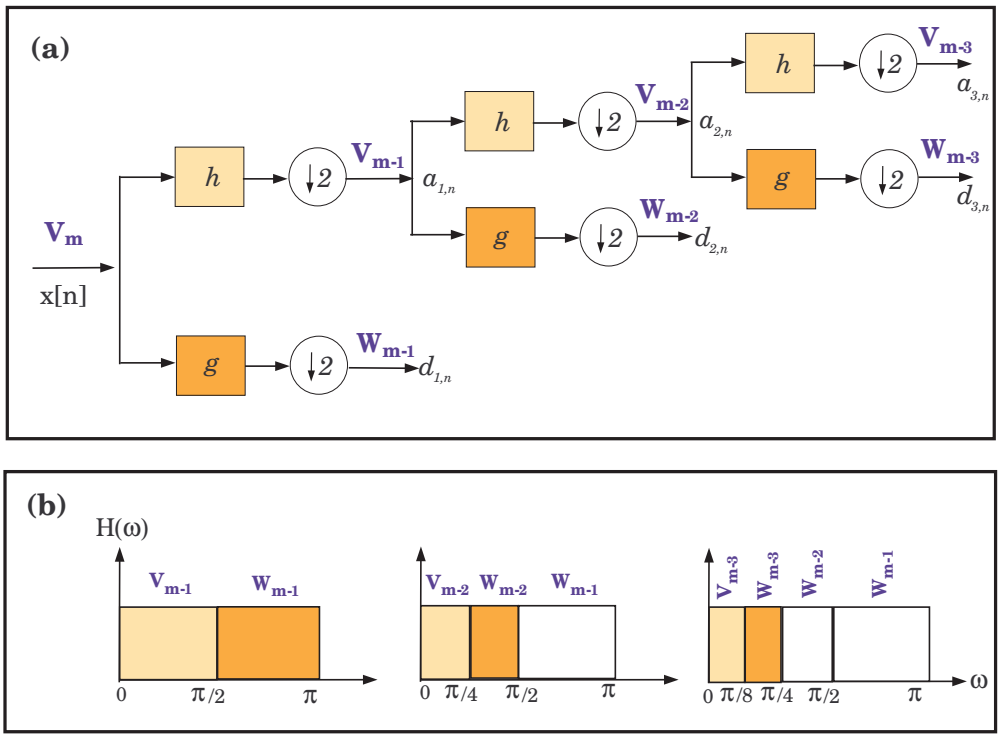


Figura 2.3: (a) Descomposición multirresolución de tres etapas de una señal. Para iniciar el AMR, los valores de la señal a procesar, $x[n]$, se consideran los coeficientes de aproximación en la resolución de más alto orden ($x[n] = a_{0,n} \in V_m$). (b) División del espectro de frecuencia realizada por los filtros $h[n]$ y $g[n]$ en cada una de las etapas presentadas.

significa que el número de niveles depende de la longitud de la señal, por ejemplo, una señal con 2^L valores puede ser descompuesta en $(L+1)$ niveles.

2.4 Transformada *wavelet* bidimensional

La transformada *wavelet* unidimensional puede ser fácilmente extendida a una transformada *wavelet* bidimensional, la cual es ampliamente aplicada a señales de dos dimensiones, por ejemplo a imágenes; esto se realiza tomando todos los productos tensoriales posibles de las funciones base unidimensionales. Estas operaciones crean a su vez cuatro funciones base bidimensionales separables: una

función de escala bidimensional, $\Phi(x,y)$, y tres funciones *wavelet* bidimensionales, $\Psi^H(x,y)$, $\Psi^V(x,y)$ y $\Psi^D(x,y)$, las cuales dan como resultado una señal o imagen de menor resolución que la original, así como información de detalle en las perspectivas horizontal (H), vertical (V) y diagonal (D). Cada una de estas funciones está definida por el producto de una función de escala unidimensional φ y su *wavelet* correspondiente ψ; de esta manera se tiene:

$$\Phi(x,y) = \varphi(x)\varphi(y), \tag{2.17a}$$
$$\Psi^H(x,y) = \psi(x)\varphi(y), \tag{2.17b}$$
$$\Psi^V(x,y) = \varphi(x)\psi(y), \tag{2.17c}$$
$$\Psi^D(x,y) = \psi(x)\psi(y). \tag{2.17d}$$

Ahora, las funciones base de escala y traslación están definidas por:

$$\Phi_{j;m,n}(x,y) = 2^{j/2}\Phi(2^j x - m, 2^j y - n), \tag{2.18a}$$
$$\Psi^d_{j;m,n}(x,y) = 2^{j/2}\Psi^d(2^j x - m, 2^j y - n), \tag{2.18b}$$

donde $j,m,n \in \mathbb{Z}$ y el superíndice d asume los valores H, V y D para identificar las *wavelets* direccionales dadas en las ecuaciones (2.17b)-(2.17d).

Similar a la TWD unidimensional y considerando que las ecuaciones (2.18a)-(2.18b) constituyen una base ortonormal para $L^2(\mathbb{R}^2)$, la expansión de una función $f(x,y)$ de energía finita es entonces definida como

$$\begin{aligned} f(x,y) = \frac{1}{\sqrt{MN}} \sum_m \sum_n \mathbf{a}_{j_0;m,n}\Phi_{j_0;m,n}(x,y) \\ + \frac{1}{\sqrt{MN}} \sum_{d=H,V,D} \sum_{j=j_0} \sum_m \sum_n \mathbf{d}^d_{j;m,n}\Psi^d_{j;m,n}(x,y), \end{aligned} \tag{2.19}$$

donde los coeficientes de escala $\mathbf{a}_{j;m,n}$ y *wavelet* $\mathbf{d}^d_{j;m,n}$ están definidos por

$$\begin{aligned} \mathbf{a}_{j;m,n} &= \int\int f(x,y), \Phi_{j;m,n}(x,y)dxdy, \\ \mathbf{d}^d_{j;m,n} &= \int\int f(x,y), \Psi^d_{j;m,n}(x,y)dxdy. \end{aligned} \tag{2.20}$$

Las expresiones (2.19) y (2.20) representan las ecuaciones de síntesis y análisis de la señal original, y juntas constituyen la transformada *wavelet* discreta bidimensional (TWD-2D). Para calcular la TWD-2D de una manera práctica se sigue también el algoritmo de Mallat [46], donde la descomposición multirresolución

de una función bidimensional o imagen (en este caso denotada por $x[m,n]$) es ahora representada por una sub-imagen de aproximación y una serie de sub-imágenes de detalle, las cuales se obtienen por medio de la transformada *wavelet* rápida bidimensional (TWR-2D) implementada por medio de filtros digitales y submuestreo. Esto está ilustrado en la figura 2.4 donde se muestra un único nivel de descomposición de dicho procedimiento, h y g corresponden a un filtro pasa bajas y a un filtro pasa altas respectivamente, cada uno de ellos seguido por una operación de submuestreo por un factor de 2; como se ve, para obtener un primer nivel de descomposición con la TWR-2D, se realiza el cálculo de la TWR unidimensional aplicada a las columnas seguido por el cálculo de la TWR unidimensional aplicada a las filas (aunque la TWR unidimensional puede aplicarse primeramente a las filas y después a las columnas). En la figura 2.5 está ilustrado el

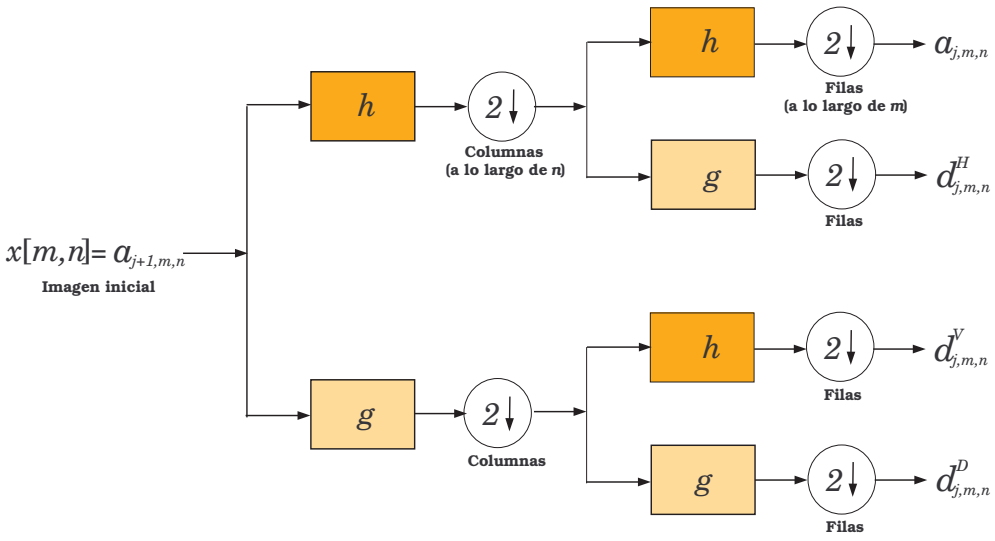


Figura 2.4: TWR-2D: estructura de bancos de filtros utilizados en una etapa de la descomposición multirresolución de una imagen. De manera semejante al caso unidimensional, la señal original bidimensional, $x[m,n]$, se considera que pertenece al primer nivel de resolución $a_{j+1,m,n}$.

resultado de aplicar tres niveles de descomposición *wavelet* a una imagen, $x[m,n]$, de dimensiones $M \times N$; después de que dicha señal bidimensional pasa a través de la estructura de bancos de filtros mostrada en la figura 2.4 se obtienen cuatro

sub-imágenes con $M/2$ filas y $N/2$ columnas; es decir, cada una de las cuatro sub-imágenes tiene un cuarto de los pixeles de la imagen de entrada. La sub-imagen de aproximación es obtenida calculando aproximaciones a lo largo de las filas de la imagen original seguida por los cálculos de las aproximaciones a lo largo de las columnas, esta sub-imagen es una versión promedio de la imagen $x[m, n]$ con un cuarto de resolución y con propiedades estadísticas similares a la señal original. El resto de las sub-imágenes da a conocer características específicas de la imagen original en determinada dirección, esto es, proporciona los coeficientes de detalle horizontal, vertical y diagonal. Para determinar el siguiente nivel de descomposición la misma transformación *wavelet* es aplicada solamente a la sub-imagen de aproximación obteniendo otra vez cuatro sub-imágenes, pero ahora con dimensiones de $M/2^2$ filas y $N/2^2$ columnas; esta iteración se repite hasta llegar al nivel de resolución deseado o hasta el nivel que permitan las dimensiones de la imagen.

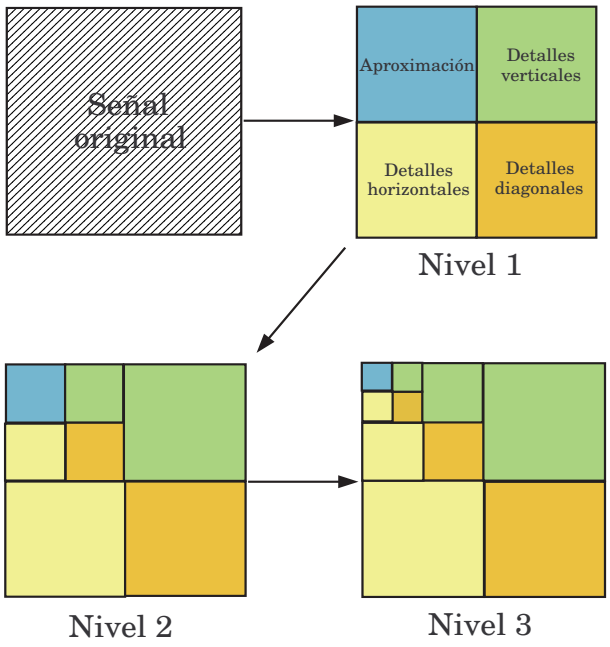


Figura 2.5: Resultado de aplicar tres niveles de la descomposición multirresolución a una imagen por medio de bancos de filtros y submuestreo.

En general, este tipo de descomposición multirresolución para una señal bidimensional da a conocer las diferencias entre las aproximaciones en dos niveles de resolución adyacentes y muestra los detalles en diferentes orientaciones, propiedades que indican que la TWD-2D es muy adecuada para detectar información significativa de la señal bidimensional o imagen original y que han sido valiosamente aprovechadas en tareas del procesamiento de imágenes tales como detección de bordes, reconocimiento y mejora de la imagen.

3

Análisis y caracterización de señales provenientes de quimiosensores

En un mundo inmerso en la tecnología en el que diariamente el ser humano se plantea la posibilidad de que una máquina lleve a cabo las tareas que le resultan monótonas, subjetivas, lentas, difíciles o peligrosas; ninguna de las etapas que de manera conjunta hacen posible el proceso de reconocer, clasificar o automatizar algo puede menospreciarse; sin embargo, dependiendo de los recursos y del grado de desarrollo en el que se encuentre tal o cual etapa suele prestarse mayor o menor interés a otra de ellas. Por ejemplo, y para dar a conocer el contexto en el que se desarrolla este capítulo, en el caso de los sistemas quimiosensoriales —cuyas partes básicas se muestran en la figura 3.1 y cuyo uso ha ido creciendo de tal manera que actualmente suelen aplicarse con el fin de emular los sentidos del olfato y del gusto humano, siendo algunas de sus aplicaciones el control de la calidad de alimentos y bebidas, el diagnóstico médico, el monitoreo de sustancias tóxicas o radiactivas y la detección de situaciones peligrosas o de zonas de difícil acceso para el ser humano— se sabe que hasta la fecha ninguno de ellos exhibe a la vez un diseño confiable, una rápida respuesta, una alta sensibilidad y un bajo consumo de potencia, por lo que el estudio acerca de la optimización de cada una de estas características es un tópico actual de investigación. Aunado a lo anterior también existe el interés por desarrollar e implementar técnicas que ayuden a manejar adecuadamente la enorme cantidad de datos generados por la instrumentación analítica moderna, ya que los grandes avances de la tecnología han permitido que el número de datos obtenidos en este tipo de experimentos vaya en aumento a la vez que impera la necesidad de su correcta interpretación para aprovecharlos más eficientemente; es decir, la aplicación de métodos que ayuden a procesar, diferenciar y extraer la información relevante de los datos obtenidos a fin de conseguir conoci-

miento a partir de ellos es también una etapa crucial, y generalmente la última, de un sistema quimiosensorial, y es justamente una muestra de lo que implica esta parte del sistema a la que se enfoca este capítulo.

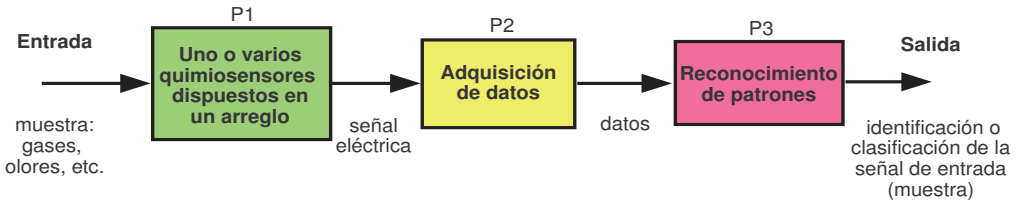


Figura 3.1: Partes básicas de un sistema quimiosensorial. A grandes rasgos: en la primera parte (P1), las señales de entrada interactúan con un quimiosensor cambiando algunas de las propiedades de éste y dichos cambios son convertidos en una señal eléctrica por medio de un transductor; después, en la segunda parte (P2), la señal eléctrica es acondicionada y almacenada apropiadamente; para finalmente, en la tercera parte (P3), al conjunto de datos obtenido se le aplica algún método o técnica de tratamiento de datos con el fin de conseguir un patrón característico de cada una de las señales de entrada, los cuales servirán para entrenar un sistema de clasificación que será utilizado en la discriminación de nuevas señales que serán o no reconocidas dependiendo de si sus respectivos patrones forman o no parte de los que han sido previamente registrados en memoria.

Por más de dos décadas se han desplegado numerosas combinaciones de modalidades en la tecnología de sensado; sin embargo, los dispositivos quimiosensoriales basados ópticamente, en particular, los sensores químicos basados en película multicapa de silicio poroso (pSi) están ganando más importancia que nunca [35, 76, 77], esto se debe a las ventajas que ofrecen las propiedades ópticas y estructurales de este material, gracias a las cuales existen algunas razones por las que han conquistado popularidad, destacando entre ellas principalmente: su promesa de detección a distancia, sus módulos compactos y de baja potencia, su facilidad de integración con tecnología de fibra óptica y la detección segura en entornos altamente combustibles. Aunque los sensores de detección de vapores o gases basados en silicio poroso han sido ampliamente utilizados en aplicaciones relacionadas a la detección de compuestos químicos

o biológicos, tales como vapores orgánicos volátiles [11, 76, 80], explosivos [7], ADN [8, 42] y proteínas [9, 63], sigue estando en discusión si estos sensores son adecuados para escenarios de quimiosensado más complejos donde la tarea de detección implique la identificación de una variedad de niveles de traza de estímulos químicos.

Puesto que a pesar del continuo esfuerzo y conocimiento generado en el campo de la ciencia de los materiales aún no se logra obtener un sensor ideal que perciba y reaccione únicamente a la estructura molecular específica de un determinado analito químico, los sensores comúnmente utilizados son inespecíficos y, no obstante la existencia de algunos más o menos selectivos (pues son ligeramente más sensibles a determinadas familias químicas, por ejemplo a solventes orgánicos, a los ácidos grasos, a gases sulfurosos, etc. [24]), para hacer frente a esta limitada selectividad se han propuesto como posibles soluciones: tanto el uso de arreglos de sensores, donde éstos pueden o no ser idénticos, junto con su respectivo procesamiento de información a través de herramientas de análisis multivariable o multianálisis; así como el empleo de sensores no selectivos y con respuesta cruzada junto con técnicas de procesamiento de la información seguidas por elementos de la inteligencia artificial. Ambas opciones dan paso a los sistemas de sensores inteligentes cuyo uso futuro se vislumbra prometedor [40]. Así pues, entre las estrategias ideadas para afrontar las limitaciones prácticas de los sensores se encuentran: el desarrollo de nuevos métodos para la extracción de información y el desarrollo o aplicación de técnicas de procesamiento de datos y reconocimiento de patrones.

Volviendo al caso particular de los quimiosensores basados ópticamente y queriendo contribuir a encontrar la respuesta a la cuestión de si es viable el uso de un solo sensor de este tipo para detectar información compleja se consideró lo siguiente. Se planeó y montó un experimento que comenzó con la modificación química, por medio de dos procesos distintos, de dos sensores ópticos de detección de gas basados en películas de silicio poroso, y se continuó con la posterior exposición de manera independiente de cada uno de los dos nuevos modelos de sensores (denominados aquí, S1 y S2) a diversas concentraciones de seis diferentes gases, siguiendo con la adquisición de sus correspondientes señales de respuesta para almacenarlas en dos respectivas bases de datos. Finalmente, utilizando métodos de tratamiento de datos se obtiene un vector característico de cada una de las señales de entrada y, a partir de un subconjunto de estos vectores, se entrena un sistema de clasificación con el cual se pueden discriminar nuevas señales. Esta

última parte, referente al reconocimiento de patrones, es el objetivo propuesto en este capítulo y para alcanzarlo se implementó una innovadora metodología basada específicamente en la transformada *wavelet* discreta bidimensional con el fin de extraer las características más significativas de las respuestas de cada uno de los sensores, y después, usar tales características para entrenar un clasificador llamado máquina de soporte vectorial, logrando de esta manera una exitosa clasificación de los gases empleados como conjunto de prueba. Cabe mencionar que este tipo de transformación aplicada unidimensionalmente ya había sido utilizada con anterioridad como extractora de características en otros trabajos relacionados [27, 29, 43, 93, 95]; sin embargo, en este trabajo se aprovecha la configuración bidimensional que exhiben en su respuesta ambos sensores y por ello se aplica el análisis con la TWD-2D.

Antes de seguir vale la pena aclarar que este capítulo se enfoca, como ya se ha hecho notar, en lograr un mejor desempeño de la última parte de un sistema quimiosensorial (de acuerdo a la figura 3.1) y que esto fundamentalmente se llevó a cabo, como también ya se ha mencionado, aplicando la transformada *wavelet* discreta bidimensional a los datos obtenidos mediante las etapas previas; por lo que en esta tesis no se hace énfasis en cada una de las etapas del diseño e implementación del experimento, efectuado en el Instituto de Biocircuitos de la Universidad de California en San Diego y cuya descripción puede consultarse en la referencia ([59]) donde se dan los detalles de la fabricación de los sensores, del sistema de dosificación de vapor de los analitos y del procedimiento de medición y obtención del conjunto de datos. Así pues, esta tesis toma como punto de partida las bases de datos obtenidas mediante el experimento y en la siguiente subsección se describe muy brevemente el procedimiento para conseguirlas y de qué constan.

3.1 Descripción general del experimento y base de datos

En la figura 3.2 se muestra a grandes rasgos el montaje del experimento y se da una breve explicación del mismo. Se puede observar que se trata de un sistema de flujo continuo supervisado de manera computacional mediante el cual se suministra el analito y se registra la respuesta del sensor; dicha respuesta corresponde al espectro de reflectancia normal del sensor óptico en análisis. Con el sistema implementado se realizaron y adquirieron 620 mediciones para cada uno de los sensores, las cuales corresponden a 10 réplicas del experimento completo, donde cada sensor fue expuesto a seis gases distintos dosificados a diversas

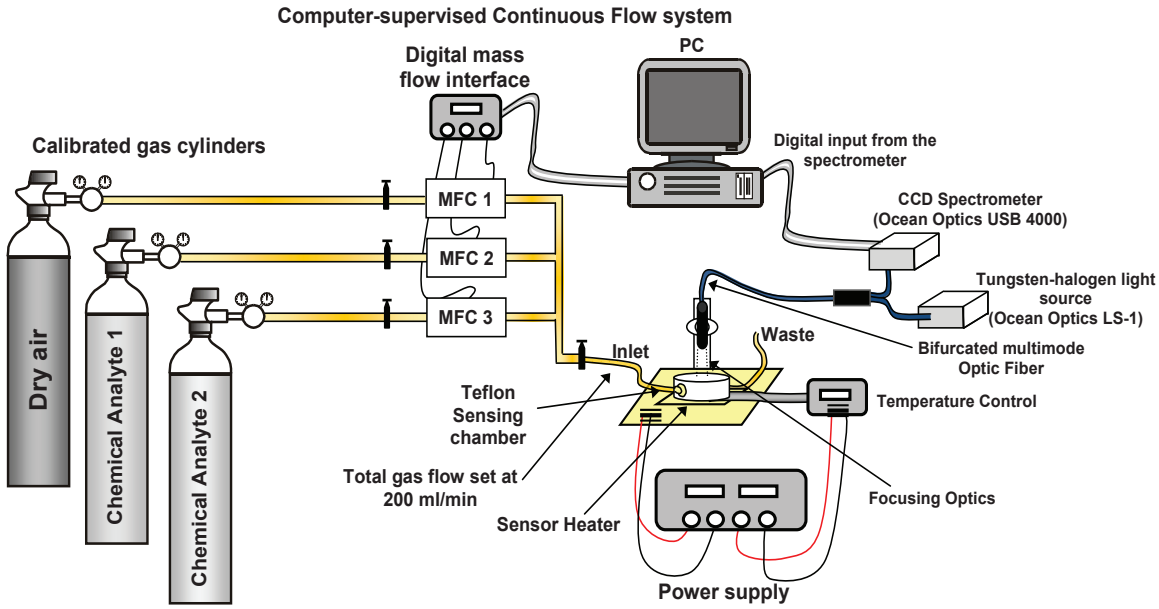


Figura 3.2: Configuración y características de la instalación experimental del sensor. En el esquema pueden apreciarse, de un modo general, las partes interconectadas del sistema de suministro de vapor utilizado para la adquisición de datos. Las respuestas de los sensores se registran en la presencia de los compuestos químicos en forma gaseosa diluidos a diferentes concentraciones en aire seco de calidad médica. El sistema de medición opera en un entorno totalmente computarizado con mínima intervención humana, el cual proporciona versatilidad en la transmisión de los olores de interés (en las concentraciones deseadas) a la cámara de detección (donde se realiza el sensado) con gran precisión, mientras mantiene constante el flujo total, permitiendo de ese modo que sólo la presencia de un odorante se refleje en la respuesta del sensor.

concentraciones, específicamente dichos gases y sus concentraciones se muestran en la tabla 3.1. La elección de estos analitos y de sus respectivas concentraciones no estuvo motivada por alguna restricción de una aplicación particular y el único criterio seguido en su elección fue la no trivialidad empleándose por ello un amplio rango de concentraciones para cada uno de los analitos elegidos. Ahora bien, las lecturas espectrales u observaciones se adquirieron a una razón de 2 Hz durante todo el experimento y cada una de las mediciones comprendió un lapso de tiempo de 13 minutos (como ilustra la figura 3.3), los cuales estuvieron distribuidos de la siguiente forma: 60 segundos fueron para la línea base (fase de estabilización del sensor), 180 segundos para la exposición del sensor a una

Tabla 3.1: Analitos y valores de las concentraciones consideradas.

Gas	Concentración en ppm										
Acetona	50	75	100	125	150	175	200	225	250	275	300
Amoniaco	50	75	100	125	150	175	200	225	250	275	300
Acetaldehido	10	20	30	40	50	60	70	80	90	100	
Benceno	10	20	30	40	50	60	70	80	90	100	
Isopropil	10	20	30	40	50	60	70	80	90	100	
Tolueno	10	20	30	40	50	60	70	80	90	100	

determinada concentración de un gas (donde, tanto el gas como su concentración fueron elegidos aleatoriamente) considerando que en una fracción de este tiempo se incrementó y conservó la nueva temperatura y, el tiempo restante, 9 minutos, para la limpieza y enfriamiento del sensor; en consecuencia, es de notar, que se cuenta con una enorme cantidad de datos pues cada medición consta de 1560 lecturas y cada lectura de 3647 datos.

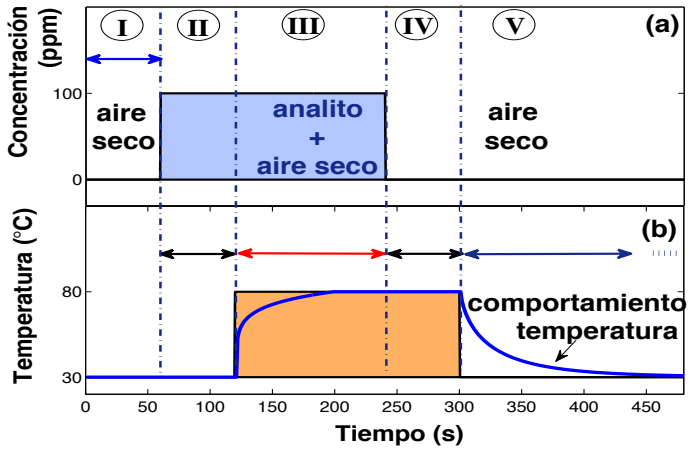


Figura 3.3: Los intervalos de tiempo para (a) la exposición del sensor y (b) el pulso de refrescado térmico. El intervalo de tiempo Ⓘ es para la fase de estabilización, Ⓘⓘ corresponde a la temperatura de la cámara en la fase de concentración, Ⓘⓘⓘ es para la temperatura elevada en la fase de concentración, Ⓘⓥ es para la fase de desorción mediada térmicamente y Ⓥ es para la fase de enfriamiento.

Matemáticamente, cada lectura es representada por un vector de datos $\vec{d} = (d_1, d_2, d_3, \ldots, d_j, \ldots, d_n)$, donde d_j, para $1 \leq j \leq n$, es el valor del j-ésimo descriptor (en este caso, el valor de la reflectancia normal del sensor relacionada a una longitud de onda específica), y cada medición es expresada como una matriz

$$\mathbf{D} = \begin{pmatrix} d_{11} & d_{12} & d_{13} & \cdots & d_{1j} & \cdots & d_{1n} \\ d_{21} & d_{22} & d_{23} & \cdots & d_{2j} & \cdots & d_{2n} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ d_{m1} & d_{m2} & d_{m3} & \cdots & d_{mj} & \cdots & d_{mn} \end{pmatrix}, \tag{3.1}$$

donde m es el instante temporal en el cual se realizó una lectura y n está relacionado a cierta longitud de onda, mientras el valor en la posición d_{ij} corresponde al valor del espectro de reflectancia en ese punto.

Como ejemplos de las lecturas realizadas (datos adquiridos en un sólo instante de tiempo), en la figura 3.4 se exhiben dos de ellas, los cuales corresponden a los espectros de luz reflejada característicos de cada uno de los dos sensores estudiados en presencia de 100 ppm de acetona. Puede observarse que el sensor S1 muestra dos picos de reflectancia, mientras el sensor S2 presenta un sólo pico. Ahora, como ejemplo de una de las mediciones adquiridas, en el lado izquierdo de la figura 3.5 pueden apreciarse los 13 minutos de lecturas grabadas como respuesta del sensor S2 ante la misma concentración e idéntico gas. Esta medición, así como cualquiera de las que forman la base de datos, puede representarse en dos dimensiones como una imagen, tal como se ilustra en el lado derecho de la misma figura, donde cada uno de sus elementos, denominado pixel, tiene asignada una posición correspondiente a un instante de tiempo y a una determinada longitud de onda y cuyo valor en ese punto es la amplitud de la respuesta del sensor.

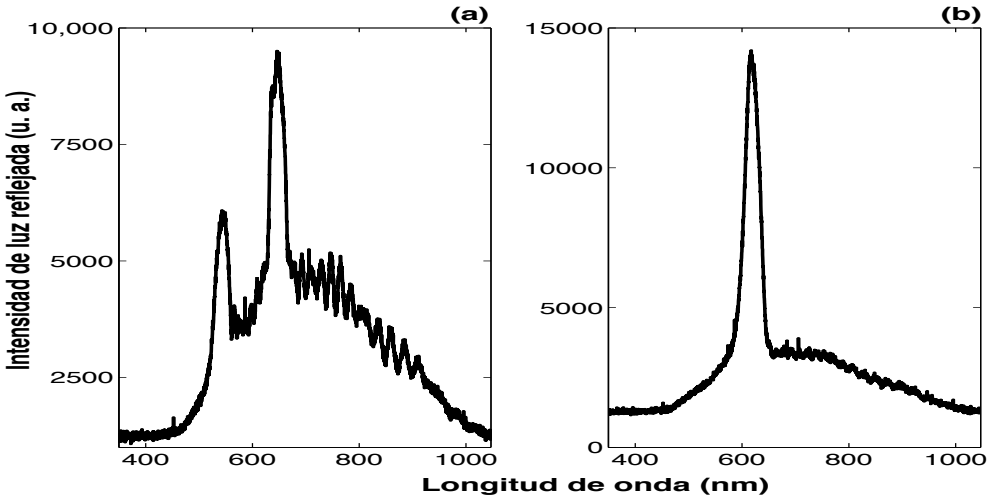
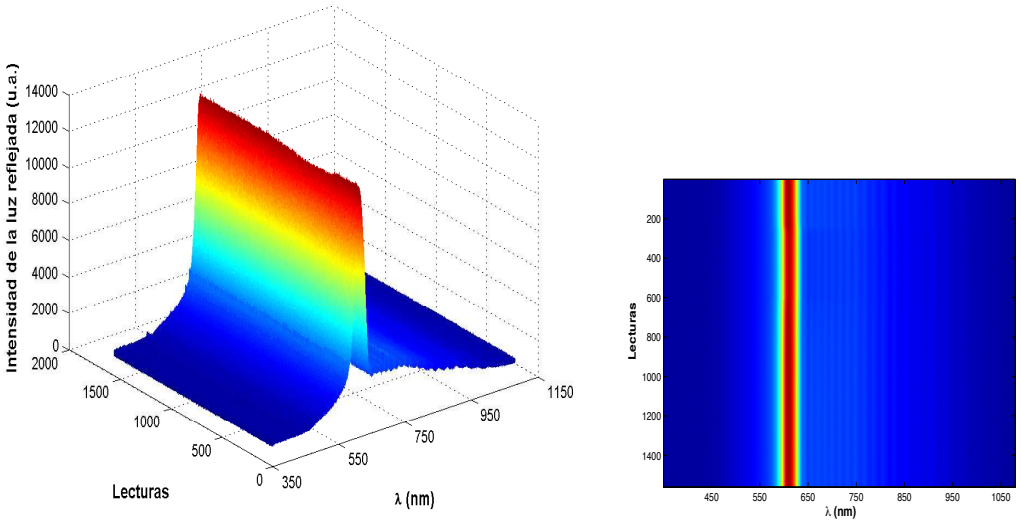


Figura 3.4: Respuesta de los sensores (a) S1 y (b) S2 en un tiempo particular en la presencia de 100 ppm de acetona.



(a) (b)

Figura 3.5: (a) Medición correspondiente al espectro de luz visible reflejado del cristal fotónico (sensor) S2 que se obtuvo como respuesta al ser expuesto ante 100 ppm de acetona. (b) Representación bidimensional de la gráfica anterior.

3.2 Discriminación y clasificación de gases por medio de la transformada *wavelet* bidimensional

Una vez que los datos han sido adquiridos y almacenados se cuenta con un conjunto de señales en una forma más apropiada para analizarlos por computadora. Este es el punto donde comienza la tercera parte del sistema quimiosensorial (de acuerdo a la figura 3.1) llamada reconocimiento de patrones, parte crítica para el sistema, pues a partir de las mediciones experimentales se obtiene información útil y el conocimiento generado a partir de ella comúnmente da paso a una acción, por ejemplo, puede ser usado para automatizar o controlar un proceso e incluso como un primer paso en un sistema inteligente.

En general, el objetivo del reconocimiento de patrones es la clasificación de objetos en un número de categorías o clases y, dependiendo de la aplicación, esos objetos pueden ser imágenes o formas de onda de señales o algún tipo de medidas que necesitan ser clasificadas [83]. Los objetos son descritos por patrones y éstos son proporcionados al sistema de reconocimiento en la forma de un conjunto de datos, en el cual, puede encontrarse confinada la información característica de los patrones observados y entonces hacer posible la clasificación [71].

La estructura de un sistema de reconocimiento de patrones, independientemente del enfoque seguido para diseñarlo, consta de varias unidades funcionales específicas [49], entre las que principalmente destacan: el preprocesamiento, llevado a cabo para simplificar las operaciones subsecuentes sin perder información relevante; la extracción de características, mediante la cual se pretende conseguir la información discriminante y reducir los datos aprovechando ciertas características o propiedades; y la clasificación, donde un clasificador evalúa la muestra presentada y toma una decisión final [15]. Aunque al diseñar un sistema de reconocimiento de patrones la elección de las transformadas, métodos u operaciones aplicados en cada una de las fases del diseño depende mayormente de la naturaleza de las señales de entrada, seleccionar una combinación adecuada dentro del gran número de combinaciones que pueden elegirse para lograr una exitosa clasificación también depende, en cierta medida, de la experiencia e intuición del diseñador.

El reconocimiento de patrones se originó en el campo del procesamiento de señales e imágenes; sin embargo, el primer estudio involucrando este tema en la literatura química se registró en 1969 y a partir de entonces ha sido ampliamente utilizado para dar solución a una variedad de problemas químicos [20].

Regresando al caso particular tratado en este capítulo y recordando que la base de datos con la que se cuenta para cada sensor corresponde a 620 mediciones generadas al replicar 10 veces el experimento, donde para cada réplica se grabó la respuesta de cada sensor ante seis distintos compuestos químicos dosificados en una amplia variedad de concentraciones (como fue presentado en la tabla 3.1), se enfoca y plantea el problema consistente de una tarea de discriminación y clasificación de seis clases, donde cada clase corresponde a un gas en particular independientemente de su concentración. En otras palabras, la tarea de quimiosensado compleja presentada en este capítulo consiste en distinguir seis gases diferentes mediante un algoritmo automatizado de reconocimiento de patrones.

Para diseñar dicho algoritmo, primeramente se investigó la naturaleza de la respuesta característica de los sensores S1 y S2 encontrando que, como en muchas otras tecnologías de sensado [89], los registros de sensores químicos de pSi basados ópticamente para la detección de vapor o gas indican que sus respuestas no son estacionarias, sino que responden a estímulos químicos con características de sensado dinámico que son, en cierta medida, específicas tanto del gas como del sensor y que, de manera similar, bajo condiciones de operación estrictamente controladas, la modalidad de sensado investigada en este trabajo exhibe una configuración bidimensional natural en su respuesta, es decir, en su espectro de luz reflejada debido a los mecanismos de transducción fisicoquímicos del cristal óptico ante la presencia de los analitos elegidos como lo atestigua la figura 3.5, donde se observa que la forma y el perfil de la respuesta son hasta cierto punto específicos para la concentración particular del compuesto químico analizado. Por consiguiente, tomando en cuenta este principio de funcionamiento, se propuso un sistema de reconocimiento de patrones que utiliza una metodología basada en la extracción de características por medio de la TWD-2D como se muestra en la figura 3.6, ya que las propiedades de este tipo de transformada permiten estudiar sistemáticamente la naturaleza bidimensional de los mecanismos de interacción fisicoquímica encontrados en la respuesta del sensor. Así, por medio de esta transformada se logra capturar simultáneamente la evolución temporal y espacial del espectro de reflectancia del cristal óptico gobernando la respuesta del sensor. Por lo que al aplicar la TWD-2D a cada una de las mediciones se esperan obtener las características específicas en el dominio *wavelet* para cada gas y su concentración particular, las cuales discriminarán apropiadamente la información que contiene la base de datos y además serán de dimensiones mucho más pequeñas que las dimensiones del espacio de trabajo inicial.

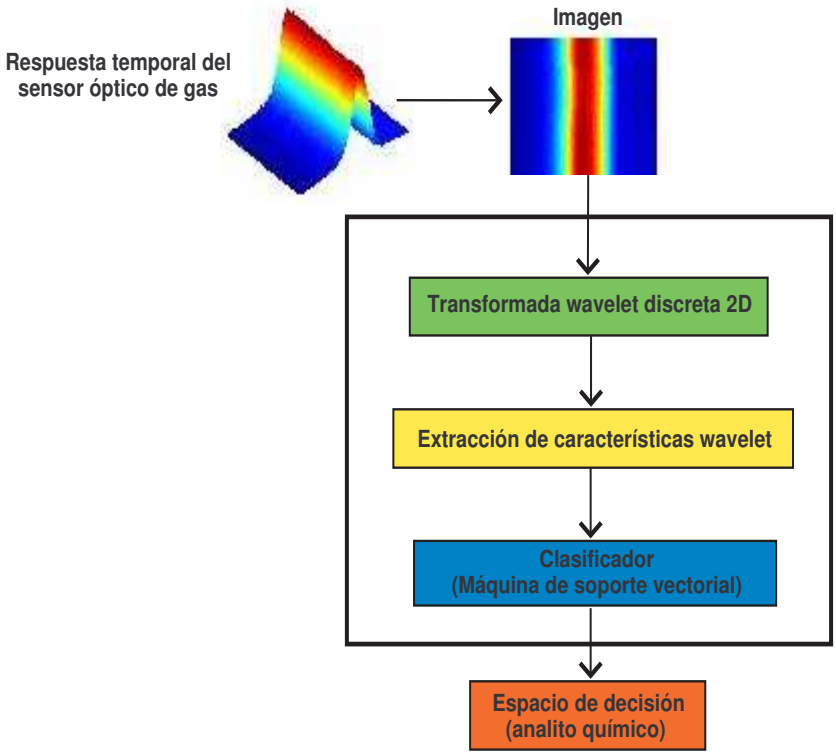


Figura 3.6: Sistema de reconocimiento de patrones propuesto para lograr la discriminación y clasificación de los gases del conjunto de prueba. La transformada *wavelet* discreta bidimensional es aplicada como extractor de características a las respuestas de los sensores químicos estudiados permitiendo encontrar sus características más importantes y mejorando así la capacidad de discriminación del sistema. Finalmente, los coeficientes *wavelet* resultantes se concatenan en forma de un vector que es usado por el clasificador máquina de soporte vectorial para tomar una decisión.

3.2.1 Preprocesamiento

Como ya se ha mencionado, la etapa de preprocesamiento busca simplificar en alguna forma las operaciones subsiguientes, por lo cual la manera en que se realiza generalmente varía dependiendo del tipo de datos y aplicación.

Para el caso planteado en este capítulo, antes de aplicar la transformación propuesta, se consideró llevar a cabo un preprocesamiento con doble finalidad:

primero, buscando reducir el gran volumen de datos que se tiene para cada sensor, conservando únicamente aquellos que aportan información útil e importante y, segundo, buscando reducir el tiempo de cálculo en las etapas siguientes. Por estas razones, y con el propósito de analizar de forma natural los aspectos bidimensionales de la respuesta de los sensores ópticos ante cada uno de los analitos químicos específicos, se inspeccionó y analizó el espectro de reflexión de cada una de las mediciones, determinando que la mayor parte de la concentración de energía de la información espectral para ambos sensores está contenida en la ventana de longitud de onda que abarca $\lambda = 400$ nm a $\lambda = 800$ nm (como puede apreciarse en la figura 3.4) y durante el tiempo de ocurrencia de la inyección del gas y el cambio de temperatura de trabajo, esto es, durante el intervalo de tiempo $t = 61$ s a $t = 300$ s (de acuerdo a la figura 3.3), decidiendo trabajar con los datos comprendidos entre estos intervalos. Entonces, considerando lo expuesto anteriormente, el nuevo conjunto de datos preprocesados para cada sensor cuenta con 620 mediciones, donde ahora cada una de ellas se representa bidimensionalmente por una imagen de 512×1024 pixeles; como ejemplo, en la parte superior de la figura 3.7 pueden verse las imágenes obtenidas después de seleccionar la ventana que contiene los datos más significativos de la respuesta del sensor óptico tipo 2 en presencia de 100 ppm de acetona (subfigura (a)) y ante 100 ppm de benceno (subfigura (b)).

3.2.2 Extracción de características por medio de la TWD-2D

Después del preprocesamiento se realizó la extracción de características aplicando la transformada *wavelet* bidimensional (descrita en la sección 2.4) a cada una de las mediciones para determinar sus correspondientes coeficientes *wavelet*. Dicha transformación se llevó a cabo hasta el sexto nivel de descomposición y utilizando tres tipos diferentes de funciones *wavelet* pertenecientes a la familia de Daubechies, a saber, la db1, db2 y db4. Los tipos de funciones *wavelet* fueron seleccionadas intencionadamente debido a sus propiedades deseables de ortogonalidad, calidad de aproximación y estabilidad numérica [10, 29, 43, 46], así como a su eficiencia de memoria y reversibilidad, haciendo de este modo su implementación computacional más eficiente y conceptualmente menos compleja que en otras bases *wavelet*. El número de coeficientes resultantes está de acuerdo al nivel de descomposición alcanzado al transformar la respuesta original del sensor y puede ser relacionado nuevamente con dicha respuesta en el sentido de que los coeficientes *wavelet*

contendrán la misma información original pero en un contexto dimensional mucho más pequeño. Por ejemplo, si a una de las mediciones, vista como una imagen de 512×1024 pixeles, se le aplica la TWD-2D hasta el sexto nivel de descomposición, tomando como base la *wavelet* db1, se obtiene una imagen en el dominio *wavelet* representada por 16 x 32 coeficientes; dicha imagen contiene cuatro sub-imágenes, una de aproximación y tres de detalles (como fue explicado en la sección 2.4), donde cada una de las cuales está formada por una matriz de 8×16 coeficientes.

En la parte central de la figura 3.7 se exhiben dos ejemplos del sexto nivel de descomposición *wavelet* obtenidos al aplicar la db4 como función base de la descomposición *wavelet* bidimensional a las respectivas imágenes de la parte superior de la misma figura. Además, en la parte inferior de la figura en mención se ven los histogramas para cada una de las sub-imágenes de aproximación y detalle correspondientes a las subfiguras (c) y (d). Las diferencias que surgen en estas gráficas sugieren la posibilidad de ser explotadas para discriminar entre las diferentes especies evaluadas. Estas diferencias llegan a ser aún más notables cuando se ilustran puramente como una comparación directa entre los coeficientes *wavelet* correspondientes a las tres sub-imágenes de detalle *wavelet* como se demuestra en la figura 3.8. En dicha figura se comparan específicamente las tres sub-imágenes de detalle *wavelet* correspondientes al sensor óptico tipo 2 en respuesta a 100 ppm de acetona (sub-imágenes en la fila superior) y a 100 ppm de benceno (sub-imágenes en la fila central); las columnas de la izquierda, central y derecha, de cada una de las filas mencionadas, corresponden respectivamente a las sub-imágenes de detalle en las direcciones horizontal, vertical y diagonal. De manera adicional, en la fila inferior de la misma figura se ilustra la diferencia absoluta entre estos coeficientes *wavelet*, en los cuales la diferencia entre las señales es incluso más notable y perceptible, particularmente, en ciertas etapas del espectro (por ejemplo, en el intervalo de muestras [50, 100]), lo cual, aparte de sugerir su utilidad discriminatoria, también hace pensar en una alta capacidad para propósitos de reducción de dimensionalidad, es decir, sirve como herramienta de selección de características.

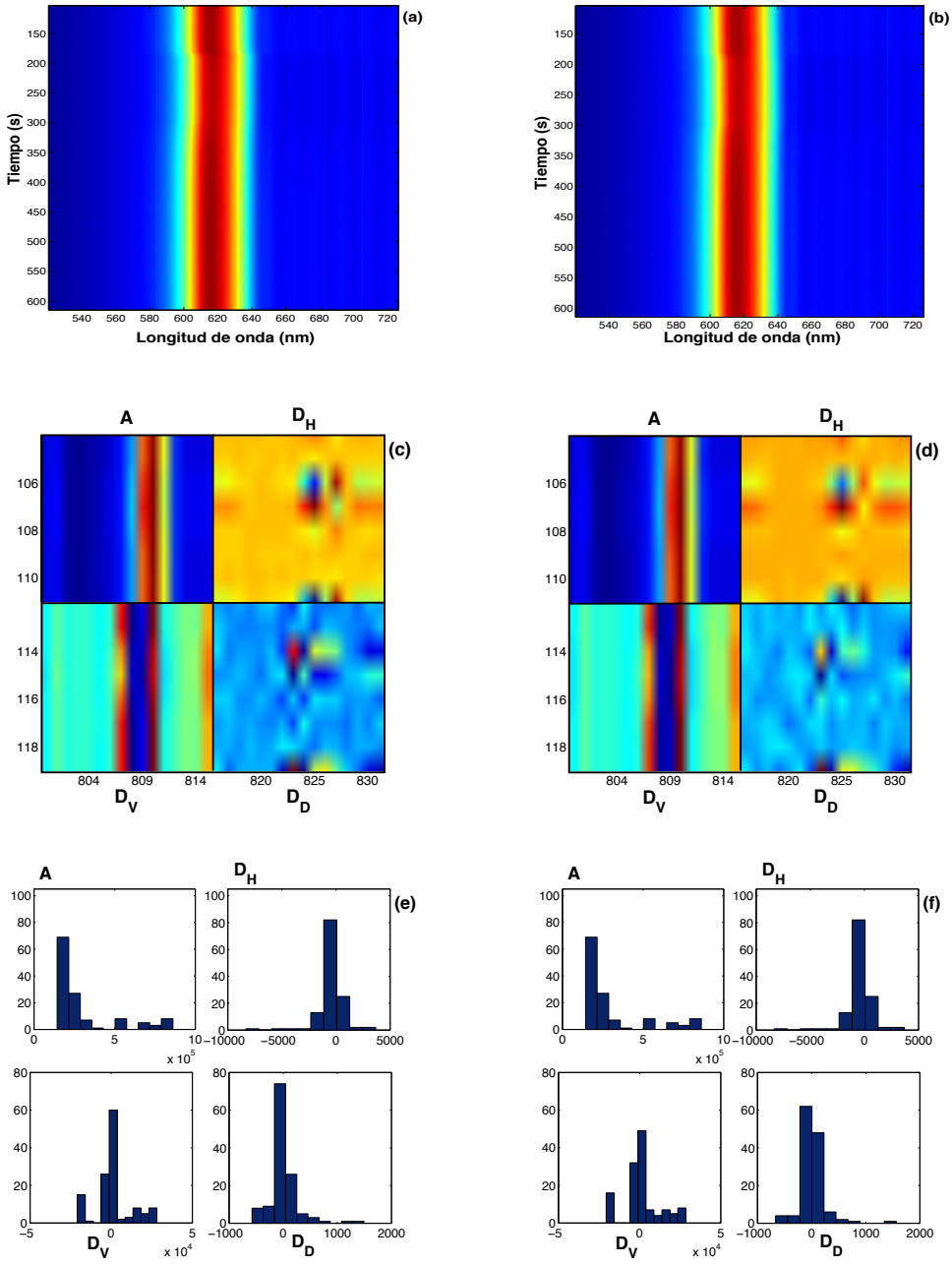


Figura 3.7: Subfiguras (a) y (b): representación bidimensional del espectro de luz visible reflejado del cristal fotónico (sensor 2), obtenido a través de una ventana óptica en la celda de flujo exhibiendo un pico espectral en la presencia de 100 ppm de acetona y benceno, respectivamente. Subfiguras (c) y (d): sexto nivel de descomposición *wavelet* bidimensional de las imágenes anteriores utilizando la *wavelet* db4 como función base. Subfiguras (e) y (f): histogramas de las sub-imágenes de aproximación y detalle *wavelet* precedentes.

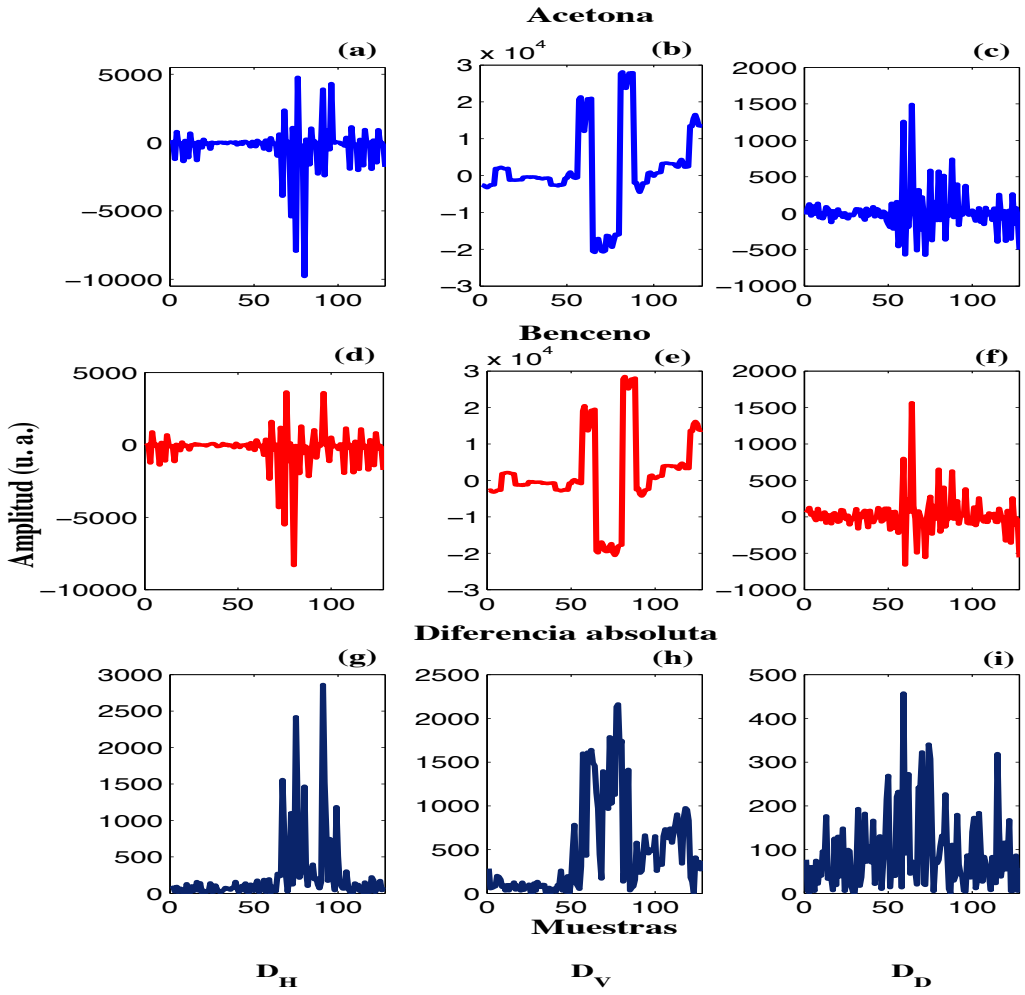


Figura 3.8: Fila superior: coeficientes de detalle (a) horizontal, (b) vertical y (c) diagonal correspondientes al sexto nivel de descomposición *wavelet* de la respuesta del sensor 2 ante la presencia de 100 ppm de acetona. Fila de en medio: los respectivos coeficientes *wavelet* para la respuesta del mismo sensor ante la presencia de 100 ppm de benceno. En ambas respuestas la descomposición *wavelet* se efectuó con la db4. Fila inferior: diferencia absoluta entre los coeficientes de detalle *wavelet* en las direcciones respectivas.

3.2.3 Exploración de datos, análisis de componentes principales

En seguida de que los coeficientes *wavelet* correspondientes a las respuestas de los sensores ópticos de vapor fueron estimados, surgió la tarea de evaluar

juiciosamente si estos coeficientes de la respuesta transformada ayudarían a discriminar correctamente los analitos químicos en cuestión. Por esta razón se aprovechó una técnica exploratoria de análisis de datos llamada análisis de componentes principales (ACP), cuyos orígenes se remontan a 1901, pero que como técnica data de 1933 y es debida a Hotelling, en la cual las variables originales, generalmente correlacionadas, son transformadas en nuevas variables no correlacionadas, llamadas componentes principales, facilitando de esta manera la interpretación de los datos; además de que permite representar óptimamente las observaciones de un espacio general p-dimensional en un espacio de dimensión más pequeña [69].

En el análisis de componentes principales se busca maximizar la varianza de una combinación lineal de las variables originales, y ninguna de éstas se designa como dependiente ni tampoco se asume ninguna agrupación de observaciones. El primer componente principal es la combinación lineal con máxima varianza, de tal forma que las observaciones están lo más separadas posible; el segundo componente principal es la combinación lineal con máxima varianza en una dirección ortogonal al primer componente principal y así sucesivamente [75]. Por tanto, para representar el conjunto original de datos suelen elegirse únicamente aquellos componentes principales que retengan el mayor porcentaje significativo de la varianza total.

Las nuevas variables no correlacionadas, $\mathbf{z}_i$, son obtenidas por medio de la transformación lineal $\mathbf{z}_i = \mathbf{A}\mathbf{x}_i$, donde $\mathbf{x}_i$ es un vector conformado por p variables (las características observadas del conjunto a analizar) y $\mathbf{A}$ es la matriz de transformación. Para conseguir dicha transformación se llevan a cabo los pasos siguientes [71, 75, 84]:

1. Considerar una matriz de datos, $\mathbf{X}$, con p variables observadas sobre n elementos:

$$\mathbf{X} = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1p} \\ x_{21} & x_{22} & \cdots & x_{2p} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{np} \end{pmatrix} = \begin{pmatrix} \mathbf{x}_1' \\ \mathbf{x}_2' \\ \vdots \\ \mathbf{x}_n' \end{pmatrix}, \tag{3.2}$$

con

$$\mathbf{x}_i = \begin{pmatrix} x_{i1} \\ x_{i2} \\ \vdots \\ x_{ip} \end{pmatrix}, \tag{3.3}$$

se estima la matriz de covarianza

$$\mathbf{S} = \frac{1}{n-1}\sum_{i=1}^{n}(\mathbf{x}_i - \bar{\mathbf{x}})(\mathbf{x}_i - \bar{\mathbf{x}})', \tag{3.4}$$

donde

$$\bar{\mathbf{x}} = \frac{1}{n}\sum_{i=1}^{n}\mathbf{x}_i = \begin{pmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \vdots \\ \bar{x}_p \end{pmatrix}, \tag{3.5}$$

siendo $\bar{x}_1$ la media correspondiente a la primer variable, $\bar{x}_2$ la media correspondiente a la segunda y así sucesivamente.

2. Realizar la eigendescomposición de $\mathbf{S}$ y calcular los p eigenvalores y eigenvectores, $\lambda_i, \mathbf{a}_i \in \mathbb{R}^p, i = 1, 2, \ldots, p$.

3. Acomodar los eigenvalores en orden descendente, $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_p$.

4. Elegir los k eigenvalores más grandes. Usualmente k se escoge tal que la diferencia entre λ_{k-1} y λ_k sea considerable.

5. Calcular los respectivos eigenvectores, $\mathbf{a}_l, l = 1, 2, \ldots, k$ y determinar los componentes

$$\begin{aligned} z_{1i} &= \mathbf{a}_1'\mathbf{x}_i \\ z_{2i} &= \mathbf{a}_2'\mathbf{x}_i \\ &\vdots \\ z_{ki} &= \mathbf{a}_k'\mathbf{x}_i \end{aligned} \tag{3.6}$$

para $i = 1, 2, \ldots, p$. La ecuación (3.6) puede ser reescrita en forma vectorial como

$$\mathbf{z}_i = \mathbf{A}_k\mathbf{x}_i, \tag{3.7}$$

donde

$$\mathbf{z}_i = \begin{pmatrix} z_{1i} \\ z_{2i} \\ \vdots \\ z_{ki} \end{pmatrix} \quad \text{y} \quad \mathbf{A}_k = \begin{pmatrix} \mathbf{a}_1' \\ \mathbf{a}_2' \\ \vdots \\ \mathbf{a}_k' \end{pmatrix}, \tag{3.8}$$

por lo que cada vector $\mathbf{x}_i$, p-dimensional en el espacio original, es transformado a un vector $\mathbf{z}_i$, k-dimensional.

La varianza explicada para el j-ésimo componente principal es simplemente la razón entre el j-ésimo eigenvalor y la varianza total [20]:

$$\%\text{Var}_j = \frac{\lambda_j}{\sum_{i=1}^{p} \lambda_i} \times 100\,\%. \tag{3.9}$$

Ya que el análisis de componentes principales hace posible, mediante una inspección gráfica, visualizar la separabilidad existente entre diferentes clases, pues por medio de un diagrama de dispersión permite identificar si existe o no correlación entre los vectores característicos correspondientes a las mismas y a partir de esto considerar su posible discriminación; algunas aplicaciones culminan con este tipo de análisis y podría ser el caso cuando se busca identificar datos atípicos, o se quiere visualizar la estructura de datos o bien, cuando sirve como algoritmo de clasificación no supervisado; sin embargo, en algunas otras, los componentes principales se utilizan como entrada a otro tipo de análisis, en los cuales, por ejemplo, se busca primero reducir las dimensiones de datos multivariados. Una explicación mucho más detallada y abundante en ejemplos respecto al análisis de componentes principales puede encontrarse en [69, 73, 75].

Retomando la tarea de evaluar si los coeficientes *wavelet* que fueron obtenidos al aplicar la transformada *wavelet* bidimensional hasta el sexto nivel de descomposición permitirían discriminar apropiadamente los gases del conjunto de prueba, se concatenaron por separado los coeficientes de detalle horizontal, vertical y diagonal resultantes para cada gas y concentración particular, considerando de manera independiente a cada uno de los sensores. Puesto que al concatenar los coeficientes se forma un vector fila, $\mathbf{x}_i$, como resultado general se obtuvo una matriz de 620 elementos (mediciones) por 128 características observadas (los coeficientes correspondientes a alguno de los tres tipos de detalle *wavelet* y a una de las tres *wavelets* utilizadas como función base al realizar la transformación). Todos estos vectores fueron parte del modelo de discriminación que más adelante se interconectó al sistema de reconocimiento de patrones.

La figura 3.9 ilustra las gráficas de dispersión del análisis de componentes principales aplicado tanto a las características *wavelet* generadas para evaluar cualitativamente su capacidad de representar los seis gases del conjunto de prueba, así como a las características generadas desde el criterio de extracción de características, ampliamente utilizado en investigación de sensores basados en pSi, que establece la estrategia de monitorear el pico de longitud de onda presentado en la respuesta del sensor [36].

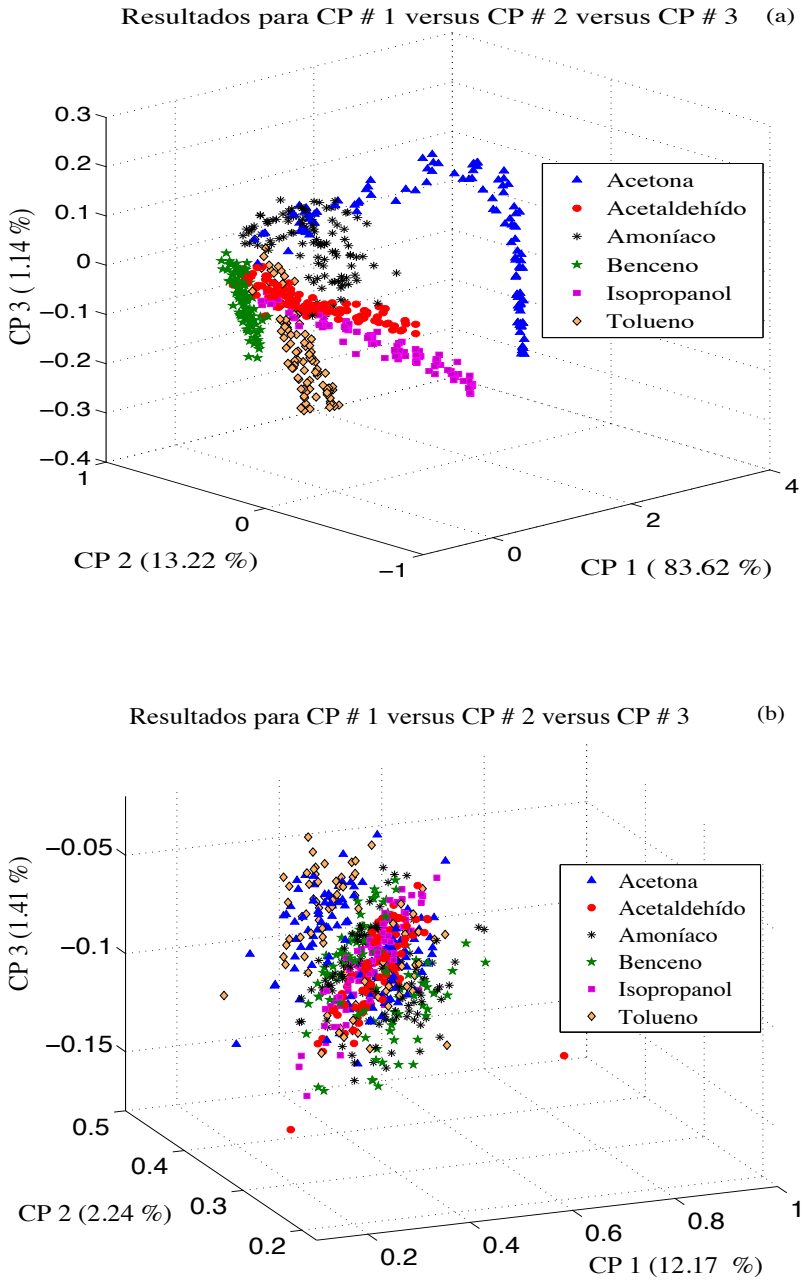


Figura 3.9: Diagramas de dispersión tridimensional para el análisis de componentes principales. Subfigura (a): utilizando las características *wavelet* extraídas para el sensor óptico de gas S2. Subfigura (b): utilizando como características los máximos de las respuesta del sensor óptico de gas óptico S2. Los datos corresponden al problema de representar las características propias de los seis gases.

A partir de las gráficas anteriores, es claro no sólo que las características extraídas por medio de la TWD-2D a la respuesta del sensor tipo 2 capturan la complejidad del problema de discriminación planteado en los tres primeros componentes principales (con una varianza del 83.63 % para el primer componente, 13.22 % para el segundo y 1.14 % para el tercero), lo cual no solamente significa una baja correlación mantenida por las características sugeridas; sino también que el espacio tridimensional proporcionado por las características *wavelet* mejora en gran medida la separación entre las especies de gas en comparación con las características típicas obtenidas a partir de los máximos de la respuesta del sensor sin perder la información relevante para estimar el valor de la concentración de gas de cada clase particular. Este resultado es particularmente positivo ya que del panorama proporcionado por la figura puede verse que las trayectorias abarcadas en el espacio tridimensional son específicas del analito, lo que implica que la identidad de la clase de analito puede ser fácilmente resuelta por la orientación de las trayectorias, conservando al mismo tiempo la información de la concentración de los analitos en la distribución de las mediciones a lo largo de la curva, facilitando de esta manera la decisión de un clasificador subsiguiente tanto para estimar la identidad del gas como su eventual concentración.

3.2.4 Clasificador, máquinas de soporte vectorial

Después de corroborar a través del análisis de componentes principales que las características *wavelet* generadas permiten realizar la discriminación de los gases de prueba, para obtener una evaluación más completa se decidió cuantificar el desempeño de los dos métodos de extracción de características empleados, esto mediante un clasificador genérico, el cual produce una tasa de clasificación relacionada con la capacidad de clasificación de cada modelo evaluado.

Como se recordará, el clasificador es la última parte del sistema de reconocimiento de patrones y se encarga de pronosticar a qué clase o categoría pertenece un objeto, para lo cual hace uso de la información esencial obtenida en las etapas previas. Mientras la mayoría de las técnicas exploratorias son no supervisadas, tal es el caso del ACP, los clasificadores son supervisados, es decir, primeramente llevan a cabo un entrenamiento o aprendizaje donde los vectores de datos se etiquetan con un descriptor, las clases se aprenden y se agrupan de acuerdo a su descripción y una vez completado el aprendizaje un vector desconocido puede ser identificado y clasificado usando las relaciones encontradas a priori a partir de los vectores de

entrenamiento [26, 78].

Ya que ninguno de los métodos de extracción de características puesto a consideración en este trabajo restringe utilizar específicamente algún clasificador, se eligió un algoritmo popular y de última generación, una máquina de aprendizaje ampliamente aprovechada en aplicaciones de clasificación, minería de datos y reconocimiento de patrones, a saber, un clasificador llamado máquina de soporte vectorial (SVM, por sus siglas en inglés). A continuación se describe de manera breve la teoría de este clasificador.

Partiendo de un espacio de características, donde los patrones están representados por vectores de características, el objetivo principal de un clasificador es dividir ese espacio en regiones asignadas a diferentes clases. Esas regiones se llaman regiones de decisión y si un vector de características se encuentra en alguna de éstas, el patrón asociado a ella se asigna a la clase correspondiente [49]. La figura 3.10 muestra un ejemplo muy sencillo, un caso de clasificación binaria donde dos clases de patrones, C_1 y C_2, son descritos por vectores de características bidimensionales, $\mathbf{x}_i = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) \in \mathbb{R}^2$. Las clases están separadas en dos regiones de decisión por medio de una línea recta llamada función de decisión lineal, $f(\mathbf{x})$, cuya ecuación, en términos de x_1 y x_2 puede escribirse como:

$$f(\mathbf{x}) = w_1 x_1 + w_2 x_2 + b = 0, \tag{3.10}$$

donde w_1 y w_2 son los coeficientes o pesos que determinan la pendiente de la línea recta.

Para un espacio de características p-dimensional, $\mathbf{x}_i = (x_1 \ x_2 \ \ldots \ x_p)' \in \mathbb{R}^p$, la generalización de la función de decisión lineal es directa, siendo ahora una superficie de decisión, o discriminante, lineal y p-dimensional llamada hiperplano:

$$\begin{aligned} f(\mathbf{x}) &= \sum_{i=1}^{p} w_i x_i + b \\ &= \langle \mathbf{w}, \mathbf{x} \rangle + b \\ &= \mathbf{w}'\mathbf{x} + b = 0. \end{aligned} \tag{3.11}$$

Este hiperplano de separación entre dos clases, en un clasificador máquina de soporte vectorial, debe ser óptimo, de tal manera que su distancia mínima con respecto a los vectores de entrenamiento más cercanos (vectores soporte), llamada margen de separación, sea máxima; esto sucede cuando la distancia $d = \frac{1}{\|\mathbf{w}\|}$, es decir,

$$\min_{\mathbf{x}_i} \mid \mathbf{w}'\mathbf{x} + b \mid = 1, \tag{3.12}$$

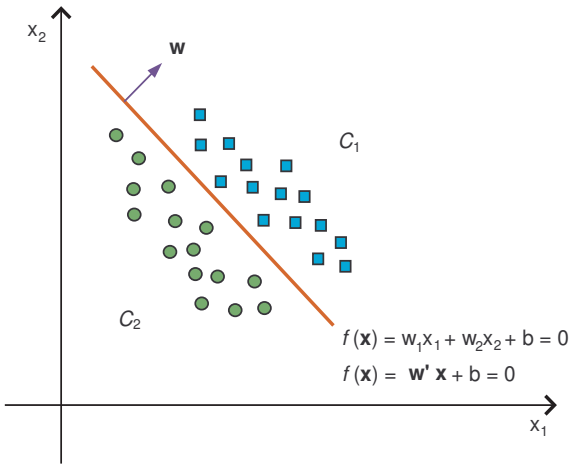


Figura 3.10: Ejemplo de clasificación binaria. Un conjunto de vectores, $\mathbf{x}_i$, con características bidimensionales (x_1 y x_2), están separados por medio de una línea recta, $f(\mathbf{x})$, en dos regiones de decisión que permiten clasificarlos como pertenecientes a la clase C_1 o C_2.

como se ilustra en la figura 3.11, donde también pueden verse expresadas matemáticamente las distancias de uno de los puntos al hiperplano y la distancia del hiperplano al origen.

Si los vectores de entrenamiento están definidos por:

$$t_i = \begin{cases} 1 & \text{si} \quad \mathbf{x}_i \in C_1 \\ -1 & \text{si} \quad \mathbf{x}_i \in C_2 \end{cases}, \tag{3.13}$$

entonces el conjunto de los vectores soporte puede ser escrito en la forma $\Omega_s = \{\mathbf{x}_i \mid t_i(\mathbf{w}'\mathbf{x}_i + b) = 1\}$.

El enfoque SVM de maximizar el margen de separación (lo cual es equivalente a minimizar la norma del vector de peso) puede expresarse como el siguiente problema de optimización restringido:

$$\begin{cases} \text{minimizar} \quad \Phi(\mathbf{w}) = \frac{1}{2}\|\mathbf{w}\|^2, \\ \text{sujeto a} \quad t_i(\mathbf{w}'\mathbf{x}_i + b) \geq 1, \quad i = 1, 2, \ldots, n. \end{cases} \tag{3.14}$$

Este tipo de problemas se resuelve por medio de multiplicadores de Lagrange y

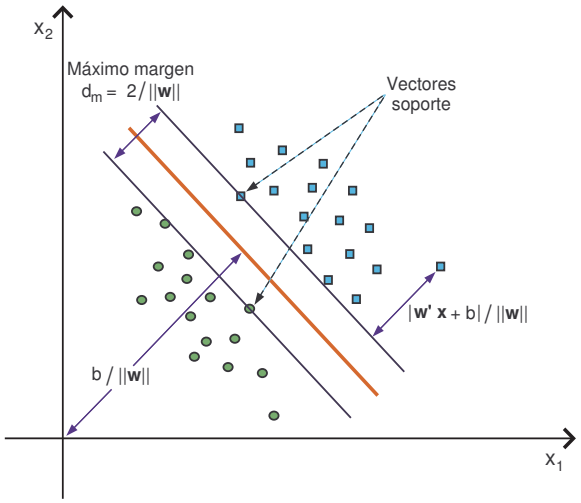


Figura 3.11: Esquema del principio básico de una máquina de soporte vectorial. El máximo margen de separación entre los vectores soporte de ambas clases es $2/\|\mathbf{w}\|$.

consiste en calcular el punto de silla de la función Lagrangiano:

$$L(\mathbf{w}, b, \alpha) = \frac{1}{2}\|\mathbf{w}\|^2 - \sum_{i=1}^{n} \alpha_i (t_i(\mathbf{w}'\mathbf{x}_i + b) - 1), \tag{3.15}$$

minimizando respecto a $\mathbf{w}$ y b y maximizando respecto a los multiplicadores de Lagrange no negativos, α_i. Haciendo lo anterior, se derivan las condiciones de optimalidad:

$$\mathbf{w} = \sum_{i=1}^{n} \alpha_i t_i \mathbf{x}_i \tag{3.16}$$

$$\sum_{i=1}^{n} \alpha_i t_i = 0. \tag{3.17}$$

Para calcular todos los pesos se necesitan los valores de los multiplicadores de Lagrange, por lo que a partir de la ecuación (3.15) y las condiciones dadas mediante las igualdades (3.16) y (3.17) se obtiene una expresión que depende sólo de α.

$$Q(\alpha) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \alpha_j t_i t_j \mathbf{x}_i' \mathbf{x}_j. \tag{3.18}$$

El problema anterior es conocido como el problema dual de optimización y consiste de maximizar $Q(\alpha)$ produciendo multiplicadores de Lagrange no negativos que satisfagan la condición presentada en la ecuación (3.17). Entonces, si $\tilde{\alpha}_i$ denota los multiplicadores de Lagrange óptimos, el vector de pesos óptimos, de acuerdo a la expresión (3.16), es:

$$\tilde{\mathbf{w}} = \sum_{i=1}^{n} \tilde{\alpha}_i t_i \mathbf{x}_i, \tag{3.19}$$

y el b óptimo, derivado del vector de pesos óptimo y de la condición dada por la ecuación (3.12) está dado por:

$$\tilde{b} = -\frac{1}{2}\tilde{\mathbf{w}}'(\mathbf{x}_{C_1} + \mathbf{x}_{C_2}), \tag{3.20}$$

donde $\mathbf{x}_{C_1}$ y $\mathbf{x}_{C_2}$ son vectores soporte de las clases $+1$ y -1 respectivamente.

La estructura de los clasificadores máquina de soporte vectorial puede modificarse para generar superficies de decisión no lineales, información al respecto puede encontrarse en las referencias ([49, 83]).

Aunque las máquinas de soporte vectorial fueron diseñadas para resolver problemas de clasificación binarios, se han desarrollado varias estrategias que permiten resolver problemas de clasificación de N clases [1, 37, 83] como el que fue planteado en este capítulo. Para resolverlo se eligió la estrategia uno contra uno, en la cual, $N(N-1)/2$ clasificadores binarios son entrenados y cada clasificador separa un par de clases, dando un voto a la clase ganadora, por lo cual la decisión se toma en base a la mayoría de votos.

Antes de aplicar un clasificador, en este caso el algoritmo SVM, es conveniente usar una técnica de normalización de datos, pues de esta manera se evita un efecto de escala que puede enmascarar las interrelaciones entre los mismos [78], en otras palabras, se evita que los datos de rangos grandes dominen sobre aquellos que tengan rangos más pequeños. La técnica de normalización de datos empleada tanto para los datos de entrenamiento como para los datos de prueba debe ser la misma, comúnmente los datos se normalizan al rango $[-1, +1]$ o $[0, 1]$.

3.2.5 Validación del clasificador

Independientemente del modelo de clasificador elegido, es necesaria su validación, ésta consiste en establecer sus capacidades de reconocimiento y de predicción, y su estabilidad o robustez. Para ello, el total de observaciones es dividido en dos

conjuntos, un conjunto de entrenamiento con el cual se desarrolla el modelo, y otro de evaluación o prueba que está formado por objetos de los que se conoce a que clase pertenecen pero que no están incluidos en el conjunto de entrenamiento. La capacidad de reconocimiento se refiere al porcentaje de objetos del conjunto de entrenamiento que son clasificados correctamente y la capacidad de predicción al porcentaje de objetos del conjunto de evaluación que son clasificados correctamente por el modelo. Por otra parte, se dice que un modelo es estable si la eliminación de uno o de unos pocos objetos, o la sustitución de unos objetos por otros en los conjuntos de entrenamiento y predicción no hace variar sus capacidades de reconocimiento y predicción [73].

La tarea de clasificación de seis clases propuesta en este capítulo se concluyó usando un clasificador máquina de soporte vectorial, multiclase y con kernel lineal validada por medio de la técnica llamada validación cruzada (en inglés, cross-validation), la cual utiliza vectores de respuesta no clasificados y está bien establecida [26]. Dicha clasificación se llevó a cabo utilizando diez conjuntos distintos de características, nueve de los cuales corresponden a características extraídas a partir de un mapeo de las respuestas del sensor al dominio *wavelet* y el restante a las características extraídas directamente de las respuestas máximas del sensor.

El procedimiento seguido para validar el clasificador está ilustrado en la figura 3.12 y consiste de los siguientes pasos: primero, para cada sensor, S1 o S2, el total del conjunto de características —como se recordará, 620 mediciones, cada una de ellas representada por un vector resultante de concatenar los 128 coeficientes de detalle *wavelet* en alguna de sus tres direcciones (horizontal, vertical o diagonal)— se divide aleatoriamente en dos subconjuntos; uno, con el 70 % del total de las mediciones que es utilizado como muestra de entrenamiento, y el otro, con el 30 % restante, que sirve como muestra de prueba pues con estos datos se estima la precisión del clasificador. Después, la muestra de entrenamiento es sometida a un proceso de validación cruzada con 10 grupos o sub-muestras (en inglés, 10-fold cross-validation); esto se refiere a que el conjunto de 434 mediciones fue dividido aleatoriamente en 10 partes (más o menos del mismo tamaño y sin intersecciones), con las cuales se lleva a cabo 10 veces el entrenamiento y selección del modelo, usando en cada ocasión y sin repetir, una de las 10 partes como conjunto de reconocimiento y las nueve restantes como el total del conjunto de entrenamiento; los modelos de clasificación seleccionados son evaluados calculando la media aritmética de la razón de clasificación exitosa para el conjunto de prueba en las 10 iteraciones realizadas. Posteriormente se repite todo el procedimiento anterior 100

veces, asegurando en cierta medida que cada vector de datos en el conjunto de datos se mantiene por lo menos una vez para la validación. Finalmente se obtiene la exactitud del modelo promediando la razón de éxito de clasificaciones correctas.

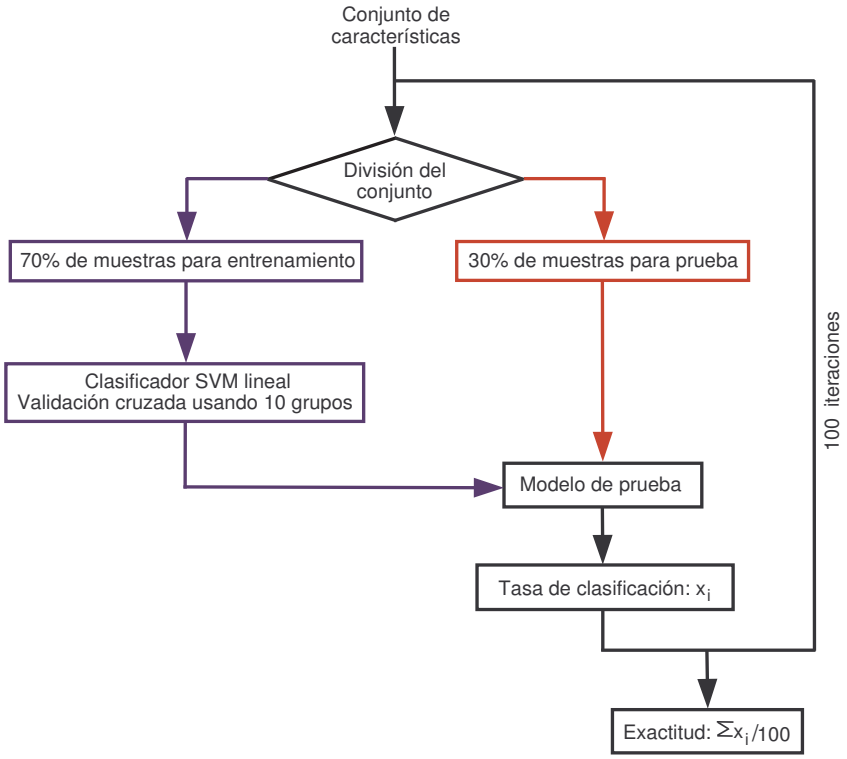


Figura 3.12: Esquema de validación propuesto para el clasificador. Partición en subconjuntos: entrenamiento/prueba. La línea azul indica el subconjunto de mediciones dedicadas a crear y validar los modelos de clasificación, mientras la línea roja representa el subconjunto de mediciones utilizadas para probar el modelo. Este episodio de partición aleatorio se repite 100 veces, asegurando en cierto grado que todas las réplicas de las mediciones han sido retenidas al menos una vez para validación.

3.3 Resultados

La tabla 3.2 indica los resultados de discriminación entre los seis gases usando como datos de entrada al clasificador las características *wavelet* obtenidas para los sensores S1 y S2 respectivamente. Claramente los resultados son excepcionales, pues cada uno de los sensores fue capaz de discriminar e identificar casi perfectamente las seis especies químicas analizadas al utilizar el esquema de validación propuesto para el clasificador SVM, esto sin importar el tipo de coeficientes de detalle *wavelet*. Específicamente, el sensor tipo 2 presenta ligeramente un mejor desempeño que el sensor tipo 1 para las características *wavelet* correspondientes a las sub-imágenes de detalle en las direcciones horizontal y vertical, lo cual puede deberse a que los mecanismos de interacción fisicoquímica causados por la difusión del analito a través de la nanoestructura parecen ser capturados más completamente por las subimágenes de detalle *wavelet* en las direcciones horizontal y vertical quizás debido al comportamiento unimodal existente encontrado inherentemente en la respuesta del sensor tipo 2. Este efecto no está presente para el sensor tipo 1, que exhibe un mejor desempeño que el sensor tipo 2 para la información *wavelet* obtenida en la dirección diagonal, lo cual sugiere estar ligado al doble pico de longitud de onda que presenta este sensor como respuesta propia ante los analitos. Sin embargo, en todos los casos, el esquema de clasificación propuesto basado en la extracción de características *wavelet* siempre supera en gran medida al que se basa en la estrategia de extracción de características a partir del pico máximo de longitud de onda como se muestra en la tabla 3.3.

Tabla 3.2: Tasa de éxito (%) estimada para la discriminación de gases usando validación cruzada para un clasificador SVM lineal y una estrategia de clasificación uno contra uno, utilizando como extractor de características a la transformada *wavelet*.

Sensor $\longrightarrow$	S1			S2		
Sub-imagen *wavelet* $\longrightarrow$	D_H	D_V	D_D	D_H	D_V	D_D
Función *wavelet* $\downarrow$						
db1	**94.06**	98.09	**94.27**	**97.59**	98.05	**87.12**
db2	90.03	97.22	86.44	94.50	97.11	79.33
db4	91.41	**98.13**	90.59	91.18	**98.62**	66.14

Tabla 3.3: Tasa de éxito (%) estimada para la discriminación de gases usando validación cruzada para un clasificador SVM lineal y una estrategia de clasificación uno contra uno utilizando como extractor de características a los máximos de la respuesta del sensor.

Sensor $\longrightarrow$	S1	S2
Interval $\downarrow$		
Λ_1	23.2279 ± 0.3770	22.4400 ± 0.9109
Λ_2	36.9964 ± 3.7660	34.7314 ± 2.0712

Los resultados anteriores fueron dados a conocer en el artículo:

- Murguía, J. S., Vergara, A., Vargas-Olmos, C., Wong, Travis J., Fonollosa, J. y Huerta, R. **Two-dimensional wavelet transform feature extraction for porous silicon chemical sensors**. En: *Analytica Chimica Acta*. 2013, vol. 785, pp. 1-15.

3.4 Conclusiones

Los resultados que se obtuvieron no sólo demuestran claramente el gran potencial y la idoneidad del esquema de clasificación propuesto basado en la extracción de características mediante la transformada *wavelet* discreta bidimensional para resolver problemas de discriminación complejos con múltiples analitos como el que se estudió en este trabajo, sino también, y lo que es más importante, confirman que los mecanismos de interacción fisicoquímica manipulados en cada sensor pSi dominan de hecho las propiedades de detección discriminatoria de los sensores de vapor óptico presentados aquí. Por lo tanto, este estudio proporciona evidencia de que los sensores pSi ópticos combinados con la superficie de estabilización química y la técnica de extracción de características apropiadas son capaces de alcanzar un alto rendimiento en tareas de quimiosensado complejas.

4

Análisis fractal de matrices de cifrado e imágenes cifradas

Durante mucho tiempo aquellos conjuntos o funciones irregulares a los que no podían aplicarse los métodos matemáticos clásicos fueron indignos de un estudio profundo siendo comúnmente ignorados y en algunas ocasiones considerados meramente como curiosidades [18]; sin embargo, esto sufrió un cambio radical después de que con su trabajo pionero el matemático Benoît Mandelbrot creara la geometría fractal para representar aquellos objetos con formas geométricas afines a diferentes escalas que no encajan en la geometría clásica y que están presentes en nuestro entorno apareciendo éstas frecuentemente en la naturaleza, como en las estructuras ramificadas de los árboles, en las nubes y en las líneas costeras, por lo que a partir de entonces se vislumbró la amplia aplicabilidad de la geometría fractal [34] y posteriormente también surgió el interés por elaborar algoritmos y/o métodos para analizar de una manera práctica si las propiedades de invariancia a la escala y autosimilaridad podían estar ocultas en funciones, señales, distribuciones o series de tiempo originadas de fenómenos complejos no sólo derivados del mundo natural. Actualmente existe una gran variedad de métodos o técnicas para analizar o detectar el comportamiento singular o fractal que puede estar presente en diferentes clases de información [28, 33], entre los que se encuentran: el método de función de estructura [61], algunos métodos basados en la transformada *wavelet* [45, 62, 5], el análisis de fluctuaciones sin tendencia (DFA, del inglés: Detrended Fluctuation Analysis) [68], el análisis de fluctuaciones sin tendencia multifractal (MF-DFA, del inglés: Multifractal Detrended Fluctuation Analysis) y sus diversas modificaciones [32, 33, 64], o el DFA implementado mediante la transformada *wavelet* discreta [47, 55]. Éstos y algunos otros métodos han permitido analizar y comprender muchos fenómenos naturales y sociales y su uso ha ido creciendo y

adquiriendo importancia día con día al ser aplicados a datos de diversa índole, tales como los datos financieros, geofísicos, climáticos, ecológicos, biológicos, biomédicos, etc. y lograr caracterizarlos.

Por otra parte, en muchas ocasiones sin siquiera percatarnos del uso cotidiano que se les da, los sistemas de encriptación están presentes en nuestra vida diaria, basta mencionar la revolución digital que la rápida evolución del internet ha provocado y el uso actual y generalizado de datos multimedia —los cuales, ya sean información altamente clasificada como podrían ser estrategias o avances tecnológicos para uso militar; información de índole gubernamental o diplomática; información en formato digital que se desee comercializar y cuyo contenido quiera mantenerse a salvo de la piratería; e incluso información personal como una llamada desde un teléfono móvil, un pago en línea, una transacción electrónica, etc., requieren mantenerse íntegros y seguros durante su transmisión, recepción y almacenamiento— por lo que las técnicas de cifrado junto con sus respectivos criterios de evaluación son tópicos actuales, relevantes y dignos de estudio. De manera particular, las imágenes, no sólo considerándolas como elementos multimedia sino de modo independiente, forman parte de un vasto y variado número de aplicaciones en las que la privacidad y/o seguridad es de vital importancia, por lo que los métodos de cifrado de imágenes así como el análisis de su eficiencia y la evaluación de su seguridad juegan un papel crucial.

Desde las perspectivas mencionadas y contribuyendo al desarrollo de ambas e inspirado en los trabajos previos presentados en ([55]) y ([56]), donde la determinación del comportamiento fractal o multifractal se ha considerado representativo de los elementos de sistemas de cifrado, así como también en la referencia ([98]), donde el valor del parámetro multifractal permitió detectar un mensaje al analizar una portadora caótica con una señal embebida, sugiriendo que dicho parámetro puede ser usado como una medida eficiente de esquemas de encriptación; este capítulo se enfoca a la implementación y aplicación de algoritmos que permiten: por un lado, determinar las propiedades de escala presentes en las principales matrices de un sistema de encriptación basado en un autómata celular de regla 90; y por otro, en determinar las propiedades de escala de imágenes cifradas mediante tres esquemas de cifrado con el fin de analizar su comportamiento. Para ello, en la siguiente sección, primeramente se da a conocer en forma breve la evolución del DFA, que es el método base de este trabajo y después se describe el procedimiento para implementarlo junto con las respectivas variantes que fueron empleadas en las secciones subsecuentes donde se describen a detalle los experimentos llevados a cabo. Como

resultados, en el caso del análisis efectuado a las matrices utilizadas en el esquema de cifrado basado en un autómata celular de regla 90 se estableció por medio del análisis realizado que éstas presentan un comportamiento multifractal y, en el caso del análisis de imágenes cifradas, se ha logrado establecer, por medio del exponente de escala, una medida objetiva de la calidad visual de la imagen, la cual está asociada a la ininteligibilidad de la misma y al desempeño en la etapa de encriptación, lo cual es de gran utilidad en la seguridad perceptual de imágenes cifradas.

4.1 Métodos

Aunque, como ya se ha mencionado, existen varios métodos mediante los cuales se puede determinar la presencia o ausencia de propiedades fractales en diferentes clases de señales, el análisis de fluctuaciones sin tendencia es un método muy práctico y fácil de implementar que se utiliza para analizar las propiedades de escala de las fluctuaciones presentes en series temporales provenientes de diversos fenómenos, fue propuesto por Peng *et al* a mediados de los años noventa con el fin de estudiar las características de largo alcance de regiones codificadas y no codificadas de las secuencias de nucleótidos del ADN [68]; casi una década después Kantelhardt y otros investigadores [32] hicieron una generalización de este algoritmo para el caso de series temporales de carácter multifractal denominándolo análisis de fluctuaciones sin tendencia multifractal, el cual encontró gran aceptación y ha sido extensamente utilizado; en el 2005, aprovechando que a partir de los coeficientes de aproximación de la transformada *wavelet* discreta se puede calcular la tendencia local de la información, Manimaran y colaboradores [47] propusieron el cálculo del MF-DFA mediante *wavelets*, algoritmo que también ha sido usado frecuentemente por requerir de un menor costo computacional y ofrecer una mejor exactitud [55, 57, 60]. Un gran número de publicaciones revela que los métodos mencionados fueron ampliamente aprovechados en distintas ramas de las ciencias; sin embargo, las señales que habían sido analizadas con ellos hasta ese entonces eran unidimensionales, hecho que no podía pasar desapercibido dada la existencia de señales de más de una variable independiente y dado además el gran porcentaje de información que recibimos en forma visual, por lo que, desde este punto de vista, surgió el interés por adecuar este tipo de algoritmos, cuya implementación podía considerarse más práctica y sencilla que la de otros métodos, para analizar las propiedades de escala presentes en señales multidimensionales. Así, también

en el 2005, se publica un trabajo en el que se adapta el DFA para aplicarlo a imágenes, en el que se estudian las características de rugosidad de la textura de cuatro imágenes determinando un exponente de escala promedio a partir del cálculo de los índices de Hurst de secuencias unidimensionales extraídas de las imágenes para cada una de las varias orientaciones a las que fue hecho el estudio [4]; un análisis similar pero implementando esa adaptación del algoritmo DFA mediante *wavelets* fue propuesta posteriormente [87], en ella se analizaron las propiedades de escala de varias imágenes solamente en dos direcciones; en el 2006, se generaliza el DFA y el MF-DFA para ser aplicado a señales multidimensionales, en particular, al caso bidimensional para distinguir las propiedades fractales y multifractales de superficies sintéticas [23]; esta generalización del MF-DFA para dos dimensiones fue adoptada para extraer importantes características de la textura de imágenes de hojas y obtener varios parámetros multifractales clave, los cuales, usando un clasificador máquina de soporte vectorial permiten distinguir hojas de diferentes especies de plantas [92].

Los métodos referidos: DFA, DFA y MF-DFA mediante *wavelets*, DFA mediante *wavelets* adaptado a imágenes y DFA bidimensional fueron utilizados para llevar a cabo el análisis presentado en una u otra de las secciones que forman parte del resto de este capítulo, por lo que el procedimiento para implementarlos se describe a continuación.

4.1.1 Análisis de fluctuaciones sin tendencia

Para una secuencia o serie temporal $x(t_k) = x[k]$, donde $t_k = k\Delta t$ y $k = 1, 2, \ldots, N$, el procedimiento estándar del DFA consiste de los siguientes pasos:

1. Calcular el perfil $Y[k]$ de la serie temporal,

$$Y[k] = \sum_{i=1}^{k} (x[i] - \mu) \tag{4.1}$$

   donde μ es el promedio de $x[k]$.

2. El perfil Y se divide en $N_s = \lfloor N/s \rfloor$ ventanas o segmentos sin traslapar de tamaño s. El símbolo $\lfloor \cdot \rfloor$ indica el cálculo de la parte entera. Debido a que la longitud de N puede no ser un múltiplo de s, la división se realiza empezando con el inicio y el final del perfil, es decir, se tienen $2N_s$ segmentos.

3. Calcular la tendencia local para cada una de las $2N_s$ ventanas por un ajuste lineal de mínimos cuadrados de la serie. Luego se calcula la varianza local asociada a cada una de las ventanas ν de longitud s, esto es,

$$F_s(\nu) = \frac{1}{s}\sum_{k=1}^{s}\{Y[(\nu-1)s+k] - Y_\nu[k]\}^2 \quad \text{para } \nu = 1, 2, \ldots, N_s, \text{ y} \tag{4.2a}$$

$$F_s(\nu) = \frac{1}{s}\sum_{k=1}^{s}\{Y[N-(\nu-N_s)s+k] - Y_\nu[k]\}^2, \tag{4.2b}$$

donde $\nu = N_s+1, N_s+2, \ldots, 2N_s$ y $Y_\nu[k]$ corresponde al polinomio lineal de ajuste en la ventana ν.

4. Promediar sobre todos los segmentos para obtener la función de fluctuación

$$F(s) = \left\{\frac{1}{2N_s}\sum_{\nu=1}^{2N_s}|F_s^2(\nu)|\right\}^{1/2}. \tag{4.3}$$

5. Repetir los pasos 2 a 4 para segmentos de diferente longitud s, donde se recomienda tener en cuenta $s_{\text{mín}} \simeq 4$ y $s_{\text{máx}} \simeq N/4$, de acuerdo a Peng *et al* [68].

Para determinar si la secuencia o serie temporal bajo análisis tiene correlaciones de rango amplio o un comportamiento de escala fractal, la función de fluctuación $F(s)$ debe observar la ley de potencia:

$$F(s) \sim s^\alpha, \tag{4.4}$$

donde α se denomina exponente de escala, el cual representa las propiedades de correlación de ley de escala de rango amplio, y se calcula a partir de la ecuación (4.4) considerando el valor de la pendiente de gráfica logarítmica de $F(s)$ en términos de s, es decir, $\alpha = \log F(s) \;/\; \log s$.

4.1.2 DFA mediante *wavelets*

El enfoque del MF-DFA mediante *wavelets* (en adelante, WT-MFDFA), fue considerado inicialmente en la referencia ([47]) y ha sido utilizado en diferentes aplicaciones, entre ellas en ([55]). La idea general reside en explotar el hecho de que la versión de aproximación o de pasa-bajas en la descomposición discreta de

la transformada *wavelet* tiene un gran parecido de la señal original de manera promediada en diferentes resoluciones. Por tanto, se puede calcular la tendencia "local" de la información a partir de los coeficientes de la versión de aproximación, a diferencia del caso tradicional en el que se utiliza un ajuste polinomial. Así, para una secuencia o serie temporal $x(t_k) = x[k]$, donde $t_k = k\Delta t$ y $k = 1, 2, \ldots, N$, el enfoque del DFA mediante *wavelets* (en adelante, W-DFA) sigue los pasos que a continuación se mencionan:

1. Calcular el perfil $Y[k]$ de la serie temporal,

$$Y[k] = \sum_{i=1}^{k} (x[i] - \mu) \tag{4.5}$$

   donde μ es el promedio de $x[k]$.

2. Calcular la descomposición multi-nivel del perfil mediante la transformada *wavelet* en cada nivel m.

3. Para cada nivel m, se extraen las fluctuaciones del perfil de la serie temporal después de sustraer la tendencia "local" de la información, es decir,

$$\Delta Y[k; m] = Y[k] - \tilde{Y}[k; m], \tag{4.6}$$

   donde $\tilde{Y}[k; m]$ es el perfil reconstruido después de la remoción sucesiva de los coeficientes de detalle en cada uno de los niveles m.

4. Las fluctuaciones $\Delta Y[k; m]$ en el nivel m se dividen en $M_s = \lfloor N/s \rfloor$ ventanas o segmentos sin traslapar de tamaño s, donde el símbolo $\lfloor \cdot \rfloor$ indica calcular la parte entera del argumento correspondiente. Debido a que la longitud de N puede no ser un múltiplo de s, la división se realiza empezando con el inicio y el final del perfil, es decir, se tienen $2M_s$ segmentos. Posteriormente, se calculan las varianzas locales asociadas a cada ventana ν,

$$F^2[\nu, s; m] = \mathrm{var}(\Delta Y[(\nu - 1)s + j; m]), \tag{4.7}$$

   donde $j = 1, \ldots, s,$, y $\nu = 1, \ldots, 2M_s$.

5. Promediar sobre todos los segmentos para obtener la función de fluctuación

$$F[s; m] = \left\{ \frac{1}{2M_s} \sum_{\nu=1}^{2M_s} |F^2[\nu, s; m]| \right\}^{1/2}. \tag{4.8}$$

6. Repetir los pasos 4 a 5 para segmentos de diferente longitud s.

De manera similar al caso tradicional, para determinar si la secuencia o serie temporal bajo análisis tiene correlaciones a rango amplio o un comportamiento de escala fractal, la función de fluctuación $F[s;m]$ debe observar la ley de potencia:

$$F[s;m] \sim s^{\alpha}, \tag{4.9}$$

donde el exponente de escala $\alpha = \log F[s;m]/\log s$.

La extensión del DFA al método MF-DFA se basa en el cálculo de la así llamada función de fluctuación de orden q-ésimo definida, utilizando *wavelets*, como

$$F_q(s;m) = \left\{ \frac{1}{2M_s} \sum_{\nu=1}^{2M_s} |F^2(\nu,s;m)|^{q/2} \right\}^{1/q}, \tag{4.10}$$

donde $q \in \mathbb{Z}$ con $q \neq 0$. El comportamiento divergente cuando $q \to 0$ puede evitarse usando un promedio logarítmico para la función de fluctuación de 0-ésimo orden $F_0(s;m) = \exp\left\{ \frac{1}{2M_s} \sum_{\nu=1}^{2M_s} \ln |F^2(\nu,s;m)| \right\}$, ver ([32]), y el comportamiento de escala fractal de una serie de tiempo se evalúa calculando la función de fluctuación $F_q(s;m)$, la cual debe revelar una escala con ley de potencia:

$$F_q(s;m) \sim s^{h(q)}. \tag{4.11}$$

En la ecuación (4.11), $h(q)$ es el llamado exponente de Hurst generalizado, ya que depende de q, mientras el exponente de Hurst original es $h(2)$. Si $h(q)$ es constante para todo q se dice que la serie de tiempo es monofractal, de otra manera se dice que la serie tiene un comportamiento multifractal. En este último caso, se pueden calcular otros exponentes de escala multifractal, tales como el espectro de singularidades o de Hölder, $f(\alpha)$, de una señal o distribución $g(t)$ como la transformada de Legendre del exponente de escala $\tau(q)$ [25], es decir,

$$\alpha = \frac{d\tau(q)}{dq}, \qquad \text{y} \qquad f(\alpha) = q\alpha - \tau(q), \tag{4.12}$$

donde α caracteriza la fuerza (strength) de las singularidades, y el espectro de Hölder de dimensiones $f(\alpha)$ es una función convexa no negativa que está soportada sobre el intervalo cerrado $[\alpha_{\min}, \alpha_{\max}]$. El espectro $f(\alpha)$ puede ser interpretado como la dimensión fractal de Hausdorff del subconjunto de datos caracterizado por el exponente de Hölder, α [54, 62]. La singularidad más frecuente, la cual corresponde al

máximo de $f(\alpha)$, ocurre para el valor de $\alpha(q=0)$, mientras que los valores límite del soporte, $\alpha_{\min}$ para $q>0$ y $\alpha_{\max}$ para $q<0$, corresponden a las singularidades más fuerte y más débil, respectivamente. Por otro lado, un comportamiento lineal de $\tau(q)$ indica monofractalidad mientras que un comportamiento no lineal indica una señal multifractal. Adicionalmente, hay una relación entre el exponente de escala $\tau(q)$ y el exponente de Hurst generalizado $h(q)$, la cual está dada por $\tau(q)=qh(q)-1$ [32].

4.1.3 DFA mediante *wavelets* adaptado a imágenes

La parte medular del procedimiento que se describe a continuación fue inicialmente descrita en la referencia ([4]) y la implementación usando *wavelets* se presentó en ([87]). Básicamente la adaptación del W-DFA para poder ser aplicado a imágenes consta de lo siguiente.

1. Considerar I como la imagen a analizar e I_θ como una sub-imagen de I con orientación θ. En este trabajo el ángulo θ sólo se considera en dos direcciones: $\theta=0°$, para la orientación de norte a sur, o $\theta=90°$, para la orientación este a oeste.

2. Definir la sub-imagen I_θ como un arreglo $A_\theta(a,b)$ donde las filas se representan por $a=1,\ldots,N$ y las columnas por $b=1,\ldots,M$.

3. Calcular el análisis de escala para cada sub-imagen determinando primeramente el W-DFA de cada una de las filas o de cada una de las columnas, llevando a cabo el procedimiento descrito en la subsección 4.1.2, obteniendo la función de fluctuación $F_\theta[a;s;m]$ o $F_\theta[b;s;m]$ según corresponda.

4. Determinar el exponente de escala tomando en cuenta el promedio geométrico de la función de fluctuación correspondiente, $F_\theta[a;s;m]$ o $F_\theta[b;s;m]$, por ejemplo, si el análisis se efectúo a las columnas de la imagen:

$$F_{\text{prom}}[j;s;m]=\left(\prod_{b=1}^{M}F_\theta[b;s;m]\right)^{1/M}, \tag{4.13}$$

   donde se considera el análisis para diferentes valores del tamaño de ventana s y el exponente de escala α_θ se calcula como la pendiente de la gráfica de $\log F_{\text{prom}}[j;s;m]$ en términos de $\log s$.

4.1.4 DFA bidimensional

La generalización del algoritmo para calcular el DFA de señales de dimensión más alta fue propuesta por Gu y Zhou en ([23]) y el procedimiento para llevarlo a cabo, en el caso bidimensional, es prácticamente el indicado a continuación. Primeramente, una señal bidimensional, es decir, una imagen $\mathbf{I}$ de tamaño $U \times V$ es considerada como una superficie y es denotada por una matriz $X(i,j)$, donde el número de filas y columnas está representado por $i = 1, 2, \ldots, U$ y $j = 1, 2, \ldots, V$, respectivamente. Después, para separar la tendencia de las fluctuaciones en las imágenes se realiza lo siguiente.

1. Dividir la superficie $X(i,j)$ en $U_s \times V_s$ ventanas cuadradas disjuntas del mismo tamaño $s \times s$, donde $U_s = \lfloor U/s \rfloor$ y $V_s = \lfloor V/s \rfloor$. Cada ventana es denotada por $X_{u,v}$ tal que $X_{u,v}(i,j) = X(i + l_1, j + l_2)$ para $1 \leq i, j \leq s$, donde $l_1 = (u-1)s$ y $l_2 = (v-1)s$.

2. Calcular la suma acumulativa para cada ventana $X_{u,v}$, posicionada por u y v, como
$$P_{u,v}(i,j) = \sum_{k_1=1}^{i} \sum_{k_2=1}^{j} (X_{u,v}(k_1,k_2) - \langle X_{u,v} \rangle), \tag{4.14}$$
donde $\langle X_{u,v} \rangle$ es el promedio de la sub-imagen $X_{u,v}$, para $1 \leq i,\ j \leq s$.

3. Determinar la tendencia de la sub-imagen obtenida ajustando el conjunto de los datos al plano $\tilde{P}_{u,v}(i,j) = ai + bj + c$, donde a, b, y c son parámetros estimados usando el método de mínimos cuadrados. En seguida, se calculan las varianzas locales asociadas a cada sub-imagen $X_{u,v}$ como
$$F^2(u,v,s) = \frac{1}{s^2} \sum_{i=1}^{s} \sum_{i=1}^{s} [P_{u,v}(i,j) - \tilde{P}_{u,v}(i,j)]^2. \tag{4.15}$$
Es importante aclarar que la tendencia de la sub-imagen puede conseguirse ajustando el conjunto de datos a otra función menos simple, sin embargo, el uso de otras funciones da casi los mismos resultados consumiendo mayor tiempo, por lo que el ajuste al plano es preferido en la práctica [23].

4. Después, se promedia sobre todas las sub-imágenes para obtener la función de fluctuación:
$$F_2(s) = \left(\frac{1}{U_s V_s} \sum_{u=1}^{U_s} \sum_{v=1}^{V_s} F^2(u,v,s) \right)^{1/2}. \tag{4.16}$$

Este procedimiento se repite para un amplio rango de segmentos de longitud s, considerando elegirlos entre $6 \leq s \leq \text{mín}(U, V)/4$. Para evaluar las propiedades de escala de la superficie, la función de fluctuación $F_2(s)$ debe exhibir una escala con ley de potencia

$$F_2(s) \sim s^{\alpha}, \tag{4.17}$$

donde $\alpha = \log F_2(s)/\log s$ es el exponente de escala e indica una medida del grado de correlación entre los pixeles de la superficie. Ya que U y V no necesariamente serán múltiplos del tamaño de la ventana, a semejanza del caso unidimensional, se considera repetir el mismo procedimiento desde las otras tres esquinas de la imagen [23].

4.1.5 Interpretación de los valores del exponente de escala

Al calcular el exponente de escala de una imagen por medio del DFA unidimensional se tienen las siguientes relaciones:

a) Si $\alpha = 0.5$ no hay correlación y los pixeles están decorrelacionados (proceso del ruido blanco).

b) Para $0 < \alpha < 0.5$, los pixeles presentan un comportamiento anticorrelacionado, lo cual significa que es más probable que un valor grande sea seguido por un valor pequeño, y viceversa; en este caso la señal se dice ser antipersistente.

c) Si $0.5 < \alpha < 1$, la correlación de los pixeles es persistente, donde es más probable que aparezcan valores grandes después de datos con valores grandes, o viceversa, valores pequeños después de datos con valores pequeños.

d) Los valores $\alpha = 1$ y $\alpha = 1.5$ corresponden respectivamente a ruido $1/f$ y movimiento Browniano.

Además, este exponente de escala puede ser considerado como una generalización del exponente de Hurst, H; satisfaciendo $0 < H < 1$ como sigue: para señales estacionarias, α es idéntico al exponente de Hurst, H, mientras para señales de tiempo no estacionarias $\alpha = H + 1$ [13, 17, 32, 60]. Por otro lado, en la referencia ([97]) se señala que la relación entre el exponente de Hurst, H, y α para el caso bidimensional es la siguiente: si la señal bidimensional es estacionaria, α es idéntica al exponente de Hurst, H; mientras que si no lo es, $\alpha = H + 2$.

4.2 MF-DFA de matrices de un sistema de cifrado

Con la finalidad de hacer esta exposición lo más explícita posible, a continuación se describe brevemente el esquema de encriptación considerado en este trabajo. Se trata del sistema de cifrado usado en la referencia ([86]), donde el fenómeno de sincronización del autómata celular (AC) ha sido aplicado para crear las dos familias de permutaciones y un generador de números pseudoaleatorios asintóticamente perfecto. El sistema de cifrado está basado en el uso de un AC que evoluciona de acuerdo a la regla local $x_i^{t+1} = \left(x_{i-1}^t + x_{i+1}^t\right) \text{ mód } 2$, la cual corresponde a la regla 90. El fenómeno de sincronización en pares acoplados del AC es descrito en detalle en la referencia ([85]), donde se encontró que un par de AC acoplados puede sincronizar si cada par de coordenadas consecutivas está separada por un bloque de $\left(2^k - 1\right)$ sitios desacoplados. Este sistema de encriptación basado en el fenómeno de sincronización de autómatas celulares es llamado ESCA (del inglés: Encryption System Cellular Automata).

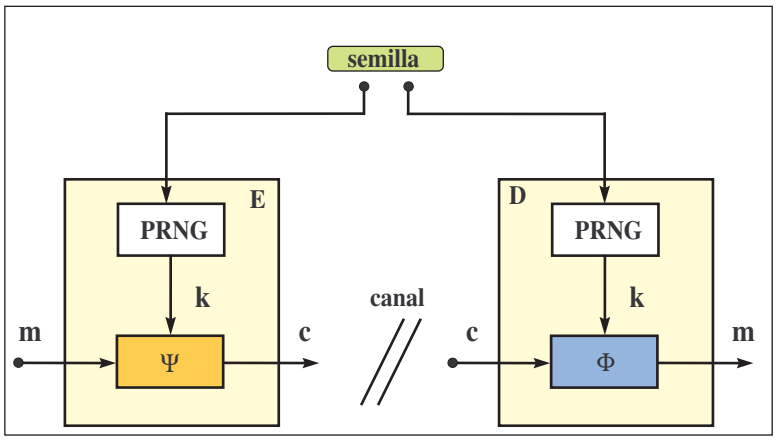


Figura 4.1: Modelo de cifrado considerado en este trabajo junto con sus principales componentes: la familia indexada de permutaciones, Ψ y Φ, y el generador pseudoaleatorio de llaves (PRNG).

La figura 4.1 muestra el sistema de encriptación completo. Básicamente, la clase del bloque del criptosistema considerado transforma una secuencia de texto plano $\mathbf{m}$ a una secuencia $\mathbf{c}$, llamado el texto cifrado. La transformación $\mathbf{m} \mapsto \mathbf{c}$ es elegida

de una familia indexada de permutaciones $\Psi = \{\psi_{\mathbf{x}} : M \to C | \mathbf{x} \in X\}$ eligiendo un índice $\mathbf{x}$ del conjunto de índices X. Todos los conjuntos M, C y X son conjuntos de palabras binarias de longitud N, es decir, Z_2^N, donde $Z_2 = \{0, 1\}$. Las palabras en M y C son llamadas los bloques claro y bloques de cifrado, respectivamente, mientras las palabras en el conjunto de índices X son las llaves de cifrado. Para revelar desde la secuencia de los bloques de cifrado, el criptosistema también proporciona la familia de permutaciones inversas $\Phi = \{\phi_{\mathbf{x}} : C \to M | \mathbf{x} \in X\}$ tal que para cada $\mathbf{x} \in X$ se tiene $\mathbf{m} = \phi_{\mathbf{x}}(\varphi_{\mathbf{x}}(m))$. Ya que el esquema de encriptación completa es privado, los procesos de cifrado y descifrado usan el mismo generador determinístico que es inicializado con una semilla común.

4.2.1 Enfoque matricial del sistema ESCA

Murguía y colaboradores [58] usaron un enfoque matricial para implementar efectivamente los componentes principales del sistema ESCA. De hecho, con algunas operaciones o transformaciones matriciales básicas sobre la matriz de la secuencia principal, denotada por $\mathbf{Q}_N$, ellos fueron capaces de implementar la gran mayoría de las etapas involucradas en el sistema de cifrado, es decir, la familia de permutaciones y el generador de números pseudoaleatorios.

Para el proceso de cifrado, $\mathbf{c} = \Psi_{\mathbf{x}}(\mathbf{m})$, se requieren dos matrices, $\mathbf{P}_N$ and $\mathbf{Q}_N$, tal que

$$\mathbf{c} = \Psi_{\mathbf{x}}(\mathbf{m}) = [(\mathbf{P}_N \times \mathbf{x}) + (\mathbf{Q}_N \times \mathbf{m})] \text{ mód } 2, \tag{4.18}$$

ambas matrices tienen dimensiones $N \times N = (2^n - 1) \times (2^n - 1)$ para $n = 1, 2, 3, \ldots$. La matriz $\mathbf{P}_N$ es inicialmente generada del vector $\mathbf{p} = [p_1, p_2, \ldots, p_N]$ el cual constituye la primera fila y los componentes con índices de posición $j = (2^n + 1) - 2^{i+1}$ e $i = 0, 1, 2, \ldots, (n - 1)$ tienen un valor de 1 y 0 en cualquier otra posición. Las filas $(N - 1)$ son generadas aplicando un desplazamiento a la derecha de una posición de la fila previa con un cero como su primer valor.

Por otra parte, la matriz principal $\mathbf{Q}_N$ puede ser generada inicialmente del vector $\mathbf{a} = [a_1, 0, \ldots, 0]$, donde el componente a_1 tiene un valor de 1, y N es el número de bits, es decir, a es un vector con N componentes. Este vector constituye la primera fila de la matriz $\mathbf{Q}_N$ y las filas $(N - 1)$ son generadas aplicando la regla 90 de la fila previa con condiciones de frontera de cero fijas a los lados izquierdo y derecho. Por ejemplo, para $N = 15$ se tiene que $\mathbf{P}_{15}$, y $\mathbf{Q}_{15}$ son de la forma expresada en la ecuación (4.19).

$$\mathbf{P}_{15} = \begin{pmatrix}
1&0&0&0&0&0&0&0&1&0&0&0&1&0&1\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&1&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix}, \quad \mathbf{Q}_{15} = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&0&0\\
0&0&0&0&1&0&1&0&1&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&0&1&0&0&0&0&0&1&0&1&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1
\end{pmatrix}. \tag{4.19}$$

En la figura 4.2 uno puede ver el patrón espacio temporal de las dos matrices de cifrado para $N = 127$, $\mathbf{P}_{127}$ y $\mathbf{Q}_{127}$, donde un patrón con una apariencia de un triángulo de Sierpinski puede notarse en la matriz $\mathbf{Q}$.

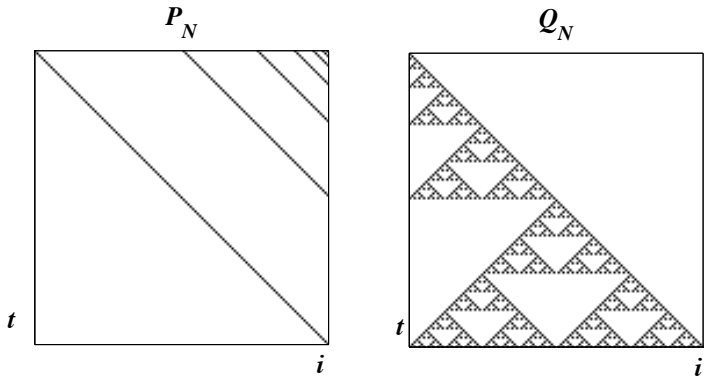


Figura 4.2: Patrón espacio-tiempo de las dos matrices, $\mathbf{P}_N$ y $\mathbf{Q}_N$, involucradas en el proceso de encriptación cuando $N = 127$ bits.

La implementación matricial de la permutación inversa $\mathbf{m} = \Phi_{\mathbf{x}}(\mathbf{c})$ tiene una estructura similar a la ecuación (4.18), esto es,

$$\mathbf{m} = \Phi_{\mathbf{x}}(\mathbf{c}) = [(\mathbf{R}_N \times \mathbf{x}) + (\mathbf{T}_N \times \mathbf{c})] \text{ mód } 2, \tag{4.20}$$

donde las matrices tienen dimensiones $N \times N = (2^n - 1) \times (2^n - 1)$ para $n = 1, 2, 3, \ldots$. De la ecuación (4.18), $\mathbf{R}_N = [-\mathbf{Q}_N^{-1}\mathbf{P}_N] \text{ mód } 2$, mientras la matriz $\mathbf{T}_N$ es sólo la inversa de $\mathbf{Q}_N$, es decir, $\mathbf{T}_N = \mathbf{Q}_N^{-1} \text{ mód } 2$. Como un ejemplo, y considerando nuevamente $N = 15$, se tiene que las matrices $\mathbf{R}_{15}$ y $\mathbf{T}_{15}$ están dadas por la ecuación (4.21).

$$\mathbf{R}_{15} = \begin{pmatrix}
1&0&0&0&0&0&0&0&1&0&0&0&1&0&1\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0\\
1&0&1&0&0&0&0&0&1&0&1&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
1&0&1&0&1&0&0&0&1&0&1&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
1&0&0&0&1&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}, \quad \mathbf{T}_{15} = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&1&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
1&0&1&0&1&0&0&0&1&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
1&0&1&0&0&0&0&0&1&0&1&0&1&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0\\
1&0&0&0&0&0&0&0&1&0&0&0&1&0&1
\end{pmatrix}. \tag{4.21}$$

En la figura 4.3 se muestran las dos matrices resultantes, $\mathbf{R}_N$ y $\mathbf{T}_N$, para $n = 7$, es decir, $N = 127$ bits. Ya que ambas matrices son el resultado de algunas operaciones matriciales sobre la matriz $\mathbf{Q}_N$ es claro que ambas deben presentar un patrón "similar".

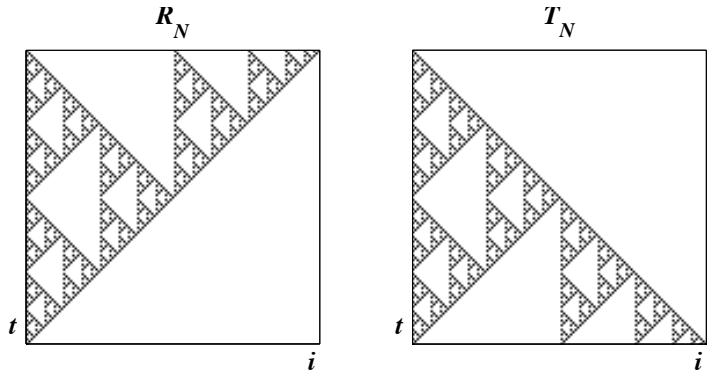


Figura 4.3: Patrón espacio-tiempo de las dos matrices, $\mathbf{R}_N$ y $\mathbf{T}_N$, involucradas en el proceso de descifrado cuando $N = 127$ bits.

En un trabajo previo, en ([56]), se introdujo una matriz secuencia $\mathbf{H}_N$ de dimensiones $(2N + 1) \times (2N + 1)$ para calcular factiblemente las secuencias pseudoaleatorias de N bits. Ya que la implementación matricial de esta matriz está descrita en ([56]) se omite su descripción y solamente se describe el formato de la

matriz $\mathbf{H}_N$ en términos de $\mathbf{Q}_N$, el cual está dado por la ecuación:

$$\mathbf{H}_N = \left(\begin{array}{c:c} \mathbf{Q}_N^{-1} & \hat{\mathbf{Q}} \\ \hdashline \mathbf{I} & \mathbf{0} \end{array}\right), \tag{4.22}$$

donde $\mathbf{I}$ es la matriz identidad con dimensiones $(N+1)\times(N+1)$, y $\mathbf{0}$ es una matriz cero con dimensiones $N\times(N+1)$. La matriz $\hat{\mathbf{Q}}$ tiene dimensiones $N\times(N+1)$, donde las primeras $(N-1)$ filas y N columnas están comprendidas en la matriz $\mathbf{Q}_N^{-1}$, pero sin la primera fila. Los componentes de la N-fila y la $(N+1)$-columna de $\hat{\mathbf{Q}}$ tienen un valor de 0 excepto en la intersección de ambos, la cual tiene un valor de 1. Por ejemplo, para $N=15$ y considerando la matriz $\mathbf{Q}_{15}$ en (4.19), se tiene la matriz (4.23) donde se puede ver directamente el papel de la matriz $\mathbf{Q}_{15}$ en la implementación de la matriz $\mathbf{H}_{15}$.

$$\mathbf{H}_{15} = \left(\begin{array}{cccccccccccccccc:cccccccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&1&0&1&0&0&0&1&0&1&0&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&1&0&0&0&0&0\\
1&0&1&0&0&0&0&0&1&0&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&0\\
1&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
\hdashline
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right), \tag{4.23}$$

4.2.2 Análisis de las propiedades multifractales de las matrices del ESCA

En la referencia ([55]) se empleó el análisis de fluctuaciones sin tendencia multifractal implementado mediante la transformada *wavelet* para determinar un posible comportamiento multifractal de algunas series de tiempo de autómatas celulares, en particular para las reglas 90, 105 y 150. Allí se encontró que estas reglas tienen un comportamiento multifractal intrínseco. Además, en un trabajo previo, ([56]), se había realizado un análisis encontrando características multifractales de la matriz $\mathbf{H}_N$, donde esta matriz fue calculada por medio de una técnica matricial ligeramente diferente. Así, de manera similar a la referencia ([55]) y ya que la secuencia de la matriz principal $\mathbf{Q}_N$ está basada en la evolución de la regla 90, aquí se analizó con el método WT-MFDFA la suma de unos en las secuencias de las filas de esta matriz. El WT-MFDFA se implementó usando la función *wavelet* db-4 perteneciente a la familia ortogonal de Daubechies [46], esta función *wavelet* se eligió debido a sus propiedades de ortogonalidad, calidad de aproximación y estabilidad numérica [46]; en suma, el algoritmo con las funciones de la familia *wavelet* de Daubechies es eficiente en memoria y es reversible, mientras que otras bases *wavelet* tienen un gasto computacional ligeramente más alto y son conceptualmente más complejas.

Los resultados para la suma de unos de las filas de la matriz de cifrado $\mathbf{Q}_N$ están ilustrados en la figura 4.4. Se consideraron $N = 2^{12} - 1 = 4095$ puntos de datos de las series de tiempo y el hecho de que el exponente de Hurst generalizado no sea una línea horizontal constante es un indicativo de un comportamiento multifractal en estas series de tiempo, ver la figura 4.4 (b). Ya que el exponente de escala τ no es de una sola pendiente, figura 4.4 (c), puede ser considerado como otra clara característica de multifractalidad. La fuerza de la multifractalidad es medida aproximadamente con el ancho, $\Delta\alpha = \alpha_{\max} - \alpha_{\min}$, del espectro de singularidades "parabólico" $f(\alpha)$ sobre el eje α, ver la figura 4.4 (d). Para esta matriz, el ancho, $\Delta\alpha_{\mathbf{Q}_{4095}} = 1.0160 - 0.0080 = 1.0080$, y la singularidad más frecuente ocurre en $\alpha_{\mathrm{mf}_{\mathbf{Q}_{4095}}} = 0.5540$.

Por otro lado, los resultados multifractales para las matrices de descifrado, $\mathbf{T}_N$ y $\mathbf{R}_N$, son exhibidos en la figura 4.5. Es de notar que ambas series de tiempo tienen un $\Delta\alpha$ más pequeño que la previa. Sin embargo, ambas presentan un comportamiento multifractal similar, por ejemplo, el ancho $\Delta\alpha_{\mathbf{R}_{4095}} = 0.9740 - 0.2180 = 0.7560$ y $\Delta\alpha_{\mathbf{T}_{4095}} = 0.9600 - 0.2180 = 0.7420$ no presentan una gran diferencia. De hecho, la singularidad más frecuente ocurre en el mismo valor alpha $\alpha_{\mathrm{mf}_{\mathrm{R}_{4095}}} = \alpha_{\mathrm{mf}_{\mathrm{T}_{4095}}} = 0.4280$.

Estos resultados eran esperados ya que estas matrices de descifrado dependen de la matriz $\mathbf{Q}_N$.

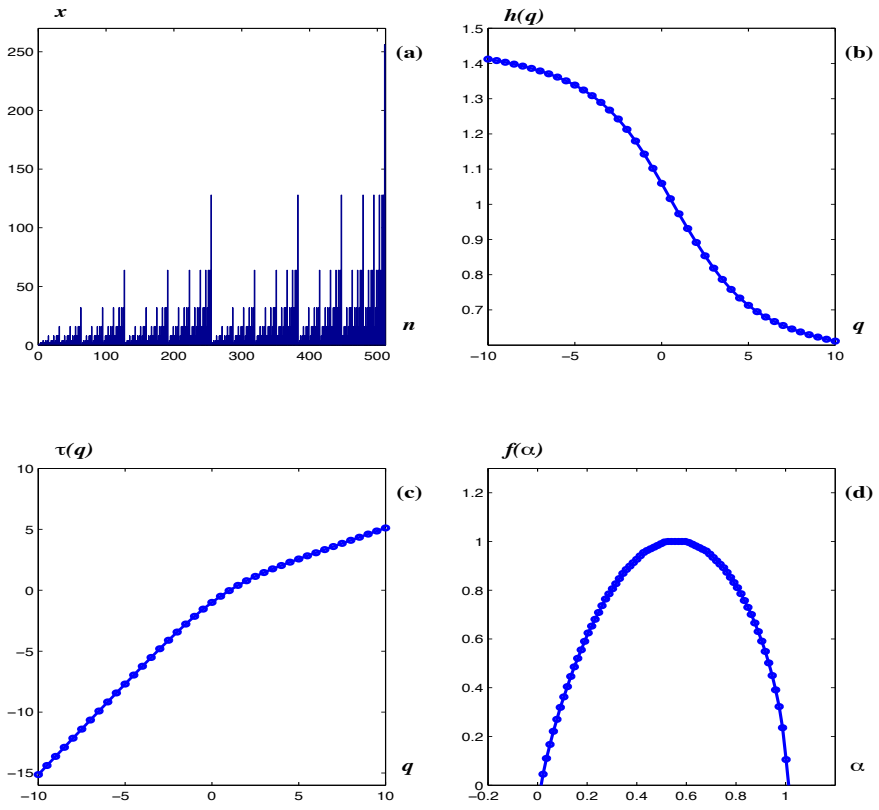


Figura 4.4: (a) Series de tiempo de la señales fila de $\mathbf{Q}_{4095}$. Solamente se muestran los primeros 2^9 puntos del conjunto total de $(2^{12}-1)$ puntos de datos; (b) el exponente de Hurst generalizado, $h(q)$; (c) el exponente τ, donde $\tau(q) = qh(q) - 1$ y (d) el espectro de singularidades $f(\alpha) = q\frac{d\tau(q)}{dq} - \tau(q)$.

Para evaluar el impacto de las longitudes de señales finitas sobre las cantidades multifractales se aplicó la técnica WT-MFDFA a la serie de tiempo obtenida de las matrices de encriptación implicadas en el sistema ESCA considerando longitudes diferentes: $N = 2^n - 1$, $n = 9, 10, 11, 12, 13$. La tabla 4.1 resume los resultados obtenidos, en ella se nota que los resultados de la matriz $\mathbf{Q}_N$ son más estables que los resultados obtenidos de las matrices de descifrado, $\mathbf{T}_N$ y $\mathbf{R}_N$. De hecho, los resultados obtenidos para $\mathbf{Q}_N$ concuerdan con aquellos presentados anteriormente en

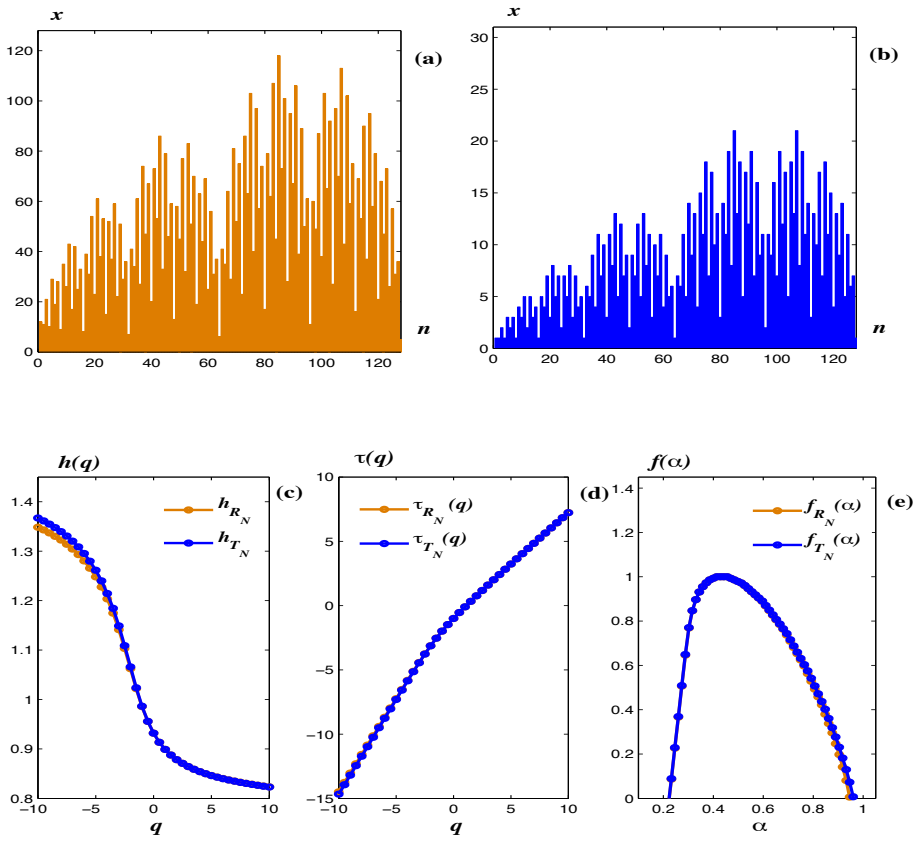


Figura 4.5: Series de tiempo de las señales fila de las matrices: (a) $\mathbf{R}_{4095}$ y (b) $\mathbf{T}_{4095}$. Solamente se muestran los primeros 2^8 puntos del conjunto total de $(2^{12}-1)$ puntos de datos. (c) El exponente de Hurst generalizado, $h(q)$, para las señales fila $\mathbf{R}_{4095}$ y $\mathbf{T}_{4095}$. (d) El exponente τ para cada señal y (e) el espectro de singularidades correspondiente $f(\alpha)$.

([55]), donde el método WT-MFDFA fue aplicado a diferentes reglas AC, incluyendo la regla AC 90.

El análisis desarrollado en esta sección fue publicado en el artículo:

- Murguía, J. S., Mejía Carlos M., Vargas-Olmos C., Ramírez-Torres, M. T., y Rosu, H. C. **Wavelet multifractal detrended fluctuation analysis of encryption and decryption matrices**. En: *International Journal of Modern Physics C*. 2013, vol. 24, no. 9, pp. 1350069.

Tabla 4.1: Los valores del ancho $\Delta\alpha = [\alpha_{\text{mín}}, \alpha_{\text{máx}}]$ y la singularidad más frecuente, α_{mf}, para diferentes dimensiones de las tres matrices $\mathbf{Q}_N$, $\mathbf{R}_N$ y $\mathbf{T}_N$ obtenidas por medio del método WT-MFDFA.

		n				
Matriz		9	10	11	12	13
$\mathbf{Q}_N$	α_{min}	0.1200	0.0500	0.0220	0.0080	0.0080
	α_{max}	1.1000	1.0580	1.0300	1.0160	1.0160
	$\Delta\alpha$	0.9800	1.0080	1.0080	1.0080	1.0080
	α_{mf}	0.6520	0.5960	0.5820	0.5540	0.5540
$\mathbf{R}_N$	α_{min}	0.0360	0.1060	0.1620	0.2180	0.2460
	α_{max}	0.8060	0.8760	0.9320	0.9740	0.9880
	$\Delta\alpha$	0.7700	0.7700	0.7700	0.7560	0.7420
	α_{mf}	0.2880	0.3440	0.4000	0.4280	0.4560
$\mathbf{T}_N$	α_{min}	0.0220	0.1060	0.1620	0.2180	0.2460
	α_{max}	0.8060	0.8760	0.9320	0.9600	0.9880
	$\Delta\alpha$	0.7840	0.7700	0.7840	0.7420	0.7420
	α_{mf}	0.3020	0.3440	0.4000	0.4280	0.4560

4.2.3 Conclusiones

Se utilizó la variante del análisis de fluctuaciones sin tendencia multifractal basado en la transformada *wavelet* para revelar las características multifractales de algunas matrices que llevan a cabo las principales funciones en un sistema de encriptación. Para lograr este objetivo se discutieron algunas cantidades multifractales tales como el exponente de Hurst generalizado, $h(q)$, el espectro de singularidades $f(\alpha)$, y el exponente de escala, $\tau(q)$, de estas matrices. En general, puede decirse que las cantidades multifractales proporcionan información estadística útil y la caracterización de las matrices usadas en algunas clases de sistemas de cifrado.

4.3 DFA bidimensional aplicado a imágenes cifradas

Como se sabe, con el fin de preservar la confidencialidad de las imágenes digitales suelen utilizarse técnicas de cifrado cuyo objetivo es transformar la imagen original en una imagen cifrada completamente ininteligible, es decir, la imagen obtenida después del proceso de encriptación no debe exhibir ninguna característica de la imagen original que la pueda hacer comprensible para el observador, lo cual se logra cuando los pixeles de la nueva imagen adquieren un comportamiento lo más "aleatorio" posible. Esta aleatoriedad de los pixeles de la imagen cifrada puede ser cuantificada en términos de la dimensión fractal de la misma, por lo que la dimensión fractal puede usarse para cuantificar la calidad del contenido multimedia cifrado [41]. Esta medida relacionada con la fractalidad no es la única que ha sido empleada en trabajos concernientes con la criptografía, en la referencia ([98]) el exponente de Hurst generalizado se consideró como una medida eficiente de esquemas de encriptación, allí los autores fueron capaces de detectar la presencia de un mensaje en una portadora caótica con una señal embebida. Por tanto, en el análisis correspondiente a esta sección, se planteó la posibilidad de que el exponente de escala fuera útil como una medida de la calidad del contenido de una imagen cifrada.

Ahora, desde otra perspectiva, ciertas características de los datos multimedia como la alta redundancia, el gran tamaño de datos y el requerimiento de interacciones en tiempo real hacen que los métodos de cifrado convencionales (tales como el AES (Advanced Encryption Standard), el RSA (Rivest, Shamir y Adleman) o el IDEA (International Data Encryption Algorithm), generalmente usados para el cifrado de texto o datos binarios) no resulten adecuados para este tipo de datos, por lo que se necesitan estudiar nuevos algoritmos de cifrado [41] o la manera apropiada de usar los ya existentes para lograr que estos sean eficientes y seguros al aplicarlos a datos multimedia. Desde este último punto de vista ya han surgido varias ideas al respecto, entre ellas, algunos autores han propuesto conseguir la seguridad multimedia usando la encriptación parcial o selectiva como, por ejemplo, en las referencias ([14]), ([44]) y ([70]).

Tomando en cuenta lo anterior y con el objetivo de develar las propiedades de escala presentes en imágenes que han sido cifradas, se aplicó el análisis de fluctuaciones sin tendencia bidimensional, descrito en la sección 4.1.4, a un banco de imágenes de prueba, formado por 18 imágenes originales y sus correspondientes imágenes cifradas por medio de tres esquemas de cifrado (dos de ellos están

basados en autómatas celulares de regla 90 y el otro es el AES), los cuales también fueron usados para efectuar la encriptación selectiva por planos de bits de las mismas imágenes. Los resultados muestran que mediante el exponente de escala calculado se puede inferir si una imagen cifrada es o no inteligible, pues aquellas imágenes cifradas e ininteligibles presentan un comportamiento persistente cercano al ruido $1/f$, por lo que el exponente de escala podría usarse como una medida de la calidad del contenido de la imagen cifrada. Además, siguiendo las ideas expresadas en la referencia ([70]), pero empleando herramientas diferentes, se encontró que la encriptación de los cuatro planos de bits más significativos es suficiente para proporcionar alta confidencialidad.

4.3.1 Material

En este estudio se utilizaron las dieciocho imágenes en escala de grises que se muestran en la figura 4.6. Trece de ellas tienen dimensiones de 512×512 pixeles y cinco tienen dimensiones de 1024×1024 pixeles. Estas imágenes fueron escogidas porque ellas han sido ampliamente usadas como imágenes de prueba estándar en el campo de procesamiento de imágenes. Esta base de datos de imágenes se encuentra libremente disponible en `http://sipi.usc.edu/database`, excepto las dos últimas imágenes. La primera del último par es una fotografía de la región Yardangs de Marte y puede ser descargada desde `https://solarsystem.nasa.gov`, mientras la última es una superficie Browniana fraccionaria con exponente de Hurst $H = 0.5$, la cual fue generada en MATLAB mediante el software FracLab 2.1 desarrollado por INRIA (de las siglas en francés: Institut National de Recherche en Informatique et en Automatique).

4.3.2 Sistemas de cifrado utilizado y experimento

La manera más simple de cifrar datos multimedia bi o tridimensionales es considerarlos como un flujo de datos unidimensionales y realizar el cifrado por medio de algún sistema de encriptación disponible, tal como el DES (Data Encryption Standard), el AES, el IDEA o algún otro [39]. Esta forma de cifrar datos multimedia es llamada encriptación total o completa y en este trabajo las imágenes de prueba fueron cifradas de esta manera utilizando tres esquemas de cifrado conocidos por su simplicidad, flexibilidad y seguridad. Éstos son: el ESCA, el cual es un sistema de encriptación basado en el fenómeno de sincronización de autómatas celulares con regla 90 implementado empleando una técnica matricial

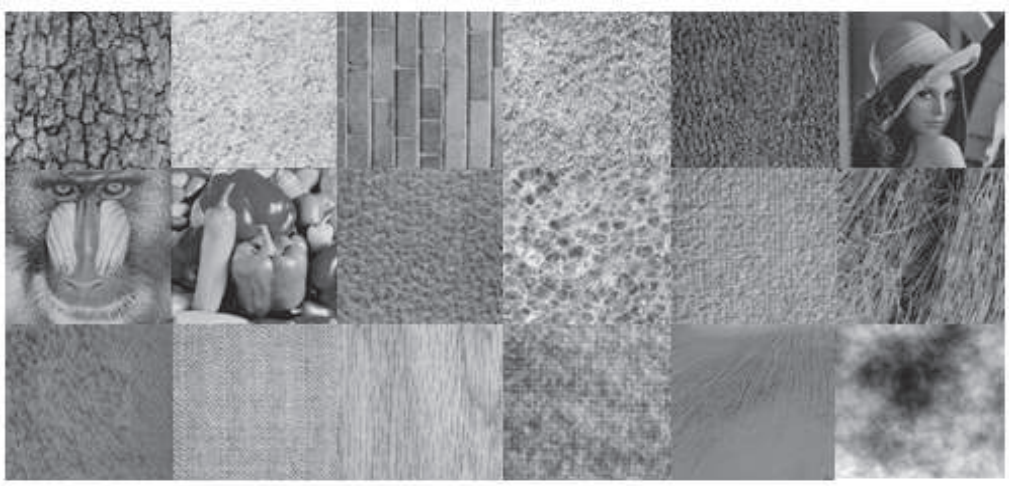


Figura 4.6: Conjunto de imágenes de prueba consideradas en este trabajo.

descrita en la referencia ([58]); una versión modificada del sistema anterior que hace su implementación matricial más flexible y mejora su seguridad, la cual se dio a conocer en ([72]); y un sistema de cifrado muy conocido, el AES en modo CBC [41]. De aquí en adelante, para mencionar estos esquemas de una manera más práctica, serán nombrados simplemente como ESCAv1, ESCAv2 y AES, respectivamente. Además, ya que la encriptación total es un proceso simple y directo que consume tiempo innecesariamente, pues el flujo de datos es cifrado en su totalidad sin contemplar la posible importancia de sólo algunas partes de los datos multimedia [39], ha sido propuesta la encriptación parcial o selectiva de las imágenes cifrando únicamente ciertas partes de los datos [14, 70] y logrando con ello reducir el tiempo computacional requerido, por lo que en esta sección también se consideró aplicar la encriptación selectiva por planos de bits.

El proceso de encriptación total para cada una de las imágenes se llevó a cabo realizando lo siguiente. En primer lugar, se consideró la representación digital de una imagen $\mathbf{I}$ como un arreglo matricial de tamaño $M \times N$ donde cada elemento de la imagen, llamado pixel, tiene cierto valor. Después, los valores de cada uno de los pixeles se ordenaron en forma vectorial acomodándolos como el elemento correspondiente a la posición en la que se encontraban al explorar la imagen de izquierda a derecha y fila por fila comenzando por el pixel superior izquierdo; dado que las imágenes con las que se trabajó están en escala de grises, los valores de

sus pixeles corresponden a un solo escalar, el cual puede estar entre 0 y 255. A continuación, cada valor del pixel fue convertido a su representación binaria tomando en cuenta 8 bits, $[b_8 \ \cdots \ b_1]$, donde b_1 es el bit menos significativo (LSB, least significant bit), mientras que b_8 es el bit más significativo (MSB, most significant bit). Finalmente, se realizó el cifrado aplicando uno de los tres esquemas de cifrado propuestos. Una ilustración describiendo este procedimiento puede verse en la figura 4.7.

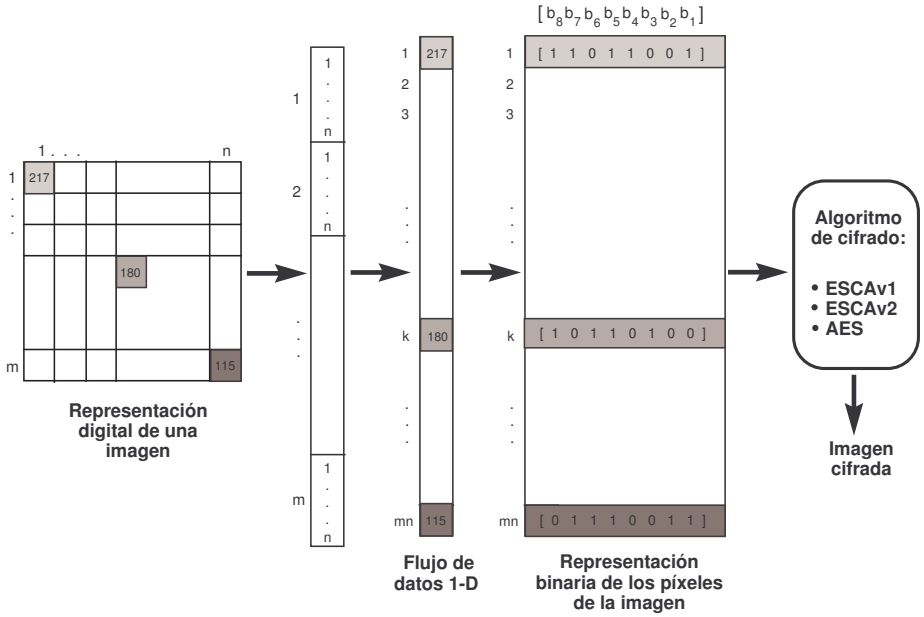


Figura 4.7: Secuencia de pasos para cifrar una imagen por medio de un sistema de cifrado convencional.

En el caso del cifrado selectivo de las imágenes se siguen los pasos anteriores, sólo que antes de realizar el cifrado de los datos, se consideró la descomposición de la imagen en planos de bits y la elección de un subconjunto de éstos a los cuales se les aplicó el algoritmo de cifrado. Los planos de bits elegidos pueden o no llevar la información más representativa de la imagen aunque comúnmente se eligen los más significativos. Cada plano de bits está asociado con una posición en la representación binaria del valor de los pixeles de la imagen, así, el plano de bits más significativo está formado por cada uno de los bits más significativos de todos

los pixeles de la imagen y el plano de bits menos significativo por los bits menos significativos de todos los pixeles de la imagen. Un ejemplo de la descomposición de una imagen en sus planos de bits se muestra en la figura 4.8, donde una imagen en escala de grises y las imágenes correspondientes a cada uno de sus ocho planos de bits pueden verse, dichas imágenes se han reconstruido considerando únicamente los valores del plano de bits indicado. Como puede apreciarse, las imágenes que corresponden a los cuatro planos de bits más significativos exhiben ciertos rasgos característicos de la imagen original lo que puede permitir distinguirla, si bien con mucho menor claridad conforme se trata de un plano menos significativo, mientras las que corresponden a los cuatro planos de bits menos significativos exhiben menos rastros de la imagen original y parecen más aleatorias.

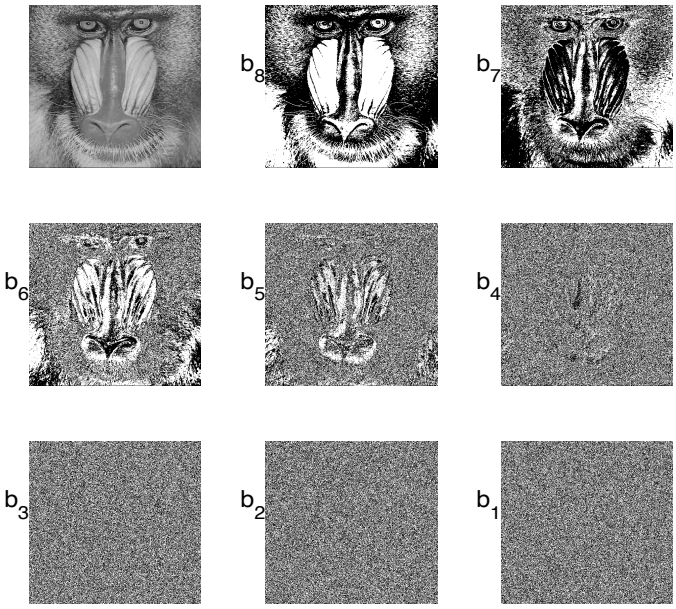


Figura 4.8: La imagen Mandrill y la reconstrucción de la misma considerando solamente los valores del plano de bits indicado $(b_8, ..., b_1)$, donde b_8 es el plano con los bits más significativos.

Un esquema que muestra la manera de realizar el cifrado selectivo de las imágenes se ilustra en la figura 4.9, como puede verse es un procedimiento muy similar al descrito para llevar a cabo el cifrado de la imagen en forma total, sólo

que se agrega el paso en el que se elige el subconjunto de planos de bits que serán cifrados. Hecho esto, los planos de bits cifrados son transmitidos junto con el resto de los planos de bits en texto plano.

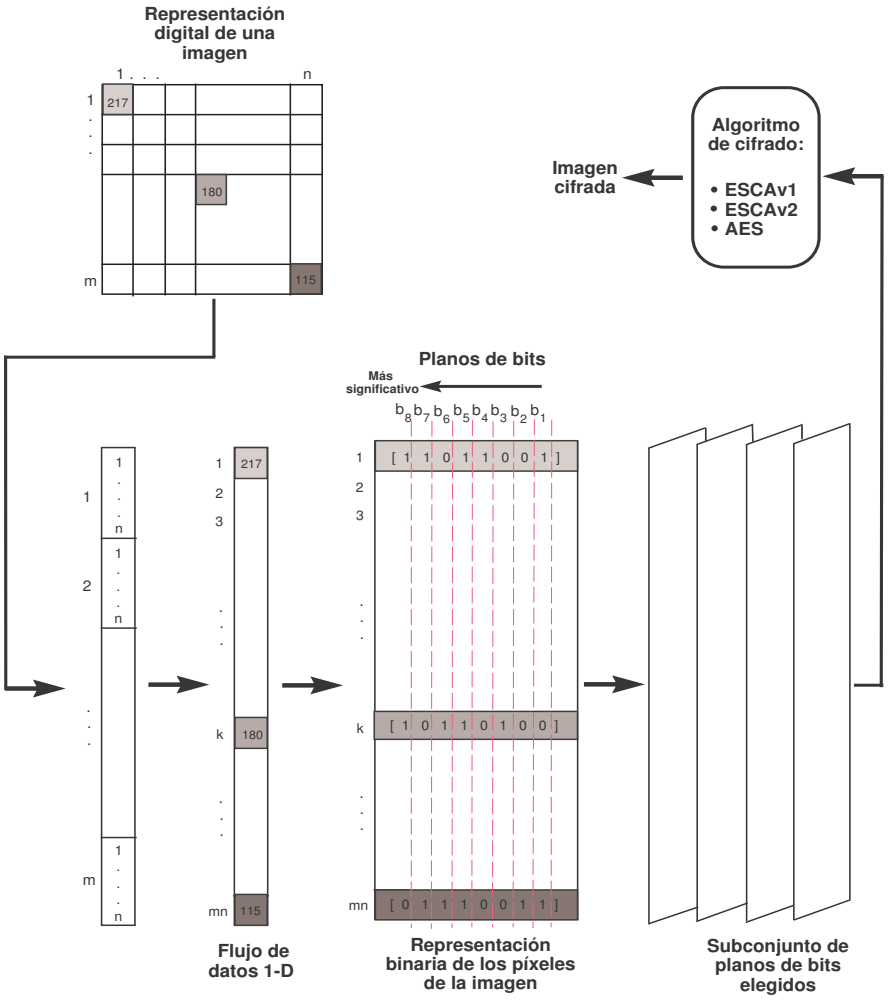


Figura 4.9: Secuencia de pasos para cifrar una imagen por medio de encriptación selectiva de planos de bits. Para el análisis de esta sección se tomó en cuenta un subconjunto de cuatro planos de bits.

4.3.3 Resultados

En esta parte se presentan los resultados obtenidos de aplicar el DFA bidimensional descrito en la subsección 4.1.4 a las dieciocho imágenes estándar en escala de grises mostradas y descritas en la subsección 4.3.1 y a las imágenes cifradas obtenidas después de aplicar los tres esquemas de cifrado elegidos. Un ejemplo que permite visualizar los resultados del desempeño del DFA bidimensional se muestra en la figura 4.10, donde se exhiben a la par de éstos, la imagen Mandrill en escala de grises y sus versiones cifradas. Se observa que la función de fluctuación $F_2(s)$ presenta un valor y comportamiento similar para los tres esquemas de cifrado en conjunto. El valor de los exponentes de escala, α, para todas las imágenes consideradas están dados en la Tabla 4.2. Ya que la mayoría de los exponentes α de las versiones cifradas son cercanos a la unidad, se puede inferir que, en general, las imágenes cifradas presentan un comportamiento persistente el cual es cercano al ruido $1/f$. Como la dimensión fractal es considerada como una métrica objetiva para medir la calidad del contenido de la imagen cifrada [41] es posible considerar el último resultado como una métrica objetiva alternativa.

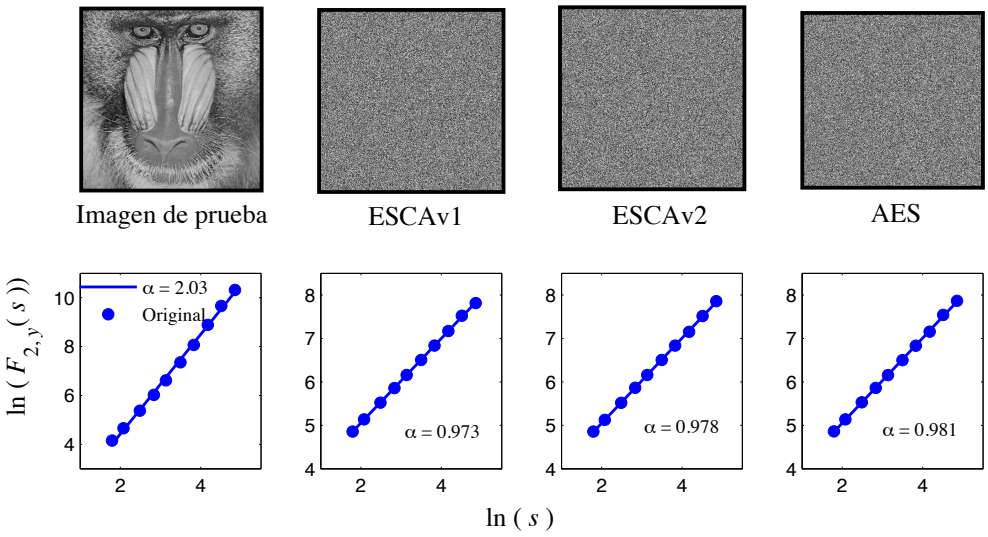


Figura 4.10: En la fila superior se muestra una de las imágenes de prueba y las diferentes versiones de cifrado, en la fila inferior se muestran los respectivos exponentes de escala obtenidos por medio de la función de fluctuación F_2.

Tabla 4.2: Valores del exponente de escala, α, obtenidos al aplicar el DFA bidimensional a las 18 imágenes de prueba y sus versiones cifradas.

Imágenes de prueba	α			
	Original	ESCAv1	ESCAv2	AES
Bark	1.8173	0.9629	0.9721	0.9745
Beach sand	1.6555	0.9946	0.9759	0.9751
Brick	1.8347	0.9954	0.9742	0.9871
Grass	1.6243	0.9894	0.9810	0.9834
Leather	1.3778	0.9623	0.9918	0.9745
Lena	2.2544	0.9826	0.9806	0.9857
Mandrill	2.0335	0.9734	0.9783	0.9808
Peppers	2.2876	0.9770	0.9633	0.9782
Pigskin	1.5552	0.9701	0.9768	0.9610
Plastic bubbles	1.9467	1.0000	0.9858	0.9884
Raffia	1.4798	0.9841	0.9486	0.9798
Straw	1.7166	0.9555	0.9713	0.9870
Water	1.5591	0.9772	0.9795	0.9918
Weave	1.3403	1.0005	0.9588	0.9723
Wood	1.6261	0.9982	0.9788	0.9804
Wool	1.8473	0.9953	0.9760	0.9714
Yardangs	1.6223	0.9583	0.9930	0.9810
fBmS	2.5114	0.9884	0.9812	0.9900

Adicionalmente, siguiendo las ideas de la referencia ([70]), se llevó a cabo una encriptación selectiva de las imágenes cifrando cuatro bits para cada pixel y a las imágenes cifradas resultantes se les aplicó el DFA bidimensional. Para realizar la prueba se eligieron cinco subconjuntos distintos de planos de bits, el primer subconjunto consta de los cuatro planos de bits más significativos, los subconjuntos siguientes se obtuvieron cambiando uno, dos, tres o los cuatro planos de bits del subconjunto inicial, comenzando por el menos significativo de éstos, por los respectivos planos de bits menos significativos. Los resultados de aplicar este tipo de cifrado considerando los subconjuntos de planos de bits anteriormente mencionados a una de la imágenes de prueba se muestran en las figuras: 4.11,

para el cifrado con el ESCAv1, 4.12 para el cifrado con el ESCAv2 y 4.13 para el cifrado con el AES.

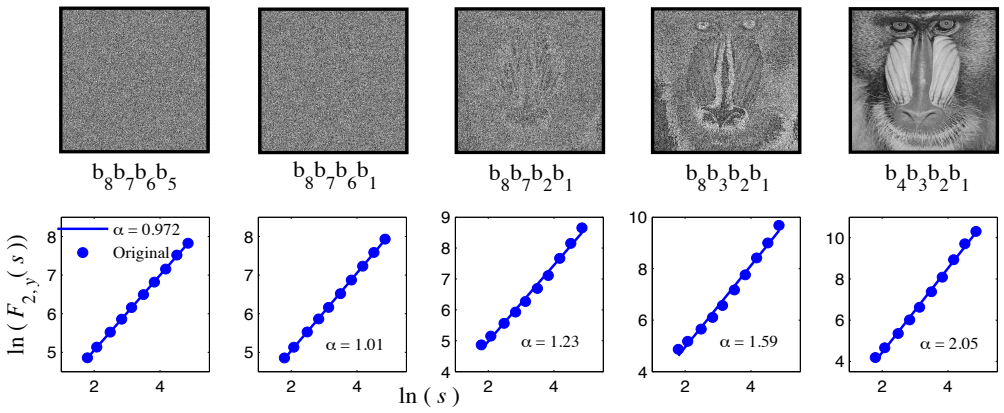


Figura 4.11: En la fila superior: imágenes obtenidas al cifrar la imagen Mandrill por medio de encriptación selectiva de cuatro planos de bits utilizando el sistema ESCAv1, en cada imagen se indican los planos de bits que fueron cifrados dejando los restantes sin cambio. En la fila inferior se da a conocer el exponente de escala proporcionado por la función de fluctuación F_2.

Los exponentes de escala, α, obtenidos para todas las imágenes y cada uno de los esquemas de cifrado considerados en este experimento se presentan en la tablas 4.3, 4.4 y 4.5. En cada una de ellas se indican los subconjuntos de planos de bits que fueron cifrados y se observa que al utilizar los sistemas de cifrado ESCAv1 y AES, los exponentes de escala de las imágenes cifradas selectivamente se acercan a los valores de los exponentes de escala de las imágenes cifradas por encriptación total conforme los planos de bits más significativos fueron cifrados, mientras que al cifrar los planos de bits menos significativos, el exponente de escala se acerca al de la imagen original. Lo anterior no sucede para el sistema de cifrado ESCAv2, en ese caso los exponentes de escala no sufrieron cambio significativo y permanecieron cercanos al de las imágenes cifradas mediante cifrado total. De hecho, si se observan las figuras 4.11, 4.12 y 4.13 puede apreciarse que tanto en la primera como en la última, alguna información de la imagen original es visible cuando se cifran los tres últimos subconjuntos de planos de bits, los cuales tienen al menos dos de los planos de bits menos significativos y corresponden a los subconjuntos

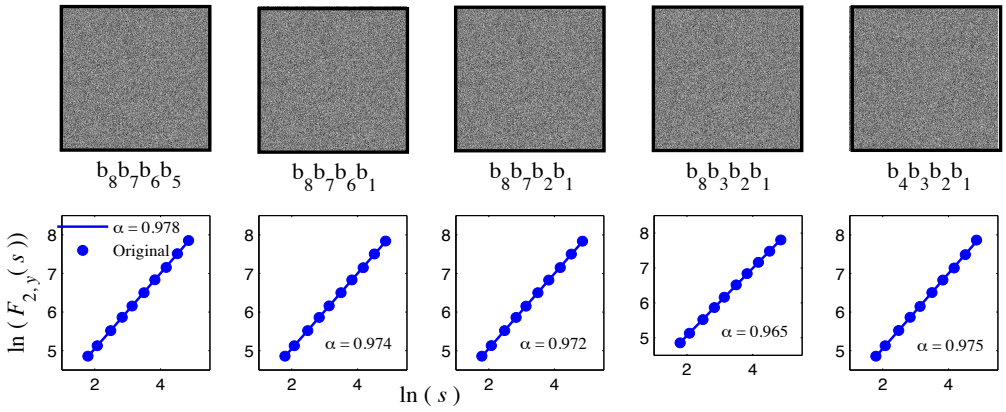


Figura 4.12: En la fila superior: imágenes obtenidas al cifrar la imagen Mandrill por medio de encriptación selectiva de cuatro planos de bits utilizando el sistema ESCAv2, en cada imagen se indican los planos de bits que fueron cifrados dejando los restantes sin cambio. En la fila inferior se da a conocer el exponente de escala proporcionado por la función de fluctuación F_2.

formados por los planos $b_8b_7b_2b_1$, $b_8b_3b_2b_1$ y $b_4b_3b_2b_1$; esto no sucede en la figura 4.12, en la que independientemente de los subconjuntos cifrados no logra verse información inteligible. Estos resultados ilustran que el sistema de encriptación ESCAv2 puede proporcionar alta confidencialidad en el caso del cifrado parcial. Además, ya que solamente se cifran la mitad de los datos, se obtiene una mejora en el tiempo de ejecución, pues éste se reduce.

Como resultado de este trabajo se derivó el artículo:

- Vargas-Olmos,C., Murguía, J. S., Ramírez-Torres, M. T., Mejía Carlos, M., Rosu, H. C. y González-Aguilar, H. **Two-dimensional DFA scaling analysis applied to encrypted images**. En: *International Journal of Modern Physics C*. 2015, vol. 26, no. 8, pp. 1550093.

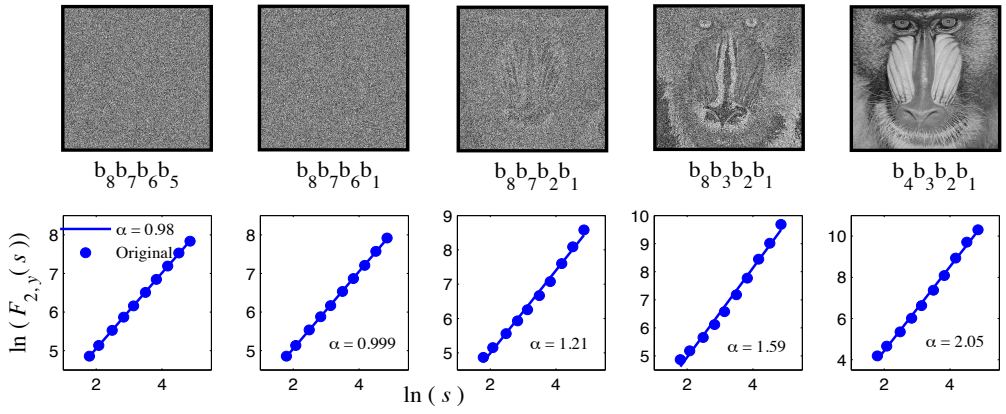


Figura 4.13: En la fila superior: imágenes obtenidas al cifrar la imagen Mandrill por medio de encriptación selectiva de cuatro planos de bits utilizando el sistema AES, en cada imagen se indican los planos de bits que fueron cifrados dejando los restantes sin cambio. En la fila inferior se da a conocer el exponente de escala proporcionado por la función de fluctuación F_2.

4.3.4 Conclusiones

El algoritmo para calcular el DFA bidimensional fue utilizado para determinar el comportamiento singular de un conjunto de imágenes en escala de grises cifradas tanto por encriptación total como selectiva aplicando tres esquemas de cifrado. Las imágenes obtenidas al aplicar cada uno de los esquemas de encriptación de manera total no exhiben características de la imagen original mostrándose aleatorias y tienen un exponente de escala similar cercano a la unidad, es decir, al ruido $1/f$. Ahora bien, realizar el cifrado de las imágenes por medio de encriptación selectiva permitió corroborar que aquellas imágenes cuyos planos de bits menos significativos han sido cifrados exhiben características que develan la imagen original y poseen un exponente de escala que se acerca al que tiene la imagen original, mientras que aquellas imágenes cuyos planos de bits más significativos han sido cifrados son ininteligibles y presentan un exponente de escala con valor cercano a uno, lo cual sugiere que el exponente de escala puede ser usado como una medida apropiada y objetiva de la calidad de los esquemas de encriptación. Dado el comportamiento de los sistemas de cifrado utilizados, se cree que un buen algoritmo de cifrado de

imágenes debe mantener el mismo exponente de escala, cercano a la unidad, en las imágenes con él cifradas a pesar de haber aplicado un cifrado selectivo, como aquí fue el caso del ESCAv2.

Tabla 4.3: Valores de los exponentes de escala, α, obtenidos después de aplicar el DFA bidimensional a las dieciocho imágenes de prueba cifradas selectivamente por medio del sistema ESCAv1.

Imágenes de prueba	α				
	$b_8b_7b_6b_5$	$b_8b_7b_6b_1$	$b_8b_7b_2b_1$	$b_8b_3b_2b_1$	$b_4b_3b_2b_1$
Bark	0.9622	0.9672	1.0337	1.3347	1.8150
Beach sand	0.9973	1.0023	1.1066	1.3791	1.6508
Brick	1.0001	1.0234	1.2576	1.6142	1.8288
Grass	0.9906	0.9952	1.0169	1.2062	1.6228
Leather	0.9646	0.9674	0.9937	1.1585	1.3769
Lena	0.9867	1.1250	1.3978	1.7999	2.2334
Mandrill	0.9718	1.0076	1.2347	1.5863	2.0460
Peppers	0.9702	1.1354	1.3487	1.7782	2.2537
Pigskin	0.9700	0.9692	1.0134	1.3231	1.5495
Plastic bubbles	0.9999	1.0033	1.1693	1.5566	1.9423
Raffia	0.9842	0.9872	1.0497	1.2177	1.4755
Straw	0.9543	0.9609	1.0253	1.3036	1.7143
Water	0.9745	0.9754	1.0885	1.3379	1.5496
Weave	1.0010	0.9992	1.0127	1.0634	1.3365
Wood	0.9976	1.0514	1.2495	1.2938	1.6204
Wool	0.9958	1.0000	1.0636	1.4865	1.8386
Yardangs	0.9599	1.0680	1.2584	1.4779	1.6275
fBmS	0.9973	1.1301	1.5487	1.8704	2.4288

Tabla 4.4: Valores de los exponentes de escala, α, obtenidos después de aplicar el DFA bidimensional a las dieciocho imágenes de prueba cifradas selectivamente por medio del sistema ESCAv2.

Imágenes de prueba	α				
	$b_8b_7b_6b_5$	$b_8b_7b_6b_1$	$b_8b_7b_2b_1$	$b_8b_3b_2b_1$	$b_4b_3b_2b_1$
Bark	0.9700	0.9690	0.9734	0.9660	0.9825
Beach sand	0.9738	0.9711	0.9732	0.9800	0.9831
Brick	0.9748	0.9794	0.9824	0.9783	0.9721
Grass	0.9812	0.9823	0.9841	0.9939	0.9968
Leather	0.9936	0.9924	0.9789	0.9716	0.9458
Lena	0.9800	0.9742	0.9750	0.9769	0.9780
Mandrill	0.9779	0.9736	0.9724	0.9653	0.9745
Peppers	0.9630	0.9643	0.9611	0.9588	0.9773
Pigskin	0.9768	0.9758	0.9766	0.9750	0.9738
Plastic bubbles	0.9867	0.9878	0.9928	0.9908	0.9763
Raffia	0.9484	0.9510	0.9504	0.9727	0.9582
Straw	0.9722	0.9738	0.9744	0.9768	0.9606
Water	0.9796	0.9825	0.9869	0.9956	0.9881
Weave	0.9606	0.9636	0.9594	0.9711	0.9701
Wood	0.9781	0.9760	0.9751	0.9841	0.9777
Wool	0.9768	0.9760	0.9709	0.9610	0.9744
Yardangs	0.9926	0.9926	0.9943	0.9779	0.9983
fBmS	0.9828	0.9845	0.9843	0.9914	0.9834

Tabla 4.5: Valores de los exponentes de escala, α, obtenidos después de aplicar el DFA bidimensional a las dieciocho imágenes de prueba cifradas selectivamente por medio del sistema AES.

Imágenes de prueba	α				
	$b_8b_7b_6b_5$	$b_8b_7b_6b_1$	$b_8b_7b_2b_1$	$b_8b_3b_2b_1$	$b_4b_3b_2b_1$
Bark	0.9828	0.9775	1.0422	1.3340	1.8149
Beach sand	0.9851	1.0006	1.1011	1.3767	1.6509
Brick	0.9924	1.0339	1.2610	1.6134	1.8286
Grass	0.9962	0.9774	1.0186	1.2051	1.6228
Leather	0.9889	0.9932	1.0101	1.1601	1.3764
Lena	0.9783	1.1135	1.4007	1.8006	2.2331
Mandrill	0.9797	0.9992	1.2076	1.5908	2.0458
Peppers	0.9790	1.1253	1.3367	1.7752	2.2546
Pigskin	0.9849	1.0030	1.0315	1.3288	1.5499
Plastic bubbles	0.9693	0.9918	1.1504	1.5570	1.9425
Raffia	0.9570	0.9985	1.0683	1.2287	1.4751
Straw	0.9697	0.9754	1.0478	1.3058	1.7140
Water	0.9805	0.9858	1.0968	1.3365	1.5489
Weave	0.9747	0.9756	1.0000	1.0293	1.3357
Wood	0.9814	1.0517	1.2443	1.2779	1.6197
Wool	0.9753	0.9917	1.0615	1.4848	1.8389
Yardangs	1.0088	1.0814	1.2683	1.4786	1.6274
fBmS	0.9944	1.1268	1.5504	1.8701	2.5114

4.4 W-DFA adaptado a imágenes y aplicado a imágenes cifradas

Después de determinar en la sección 4.3 que para las imágenes que han sido cifradas, ya sea mediante encriptación total o selectiva, un valor del exponente de escala cercano a la unidad (correspondiente al ruido $1/f$), obtenido mediante el DFA bidimensional, garantiza la aleatoriedad de los pixeles de la imagen cifrada pues en ese caso la imagen es ininteligible para el observador; se quiso ampliar el análisis realizado en la misma con el fin de examinar el comportamiento del exponente de escala cuando es utilizado otro método para calcularlo y cuando son usados otros subconjuntos de planos de bits para realizar el cifrado selectivo de las imágenes de prueba. Para ello, en esta sección, primero se determinó el exponente de escala del conjunto de imágenes de prueba empleado en la sección 4.3 y que puede verse en la figura 4.6 por medio del W-DFA adaptado a imágenes descrito en la subsección 4.1.3. Además, se extendió el análisis considerando más subconjuntos de planos de bits para realizar el cifrado selectivo y también se averiguó si el cifrado selectivo de planos de bits con el sistema de encriptación ESCAv2 es exitoso al cifrar al menos cuatro planos de bits o si sigue siéndolo al utilizar una menor cantidad de planos de bits conservando una alta confidencialidad, a este respecto se calculó también el exponente de escala de imágenes cifradas por medio de encriptación selectiva de tres planos de bits. Adicionalmente, tomando en cuenta que la evaluación de la seguridad de una imagen cifrada requiere la evaluación de su seguridad criptográfica y de su seguridad perceptual, refiriéndose la primera a la habilidad del esquema de encriptación para resistir técnicas de criptoanálisis tales como: ataque diferencial, ataques relacionados a la llave y ataques estadísticos, entre otros; mientras la segunda se refiere a la alta degradación visual que presenta el contenido de la imagen haciéndola ininteligible a la percepción humana [41], aquí, en base a los resultados obtenidos, se presenta el exponente de escala, α, como una potencial métrica objetiva para medir la seguridad perceptual de una imagen cifrada. Esto es importante porque mientras una métrica subjetiva está basada en la inspección visual la cual es llevada a cabo por personas que actúan como árbitros cuyo juicio depende de decisiones personales tales como estado emocional o condición física; la métrica objetiva es consistente, eficiente y robusta, está definida matemáticamente y puede ser usada automáticamente además de consumir menos tiempo. Finalmente, para concluir el análisis y establecer una

comparación de los resultados obtenidos, se determinó la razón pico señal a ruido o PSNR (del inglés: Peak Signal to Noise Ratio) de las imágenes cifradas.

4.4.1 Material y experimento

Como ya se ha mencionado, para llevar a cabo el análisis de esta sección se utilizó el banco de imágenes de prueba descrito en la subsección 4.3.1. Respecto al experimento, éste sigue la secuencia del realizado en la sección 4.3. Primero se llevó a cabo el cifrado total de las imágenes (cuyo procedimiento es descrito en la subsección 4.3.2 y puede ser visto rápidamente en la figura 4.7) y después el cifrado parcial mediante selección de planos de bits (también descrito en la subsección 4.3.2 y representado en la figura 4.9), aunque aquí, para llevar a cabo el cifrado selectivo de las imágenes, en vez de cinco, se eligieron ocho subconjuntos de cuatro planos de bits y aparte también se eligió otro grupo de ocho subconjuntos de tres planos de bits. En cuanto a los esquemas de cifrado con los que se trabajó, éstos fueron ESCAv1, ESCAv2 y el AES en modo RBT [50].

El exponente de escala para las imágenes se determinó calculando el W-DFA adaptado a imágenes, haciendo el análisis en dos orientaciones: a $0°$ de norte a sur y a $90°$ de este a oeste, la *wavelet* empleada fue la db-4 de MATLAB, la cual tiene ocho coeficientes y retiene la tendencia polinomial cúbica de los datos [48] proporcionando así una determinación más exacta de sus características de escala, lo cual está de acuerdo con las conclusiones de las referencias ([64]) y ([65]).

4.4.2 Resultados

En la figura 4.14 se muestra como ejemplo uno de los resultados obtenidos al aplicar el W-DFA adaptado a imágenes usando la función *wavelet* db-4; este ejemplo corresponde a la imagen Mandrill y a sus versiones cifradas por encriptación total, para hacer el análisis se consideraron ambas orientaciones, norte-sur, $0°$, y este-oeste, $90°$. En dicha figura se observa que los valores del exponente de escala α proporcionados por los tres sistemas de cifrado utilizados presentan un comportamiento similar en ambas direcciones.

Todos los resultados de los exponentes de escala obtenidos mediante el W-DFA adaptado a imágenes para el conjunto de imágenes de prueba, así como para sus versiones cifradas están dados en las tablas: 4.6, para la orientación a $0°$, y 4.7, para la orientación a $90°$. En estos resultados es de notar que la mayoría de los exponentes de escala de las imágenes cifradas, en cualquiera de las dos

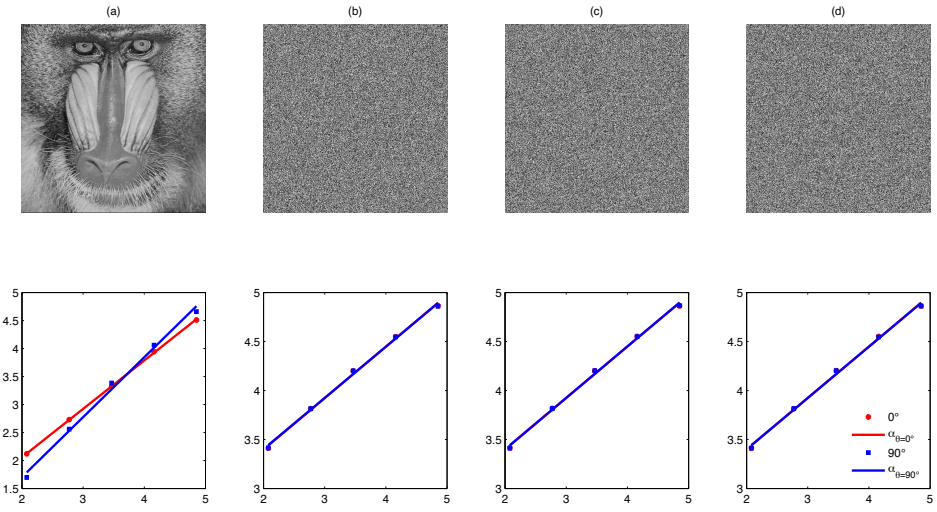


Figura 4.14: En la fila superior: (a) la imagen Mandrill, y sus versiones cifradas con: (b) el sistema ESCAv1, (c) el sistema ESCAv2, y (d) el sistema AES. En la fila inferior las respectivas funciones de fluctuación y los exponentes de escala obtenidos por el método W-DFA adaptado a imágenes.

orientaciones ($\alpha_{0°}$ o $\alpha_{90°}$), tienen un valor cercano a 0.5, el cual sugiere que las imágenes cifradas presentan un comportamiento cercano al ruido Gaussiano.

En el caso de la encriptación selectiva por planos de bits, ésta se llevó a cabo eligiendo dos grupos con diferentes subconjuntos de cuatro y tres planos de bits para cada una de las imágenes. En cada uno de los grupos el primer subconjunto se formó por los planos de bits más significativos y, para tomar en cuenta todas las posibles combinaciones, los subconjuntos siguientes se conformaron considerando como su primer elemento al plano de bits correspondiente al realizar un desplazamiento circular de un plano de bits a la derecha en el subconjunto anterior y eligiendo el resto de los elementos del subconjunto consecutivamente, esto se hizo hasta obtener ocho subconjuntos. De esta manera, los subconjuntos con cuatro planos de bits tomados en cuenta fueron: $b_8b_7b_6b_5$, $b_7b_6b_5b_4$, $\ldots$, $b_4b_3b_2b_1$, $b_3b_2b_1b_8$, $b_2b_1b_8b_7$, $b_1b_8b_7b_6$. De igual forma, los subconjuntos con tres planos de bits con los que se trabajó fueron: $b_8b_7b_6$, $b_7b_6b_5$, $\ldots$, $b_3b_2b_1$, $b_2b_1b_8$, $b_1b_8b_7$. Lo cual permitió analizar tanto subconjuntos

Tabla 4.6: Valores del exponente de escala α obtenidos de aplicar el W-DFA adaptado a imágenes en la orientación $0°$ a las dieciocho imágenes de prueba y sus versiones cifradas.

Imágenes de prueba	$\alpha_{0°}$			
	Original	ESCAv1	ESCAv2	AES
Bark	1.3328	0.5239	0.5218	0.5245
Beach sand	1.2326	0.5109	0.5111	0.5126
Brick	1.0595	0.5257	0.5227	0.5235
Grass	1.2586	0.5109	0.5123	0.5104
Leather	1.2498	0.5224	0.5243	0.5260
Lena	1.3219	0.5253	0.5255	0.5244
Mandrill	0.8647	0.5253	0.5240	0.5247
Peppers	1.5540	0.5225	0.5239	0.5247
Pigskin	1.2370	0.5246	0.5238	0.5249
Plastic bubbles	1.2790	0.5111	0.5104	0.5138
Raffia	1.2383	0.5240	0.5245	0.5262
Straw	1.4725	0.5273	0.5233	0.5209
Water	1.5743	0.5248	0.5250	0.5258
Weave	1.1953	0.5254	0.5248	0.5248
Wood	1.4895	0.5240	0.5234	0.5244
Wool	1.2503	0.5273	0.5252	0.5218
Yardangs	1.0099	0.5121	0.5110	0.5133
fBm	1.4099	0.5107	0.5123	0.5122

de planos de bits que preservan la información más representativa de la imagen y otros que no.

Al igual que en la encriptación total, los resultados de aplicar el W-DFA adaptado a imágenes a las imágenes cifradas por encriptación selectiva en ambas orientaciones son muy semejantes, esto puede apreciarse en la figura 4.15 para los subconjuntos de cuatro planos de bits y en la figura 4.16 para los subconjuntos de tres planos de bits; por lo cual podría aplicarse indistintamente el análisis en una sola de las orientaciones aquí consideradas.

Tabla 4.7: Valores del exponente de escala α obtenidos de aplicar el W-DFA adaptado a imágenes en la orientación $90°$ a las dieciocho imágenes de prueba y sus versiones cifradas.

Imágenes de prueba	$\alpha_{90°}$			
	Original	ESCAv1	ESCAv2	AES
Bark	1.4417	0.5229	0.5269	0.5251
Beach sand	1.2303	0.5118	0.5112	0.5121
Brick	1.3764	0.5232	0.5253	0.5257
Grass	1.2041	0.5112	0.5118	0.5119
Leather	1.1360	0.5250	0.5257	0.5273
Lena	1.3800	0.5251	0.5227	0.5274
Mandrill	1.0709	0.5229	0.5257	0.5240
Peppers	1.6164	0.5260	0.5225	0.5246
Pigskin	1.3980	0.5213	0.5235	0.5253
Plastic bubbles	1.2990	0.5121	0.5121	0.5132
Raffia	1.4390	0.5207	0.5232	0.5238
Straw	1.1291	0.5245	0.5239	0.5234
Water	1.0973	0.5214	0.5241	0.5243
Weave	1.2038	0.5241	0.5208	0.5232
Wood	1.0382	0.5224	0.5220	0.5244
Wool	1.2571	0.5252	0.5239	0.5257
Yardangs	0.9892	0.5103	0.5145	0.5110
fBm	1.4061	0.5118	0.5115	0.5115

Al visualizar los resultados puede notarse que para los sistemas de encriptación ESCAv1 y AES, los valores del exponente de escala de las imágenes cifradas se acercan a los valores del exponente de escala de las imágenes originales conforme se han cifrado los subconjuntos con los planos de bits menos significativos, lo cual sucede para los subconjuntos quinto y sexto dependiendo si se han elegido subconjuntos con cuatro o tres planos de bits respectivamente; mientras que para el sistema de encriptación ESCAv2 el exponente de escala permanece sin cambio significativo y cercano a 0.5. Por lo tanto, estos resultados ilustran que este último sistema de encriptación puede proporcionar alta confidencialidad cuando se lleva

a cabo la encriptación selectiva por planos de bits. Un ejemplo, para ver más en detalle este comportamiento se presenta en las figuras 4.17 a 4.19, donde se muestran las imágenes obtenidas después de aplicar el cifrado selectivo eligiendo subconjuntos de tres planos de bits a una de las imágenes de prueba. Puede observarse que en algunas de las imágenes, cuando se utilizan los esquemas ESCAv1 y AES, hay suficiente información estructural que permite percibir la imagen original. De hecho, para estos esquemas, solamente cuando el primer subconjunto de planos de bits es cifrado, el cual contiene los tres planos de bits más significativos, no puede apreciarse ninguna información estructural.

4.4.3 Razón pico señal a ruido

La evaluación de la calidad de las imágenes (IQA, del inglés: image quality assessment) juega un papel de importancia fundamental en diversas aplicaciones del procesamiento de imágenes, donde el objetivo de los métodos IQA es evaluar automáticamente la calidad de las imágenes de acuerdo a la apreciación que se logra con el sentido de la vista humano de un observador promedio [51]. Para ello se han propuesto y desarrollado varias métricas objetivas que, en base a la disponibilidad que tengan de una imagen de referencia, pueden clasificarse como de referencia completa, sin referencia y de referencia reducida [51, 82, 96]. Una de las métricas de referencia completa que ha sido usada frecuentemente para evaluar la pérdida de calidad que han sufrido imágenes sometidas a operaciones tales como la compresión, la remoción de ruido y la transmisión es la razón pico señal a ruido (PSNR, del inglés Peak Signal-to-Noise Ratio) [30], la cual también ha sido usada normalmente como una métrica objetiva de la calidad de imágenes cifradas [14, 30, 41, 70, 91] pues indica los cambios en los valores de los pixeles entre la imagen plana y la imagen cifrada [3]. La PSNR se mide en decibeles (dB) y está definida matemáticamente por:

$$PSNR = 10\log_{10}\frac{L^2}{MSE}, \tag{4.24}$$

donde $L = (2^B - 1)$ es el número de niveles de gris de los pixeles de la imagen, siendo B el número de bits y MSE el error cuadrático medio, definido como

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\|\mathbf{I}(m,n) - \hat{\mathbf{I}}(m,n)\|, \tag{4.25}$$

donde $\mathbf{I}$ es la imagen original o plana de tamaño $M \times N$ e $\hat{\mathbf{I}}$ es la imagen reconstruida o cifrada. Se considera que entre más alto sea el valor de la PSNR, la imagen

reconstruida tiene mejor calidad pues indica más semejanza con la original por lo que en el caso de imágenes cifradas un valor muy bajo de la PSNR es un indicativo de un buen algoritmo de cifrado [41] y representa una mejor calidad de la encriptación [3].

Con el objetivo de medir la pérdida de calidad de las imágenes cifradas mediante los esquemas de encriptación selectiva aquí utilizados se calculó la PSNR de las mismas y los resultados se exhiben en las figuras 4.20 y 4.21 para los subconjuntos cifrados de cuatro y tres planos de bits respectivamente. Puede apreciarse que los resultados obtenidos con esta métrica presentan la misma tendencia que los exponentes de escala (figuras 4.15 y 4.16). Sin embargo, en ([79]) se calculó la PSNR para evaluar la calidad de las imágenes cifradas y se encontró un desajuste entre los valores numéricos y la calidad visual percibida y en ([81]) se encontró que los valores de la PSNR no trabajan apropiadamente para evaluar la seguridad visual de algunos algoritmos de encriptación. Esto significa que algunas veces dicha métrica no puede reflejar acertadamente la seguridad visual de las imágenes cifradas.

Como resultado del análisis llevado a cabo en esta sección se publicó el artículo:

- Vargas-Olmos, C., Murguía, J. S., Ramírez-Torres, M. T., Mejía Carlos, M., Rosu, H. C. y González-Aguilar H. **Perceptual security of encrypted images based on wavelet scaling analysis**. En: *Physica A*. 2016, vol. 456, pp. 22-30.

4.4.4 Conclusiones

En esta sección se ha analizado el comportamiento de escala de un grupo de imágenes en tonos de gris que han sido encriptadas a través de tres esquemas de cifrado aplicando encriptación total y selectiva. El exponente de escala ha sido calculado usando el método W-DFA adaptado a imágenes y los resultados muestran que cuando el cifrado total es aplicado, las imágenes son ininteligibles y presentan un exponente de escala cercano a 0.5, que es el correspondiente al del ruido gaussiano. Dicho valor se mantiene al aplicar el cifrado selectivo a las imágenes si se eligen los planos de bits más significativos; en cambio, el valor del exponente de escala se acerca más al de la imagen original conforme se eligen los planos de bits menos significativos.

A pesar del hecho de que la PSNR es algunas veces considerada como una métrica objetiva de imágenes cifradas, es más adecuada para detectar la calidad

(relacionada con la degradación que sufre la imagen) que la ininteligibilidad de las mismas [41], además se ha encontrado que la PSNR presenta en algunas ocasiones inconvenientes para aseverar la seguridad visual objetiva [81]. Por esta razón, se afirma que el valor del exponente de escala el cual es cercano a ese del ruido Gaussiano (0.5), cuando el método W-DFA adaptado a imágenes ha sido utilizado, puede ser una buena elección al ser escogido como una medida objetiva de la seguridad perceptual de imágenes cifradas, pues está estrechamente relacionado con sus características de ininteligibilidad. Esto es porque cuando tales valores ocurren, las imágenes cifradas no revelan ninguna información que pueda permitir distinguir la imagen original. Además, aunque la PSNR de las imágenes cifradas tienen la misma tendencia, es una métrica referenciada, por lo que son necesarias ambas imágenes, la original y la cifrada para hacer los cálculos apropiados. Lo cual no es necesario para determinar el valor del exponente de escala, el cual puede ser calculado sin tener la imagen original, por lo que sería una métrica no referenciada con las ventajas que ello supone.

Sin embargo, aunque la imagen cifrada presente un exponente de escala, alrededor del 0.5, con el cual se afirme que la imagen es completamente ininteligible y esto confirme su seguridad perceptual, no se puede garantizar plenamente que una imagen cifrada que presente tal valor sea absolutamente inmune a cualquier tipo de ataque, porque si bien es cierto que el AES y el ESCAv2 son muy confiables con respecto a los ataques de texto claro cuando un esquema de cifrado completo fue aplicado a la imagen, esto no es así para el ESCAv1.

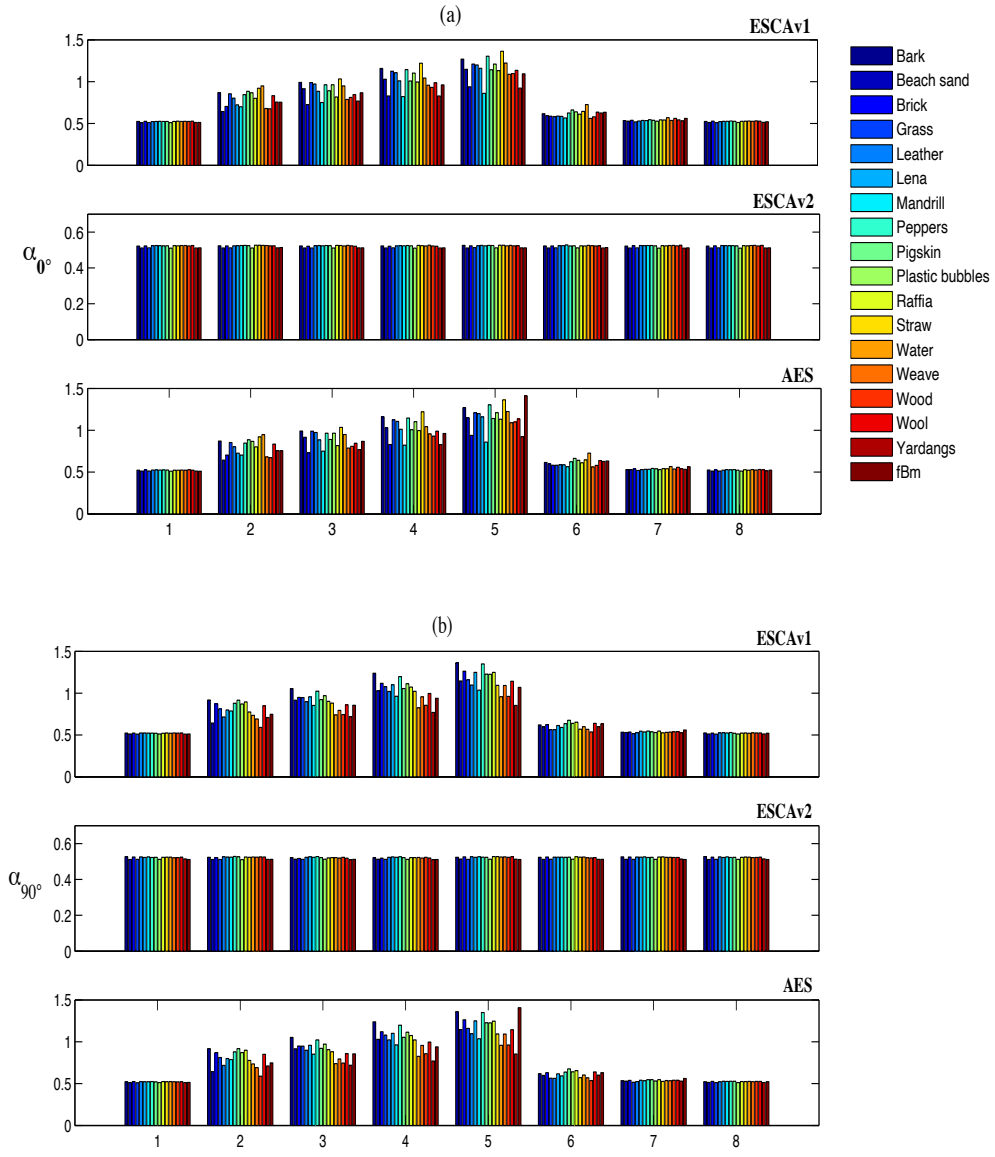


Figura 4.15: Exponentes de escala de las imágenes cifradas considerando ocho subconjuntos de cuatro planos de bits (en las gráficas, de izquierda a derecha: $b_8b_7b_6b_5$, $b_7b_6b_5b_4$, $b_6b_5b_4b_1$, $b_5b_4b_3b_2$, $b_4b_3b_2b_1$, $b_3b_2b_1b_8$, $b_2b_1b_8b_7$, $b_1b_8b_7b_6$) cuando el algoritmo W-DFA es aplicado. Es de notar el comportamiento similar que tienen los exponentes de escala en ambas orientaciones independientemente del esquema de cifrado.

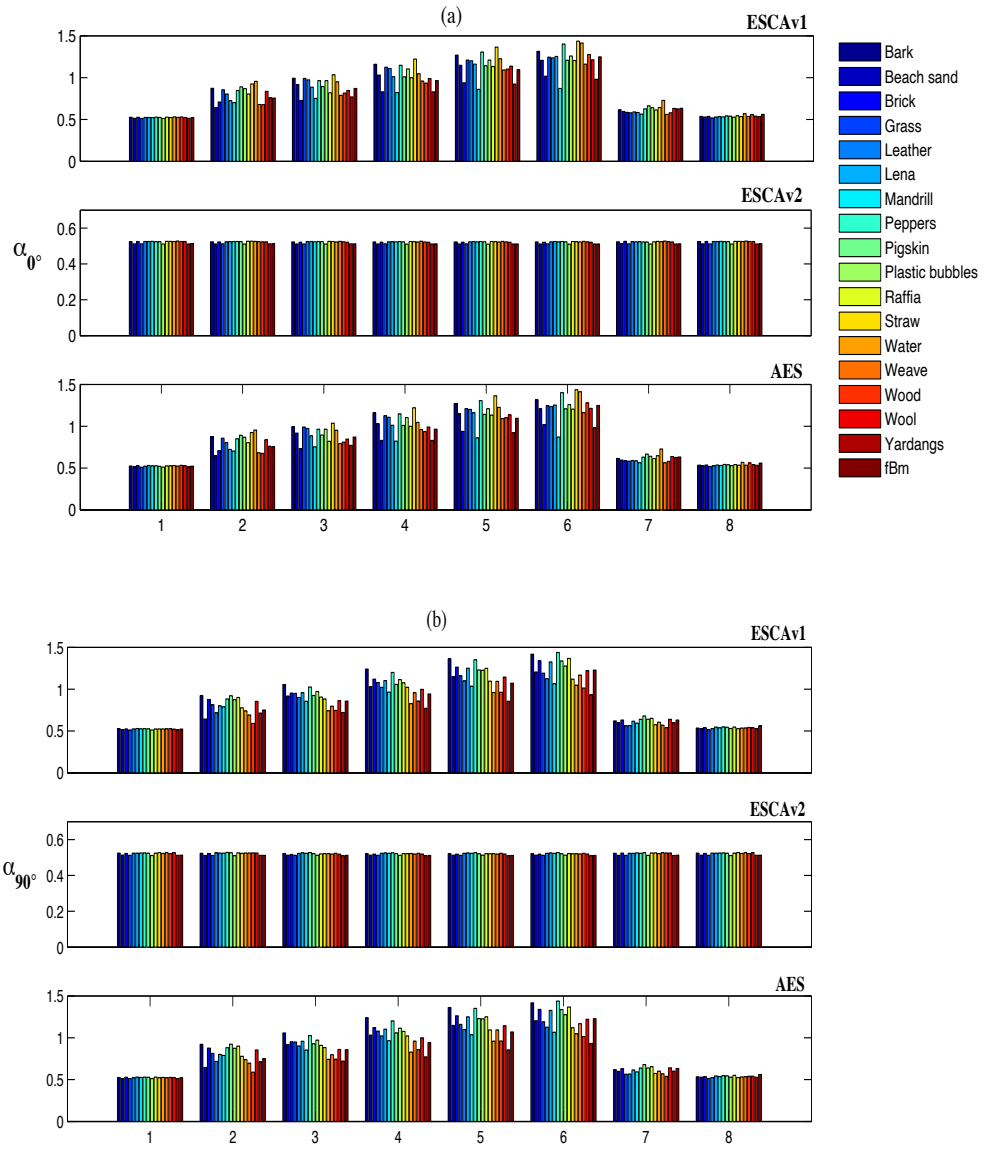


Figura 4.16: Exponentes de escala de las imágenes cifradas considerando ocho subconjuntos de tres planos de bits (en las gráficas, de izquierda a derecha: $b_8b_7b_6$, $b_7b_6b_5$, $b_6b_5b_4$, $b_5b_4b_3$, $b_4b_3b_2$, $b_3b_2b_1$, $b_2b_1b_8$, $b_1b_8b_7$) cuando el algoritmo W-DFA es aplicado. Es de notar el comportamiento similar que tienen los exponentes de escala en ambas orientaciones independientemente del esquema de cifrado.

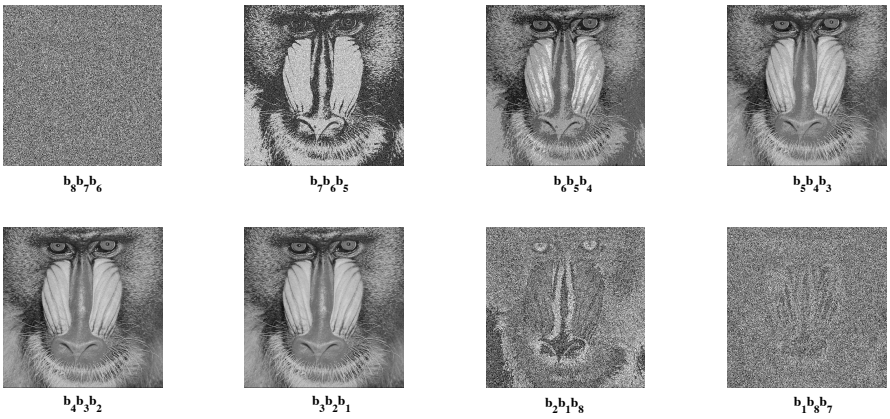


Figura 4.17: Encriptación selectiva de la imagen Mandrill considerando subconjuntos de tres planos de bits y el esquema de cifrado ESCAv1. Solamente el cifrado del primer subconjunto no revela detalles de la imagen original.

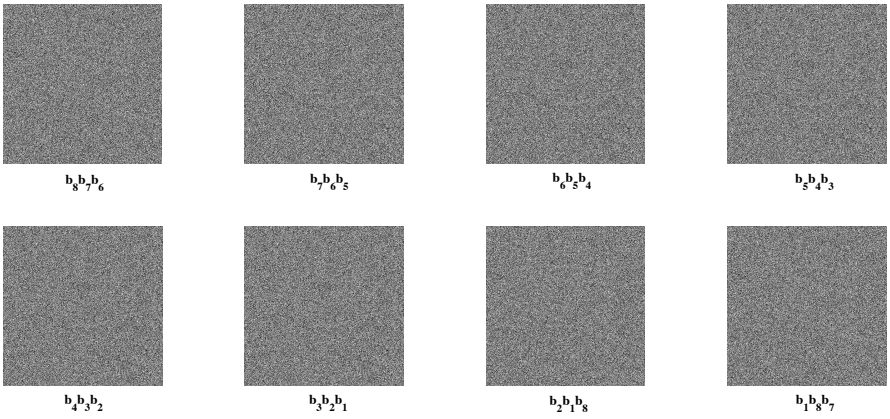


Figura 4.18: Encriptación selectiva de la imagen Mandrill considerando subconjuntos de tres planos de bits y el esquema de cifrado ESCAv2. El cifrado de cualquier subconjunto (independientemente de los planos de bits contenidos en él) no revela detalles de la imagen original.

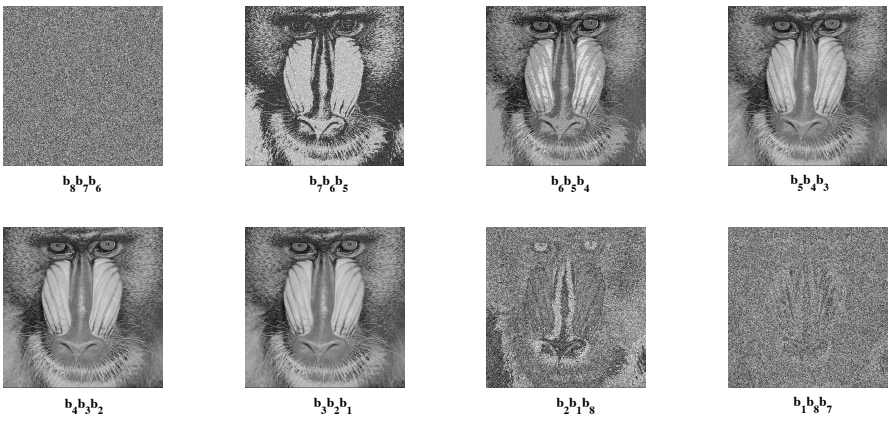


Figura 4.19: Encriptación selectiva de la imagen Mandrill considerando subconjuntos de tres planos de bits y el esquema de cifrado AES. Solamente el cifrado del primer subconjunto no revela detalles de la imagen original.

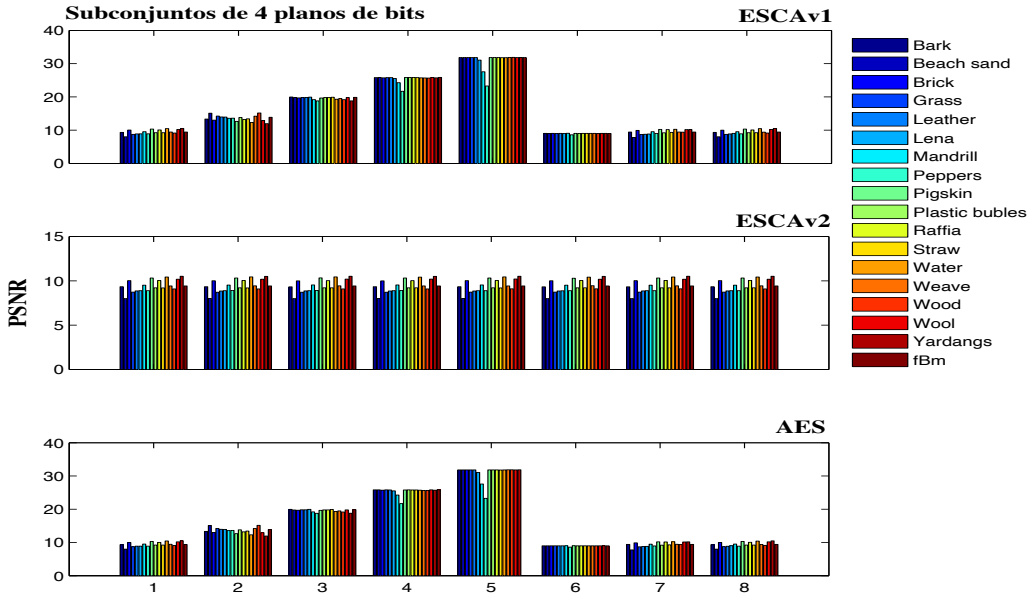


Figura 4.20: PSNR de las imágenes cifradas considerando cuatro planos de bits.

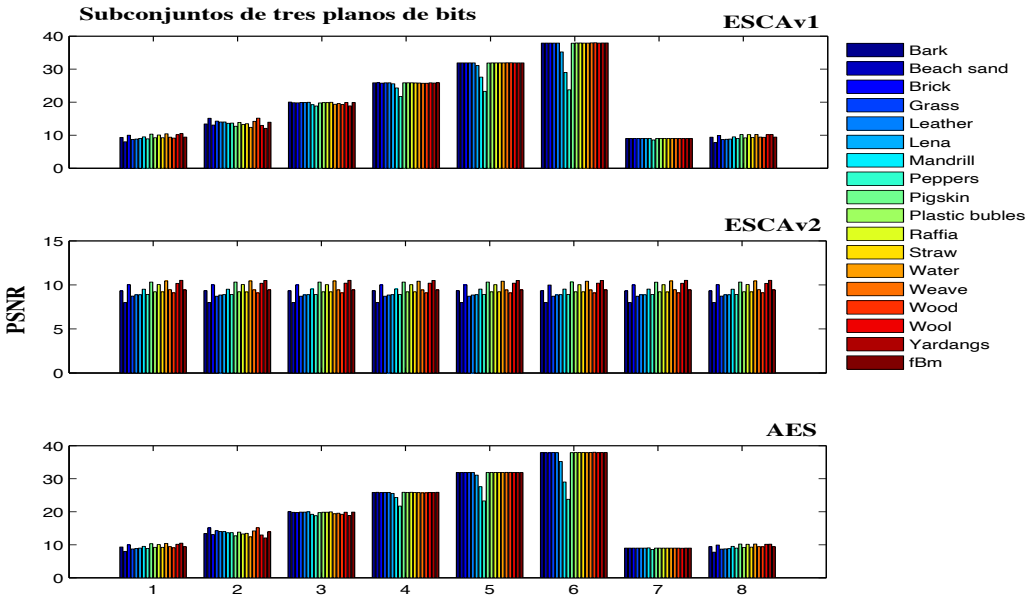


Figura 4.21: PSNR de las imágenes cifradas considerando tres planos de bits.

5

Conclusiones generales y trabajo futuro

En este trabajo se ha presentado una pequeña muestra del amplio conjunto de problemas que pueden resolverse gracias a la versatilidad de la transformada *wavelet*, la cual junto a otras herramientas puede potenciar su alcance y contribuir a la solución de innumerables cuestiones. Son varias las contribuciones específicas que aporta esta tesis.

- En la primera parte:
  - Ante el problema de clasificar los datos correspondientes a un gas de entre los datos de diversas concentraciones de seis gases distintos, se logró establecer que el conjunto de datos recabados durante la exposición de los gases a cada sensor (13 minutos de lecturas del espectro de reflectancia para cada gas y concentración en particular) al ser visualizados como una señal bidimensional, permiten aplicar un sistema de reconocimiento de patrones empleando un novedoso extractor de características basado en la transformada *wavelet* discreta bidimensional, el cual reduce en gran cantidad el número de datos y logra mantener las características relevantes en cada medición, dando paso a una exitosa discriminación y clasificación por medio del clasificador llamado máquina de soporte vectorial. Este clasificador no es exitoso cuando tiene como entradas a las características obtenidas por medio del extractor típicamente usado en clasificación de gases.
  - Gracias a que el sistema de reconocimiento implementado fue exitoso ahora se sabe que los sensores ópticos de gas modificados químicamente pueden emplearse junto a técnicas de extracción de características apropiadas y sistemas de reconocimiento para resolver tareas de quimiosensado complejas.

- Y en la segunda:
  - Se logró establecer las propiedades multifractales de las principales matrices de un sistema de cifrado basado en un autómata celular de regla 90.
  - Por medio del DFA bidimensional aplicado a imágenes cifradas se ha logrado establecer que las imágenes cifradas e ininteligibles presentan un exponente de escala que define un comportamiento persistente cercano al ruido $1/f$.
  - Por medio del DFA mediante *wavelets* aplicado a imágenes se consiguió establecer que la ininteligibilidad de las imágenes cifradas está relacionada con un exponente de escala evaluado unidimensionalmente igual a 0.5, el cual corresponde al ruido gaussiano; además, que este exponente garantiza la seguridad perceptual de las imágenes cifradas, cuyo valor se aleja del 0.5 conforme la imagen cifrada se hace más inteligible. Estos resultados dan indicio de que el exponente de escala puede usarse como una métrica objetiva y no referenciada de la seguridad perceptual y a su vez de la calidad del cifrado.
  - El análisis efectuado a las imágenes cifradas por medio de encriptación selectiva de bits muestra que de los tres métodos evaluados, el ESCAv2 es más efectivo para este tipo de cifrado.

Como futuras líneas de investigación relacionadas a la primera parte de este trabajo se establece claramente la evaluación de métodos de extracción de características tomando en cuenta funciones *wavelets* más sofisticadas, el análisis en áreas de transición de los datos y la evaluación de otros tipos de clasificadores. Mientras en la segunda parte de este trabajo puede profundizarse en la caracterización de los elementos de otros sistemas de cifrado para su uso en criptoanálisis, en el uso de la transformada *wavelet* discreta bidimensional para extraer las tendencias de las señales e implementar un algoritmo que calcule el DFA bidimensional mediante *wavelets* como en el caso del DFA unidimensional, en el análisis de la ininteligibilidad de las imágenes cifradas por otros esquemas, en la posible evaluación de algoritmos de encriptación perceptual para fines comerciales por medio del cálculo del exponente de escala y en el posible uso de la transformada *wavelet* bidimensional como detector de bordes o de información relevante en criptoanálisis.

Bibliografia

[1] Abe, Shigeo. *Support Vector Machines for Pattern Classification*. 2da. edición. Londres: Springer, 2010.

[2] Acharya, Tinku y Ray, Ajoy K. *Image processing: principles and applications*. USA: John Wiley & Sons, Inc., 2005.

[3] Ahmad, Jawad y Ahmed Fawad. Efficiency analysis and security evaluation of image encryption schemes. En: *International Journal of Video & Image Processing and Network Security*. 2012, vol. 12, no. 4, pp. 18-31.

[4] Alvarez-Ramirez, J., Rodriguez, E., Cervantes, I. y Echeverria, J. C. Scaling properties of image textures: A detrending fluctuation analysis approach. En: *Physica A*. 2006, vol. 361, pp. 677-698.

[5] Arneodo, A., Bacry, E. y Muzy, J. F. The thermodynamics of fractals revisited with wavelets. En: *Physica A*. 1995, vol. 213, pp. 232-275.

[6] Burrus, C. Sidney, Gopinath, Ramesh A. y Guo, Haitao. *Introduction to wavelets and wavelet transforms: a primer*. USA: Prentice Hall, 1998.

[7] Content, S., Trogler, W. C. y Sailor, M. J. Adv. Funct. Mater. 13 (5) (2001) 335-338.

[8] Chan, S., Fauchet, P. M., Li, Y., Rothberg, L. J. y Miller, B. L. Porous Silicon Microcavities for Biosensing Applications. En: *Phys. Status, Solidi A*. 2000, vol. 182, no. 1, pp. 541-546.

[9] Dancil, K.-P. S., Greiner, D. P. y Sailor, M. J. A Porous Silicon Optical Biosensor: Detection of Reversible Binding of IgG to a Protein A-Modified Surface. En: *J. Am. Chem. Soc.* 1999, vol. 121 no. 34, pp. 7925-7930.

[10] Daubechies, Ingrid. *Ten Lectures on Wavelets*. Philadelphia, PA: SIAM, 1992.

[11] De Stefano, L., Moretti, L., Rendina, I. y Rossi, A. M. Quantitative optical sensing in two-component mixtures using porous silicon microcavities. En: *Phys. Status. Solidi A*. 2004, vol. 201, no. 5, pp. 1011-1016.

[12] Debnath, Lokenath y Mikusiński, Piotr. *Hilbert Spaces with Applications* 3ra. edición. USA: Elseiver Academic Press, 2005, p. 433.

[13] Delignières, D., Ramdani, S., Lemoine, L., Torre, K., Fortes, M. y Ninot, G. Fractal analysis for short time series: A reassessement of classical methods. En *J. Math. Psychol.* 2006, vol. 50, pp. 525-544.

[14] Droogenbroeck, M. Van y Benedett, R. Techniques for a selective encryption of uncompressed and compressed images. En: *Proc. Advanced Concepts for Intelligent Vision Systems, ACIVS*. Ghent, Belgium: 2002, pp. 90-97.

[15] Duda, Richard O., Hart, Peter E. y Stork, David G. *Pattern Classification* 2da. edición. USA: John Wiley & Sons, Inc. 2001.

[16] Easwaramoorthy, D. y Uthayakumar, R. Analysis of Biomedical EEG Signals using Wavelet Transforms and Multifractal Analysis. En: *IEEE International Conference on Communication Control and Computing Technologies - 2010 (ICCCCT-2010)*. 2010, pp. 544-549.

[17] Eke, A., Herman, P., Bassingthwaighte, J. B., Raymond, G. M., Percival, D. B., Cannon, M., Balla, I. y Ikrényi, C. Physiological time series: distinguishing fractal noises from motions. En: *Pflügers Arch.* 2000, vol. 439, no. 4, pp. 403-415.

[18] Falconer, Kenneth. *Fractal Geometry. Mathematical Foundations and Applications*. 2da. edición. England: John Wiley & Sons Ltd., 2003.

[19] Feder, J. *Fractals*. New York: Plenum Press, 1998.

[20] Lavine, Barry K. y Davidson, Charles E. Classification and Pattern Recognition. En: Gemperline, Paul, ed. *Practical Guide to Chemometrics*. 2da. edición. USA: Taylor & Francis, 2006. pp. 90, 341.

[21] James, Glyn. *Matemáticas avanzadas para ingeniería*. 2da edición. México: Pearson Educación, 2002. p. 280.

[22] Goswami, Jaideva C. y Chan, Andrew K. *Fundamentals of wavelets: theory, algorithms, and applications*. USA: John Wiley & Sons, Inc., 1999.

[23] Gu, G. F. y Zhou, W. X. Detrended fluctuation analysis for fractals and multifractals in higher dimensions. En: *Phys. Rev. E*. 2006, vol. 74. pp.

[24] Gualdrón, Guerrero Oscar Eduardo. *Desarrollo de diferentes métodos de selección de variables para sistemas multisensoriales.* Tesis doctoral. Universitat Rovira I Virgili, Tarragona, España, 2006.

[25] Halsey, T. C., Jensen, M. H., Kadanoff, L. P., Procaccia, I. y Shraiman, B. I. Fractal measures and their singularities: the characterization of strange sets. En: *Phys. Rev. A.* 1986, vol. 33, no. 2, p. 1141.

[26] Hines, Evor L., Boilot, P., Gardner, Julian W. y Gongora, Mario A. Pattern Analysis for Electronic Noses. En: Pearce, T. C., Schiffman, S. S., Nagle, H. T. y Gardner, J. W. *Handbook of Machine Olfaction. Electronic Nose Technology.* Alemania: WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim, Weinheim, 2003, pp. 133-160.

[27] Huang, X. J., Choi Y. K., Yun, K. S. y Yoon, E. Oscillating behaviour of hazardous gas on tin oxide gas sensor: Fourier and wavelet transform analysis. En: Sens. Actuators B. 2006. vol. 115, (2006), pp. 357-364.

[28] Ihlen, Espen. A. F. Multifractal analyses of response time series: A comparative study. En: *Behavior Research Methods*. 2013, vol. 45 no. 4, pp. 928-945.

[29] Ionescu, R. y Llobet, E. Wavelet transform-based fast feature extraction from temperature modulated semiconductor gas sensors. En: *Sens. Actuators B.* 2002, vol. 81, no. 2, pp. 289-295.

[30] Jagadeesh, P., Nagabhushan, P. y Kumar, R. P. A novel perceptual image encryption scheme using geometric objects based kernel. En: *International Journal of Computer Science & Information Technology*. 2013, vol. 5, no. 4, pp. 165-173.

[31] Jorgensen, Palle E. T. *Analysis and probability wavelets, signals, fractals.* New York: Springer, Graduate Text in Mathematics. 2006.

[32] Kantelhardt, J. W., Zschinegner, S. A., Koscielny-Bunde, E., Havlin, S., Bunde, A. y Stanley, H. E. Multifractal detrended fluctuation analysis of nonstationary time series. En: *Physica A*. 2002, vol. 316, pp. 87-114.

[33] Kantelhardt, J. W. *Encyclopedia of Complexity and Systems Science*. Berlin: Springer, 2009

[34] Kautz, Richard. *Chaos. The Science of Predictable Random Motion*. USA: Oxford University Press, 2011.

[35] King, B. H., Ruminski, A. M., Snyder, J. L. y Sailor, M. J. Optical-fiber-mounted porous silicon photonic crystals for sensing organic vapor breakthrough in activated carbon. En: *Adv. Mater.* 2007, vol. 19, pp. 4530-4534.

[36] King, B. H., Wong, T. y Sailor, M. J. Detection of pure chemical vapors in a thermally cycled porous silica photonic crystal. En: *Langmuir*. 2011, vol. 27, pp. 8576-8585.

[37] Kim, Guk H., Kim, Young W., Lee, Sang J. y Jeon, Gi J. Multi-Class System based on SVM for real-time Gas Mixture Classification. En: *Proceedings of SICE Annual Conference 2010*. Taipei, Taiwan: 2010, pp. 1764-1767.

[38] Kitlas Golińska, Agnieszka. Detrended Fluctuation Analysis (DFA) in biomedical signal processing: selected examples. En: *Studies in logic, grammar and rhetoric*. 2012, vol. 29, no. 42, pp. 107-115.

[39] Kulkarni, N. S., Raman, B. y Gupta, I. Multimedia encription: A brief overview. En: M.Grgic, K. Delac, M. Ghanbari (Eds.), *Recent Advanced in Multimedia Signal Processing and Communications*. Berlin Heidelberg: Springer, 2009, pp. 417-449.

[40] Leija, Lorenzo. *Métodos de procesamiento avanzado e inteligencia artificial en sistemas sensores y biosensores*. México: Ed. Reverté, 2009, p. 8.

[41] Lian, S. *Multimedia Content Encryption. Tecniques and Applications* Boca Raton: CRC Press Taylor and Francis group, 2009.

[42] Lin, V.S-Y, Motesharei, K., Dancil, K. S., Sailor, M. J. y Ghadiri M. R., A Porous Silicon-Based Optical Interferometric Biosensor. En: Science 1997, vol. 278, no. 5339, pp. 840-843.

[43] Llobet, E., Brezmes, J., Ionescu, R., Vilanova, X., Al-Khalifa, S. y Gardner, J. W., Barsan, N. y Correig, X. Wavelet transform and fuzzy ARTMAP-based pattern recognition for fast gas identification using a micro-hotplate gas sensor. En: *Sens. Actuators B*. 2002, vol. 83, pp. 238-244.

[44] Lookabaugh, T. y Sicker, D. C. Selective encryption for consumer applications. En: *IEEE Commun. Mag.* 2004, vol. 42, pp. 124-129.

[45] Mallat, S. y Hwang, W. L. Singularity detection and processing with wavelets. En: *IEEE Trans. Inform. Theory*. 1992, vol. 38, pp. 617-643.

[46] Mallat, Stéphane. *A wavelet tour of signal processing*, 2da. ed. USA: Academic Press, 1999.

[47] Manimaran, P., Panigrahi, P. K. y Parikh, J. C. Wavelet analysis and scaling properties of time series. En: *Phys. Rev. E*. 2005, vol. 72.

[48] Manimaran, P., Panigrahi, P. K. y Parikh, J. C. Multiresolution analysis of fluctuations in non-stationary time series through discrete wavelets. En: *Physica A*. 2009, vol. 388, pp. 2306-2314.

[49] Marques de Sá, J. P. *Pattern Recognition. Concepts, Methods and Applications*. Springer, 2001.

[50] Mogollon, Manuel. *Cryptography and Security Services: Mechanisms and Applications*. Hershey, PA, USA: IGI Publishing, 2008.

[51] Mohammadi, Pedram; Ebrahimi-Moghadam, Abbas y Shirani, Shahram. Subjective and Objective Quality Assessment of Image: A Survey. En: *Majlesi Journal of Electrical Engineering*. 2015, vol. 9, no. 1.

[52] Moon, Todd K. y Stirling, Wynn C. *Mathematical methods and algorithms for signal processing*. USA: Prentice Hall, Inc., 2000. p. 194.

[53] Murguía, J. S., *Tratamiento multirresolución de señales e imágenes con ondeletas de Haar*, Tesis de maestría en Ingeniería Eléctrica, UASLP, San Luis Potosí, 1999.

[54] Murguía, J. S. y Urías, J. On the wavelet formalism for multifractal analysis. En: *Chaos*. 2001, vol. 11, no. 4, pp. 858-863.

[55] Murguía, J. S., Perez-Terrazas, J. E. y Rosu, H. C. Multifractal properties of elementary cellular automata in a discrete wavelet approach of MF-DFA. En: *Europhys. Lett.* 2009, vol. 87, no. 2, pp. 28003.

[56] Murguía, J. S., Mejía Carlos, M., Rosu, H. C. y Flores-Eraña G. Improvement and analysis of a pseudo-random bit generator by means of cellular automata. En: *Int. J. Mod. Phys. C.* 2010, vol. 21, no. 6, pp. 741-756.

[57] Murguía, J. S. y Rosu, H. C. Multifractal analyses of row sum signals of elementary cellular automata. En: *Physica A.* 2012, vol. 391, no. 13, pp. 3638-3649.

[58] Murguía, J. S., Flores-Eraña G., Mejía Carlos, M. y Rosu, H. C. Matrix approach of an encryption system based on cellular automata and its numerical implementation. En: *Internat. J. Modern. Phys. C.* 2012, vol. 23, no. 11, pp. 1250078.

[59] Murguía, J. S., Vergara, A., Vargas-Olmos, C., Wong, Travis J., Fonollosa, J. y Huerta, R. Two-dimensional wavelet transform feature extraction for porous silicon chemical sensors. En: *Analytica Chimica Acta.* 2013, vol. 785, pp. 1-15.

[60] Murguía, J. S., Rosu, H. C., Jiménez, A., Gutiérrez-Medina, B. y García-Meza, J. V. The Hurst exponents of Nitzschia sp. diatom trajectories observed by light microscopy. En: *Physica A.* 2015, vol. 417, pp. 176-184.

[61] Muzy, J. F., Bacry, E. y Arneodo, A. Multifractal formalism for fractal signals: The structure-function approach versus the wavelet-transform modulus-maxima method. En: *Phys. Rev. E.*1993, vol. 47, pp. 875-884.

[62] Muzy, J. F., Bacry, E. y Arneodo, A. The multifractal formalism revisited with wavelets. En: *Int. J. Bifurcation Chaos.* 1994, vol. 4, no. 2, pp. 245-302.

[63] Orosco, M. M., Pacholski, C., Miskelly, G. M. y Sailor, M. J. Protein-coated porous silicon photonic crystals for amplified optical detection of protease activity. En: *Adv. Mater.* 2006, vol. 18, pp. 1393-1396.

[64] Oświęcimka, P., Kwapień, J. y Drożdż, S. Wavelets versus detrended fluctuation analysis of multifractal structures. En: *Phys. Rev. E.* 2006, vol. 74.

[65] Oświęcimka, P., Kwapień, J. y Drożdż, S. y Gó, A. Z. Effect of detrending on multifractal characteristics. En: *Acta Phys. Polon.* 2013, vol. 123, pp. 597-603.

[66] Otto, Matthias. *Chemometrics: statistics and computer application in analytical chemistry*. Federal Republic of Germany: WILEY-VCH, 1999.

[67] Ouahabi, Abdeldjalil. *Signal and Image Multiresolution Analysis*, USA: ISTE Ltd y John Wiley & Sons, Inc. 2012. pp 6.

[68] Peng, C. K., Buldyrev, S. V., Havlin, S., Simons, M., Stanley, H. E. y Goldberger, A. L. Mosaic organization of DNA nucleotides. En: *Phys. Rev. E*. 1994, vol. 49, pp. 1685-1689.

[69] Peña, Daniel. *Análisis de datos multivariantes*, España: McGraw-Hill, 2002. pp. 134.

[70] Podesser, M., Schmidt, H. P. y Uhl, A. Selective bitplane encryption for secure transmission of image data in mobile environments. En: *Proceedings of the 5th IEEE Nordic Signal Processing Symposium (NORSIG 2002)*, 2002.

[71] Quinquis, André. *Digital Signal Processing using MATLAB*. Great Britain: ISTE Ltd y John Wiley & Sons, Inc. 2008. pp 343.

[72] Ramírez-Torres, M. T., Murguía, J. S. y Mejía Carlos, M. Image encryption with an improved cryptosystem based on a matrix approach. En: *Internat. J. Modern. Phys. C*. 2014, vol. 25, no. 10, pp. 1450054

[73] Ramis Ramos, Guillermo y García Álvarez-Coque M.^{a} Celia. *Quimiometría*. España: Editorial SÍNTESIS, pp. 157-196

[74] Reljin, I., Reljin, B., Pavlović,I. y Rakočević, I. Multifractal Analysis of Gray-Scale Images. En: *10^{th} Mediterranean Electrotechnical Conference, MEleCon 2000, Vol. II*, IEEE, 2000.

[75] Rencher, Alvin C. y Christensen, William F. *Methods of multivariate analysis*, 3ra. edición, USA: John Wiley & Sons, Inc. 2012, pp. 64-68, 405-430

[76] Ruminski, A.M., Moore, M. y Sailor, M. J. Humidity-Compensating Sensor for Volatile Organic Compounds Using Stacked Porous Silicon Photonic Crystals. En: *Adv. Funct. Mater.*2008, vol. 18, pp. 3418-3426.

[77] Ruminski, A.M., King, B. H., Salonen, J., Snyder, J. L. y Sailor, M. J. Porous silicon-based optical microsensors for volatile organic analytes: effect of surface chemistry on stability and specificity. En: *Adv. Funct. Mater.* 2010, vol. 20, no. 10, pp. 2874-2883.

[78] Scott, Simon M.; James, Davis y Ali, Zulfiqur. Data analysis for electronic nose systems. En: *Microchimica Acta*. 2007, vol. 156, pp. 183-207.

[79] Skrepth, Champskud J. y Uhl, Andreas. Selective encryption of visual data. En: B. Jerman-Blaži et al.(eds.), *Advanced Communications and Security*. New York: Springer, 2002, pp. 213-226.

[80] Snow, P. A., Squire, E. K., Russell, P. S. J. y Canham, L. T. Vapor sensing using the optical properties of porous silicon Bragg mirrors. En: *J. Appl. Phys.* 1999, vol. 86, no. 4, pp. 1781-1784.

[81] Sun, J., Xu, Z., Liu, J., Yao, Y. An objective visual security assessment for cipher- images based on local entropy. En: *Multimedia Tools Appl.* 2011, vol. 53, pp. 75-95.

[82] Tang, Chongwu; Yang, Xiaokang y Zhai Guangtao. Image quality/distortion metric based on α-stable model similarity in wavelet domain. En: *J. Vis. Commun. Image. R.* 2014, vol. 25, pp. 1746-1757.

[83] Theodoridis, Sergios y Koutroumbas, Konstantinos. *Pattern Recognition*. 4a. edición. Canadá: Elsevier, 2009.

[84] Theodoridis, Sergios; Pikrakis, Aggelos; Koutroumbas, Konstantinos y Cavouras, Dionisis. *Introduction to Pattern Recognition. A MATLAB® Approach*. USA: Elsevier, 2010. pp. 79-80.

[85] Urías, J., Salazar, G. y Ugalde, E. Synchronization of cellular automaton pairs. En: *Chaos*. 1998, vol.8, no. 4, pp. 814-818.

[86] Urías, J., Ugalde, E. y Salazar, G. A cryptosystem based on cellular automata. En: *Chaos*. 1998, vol. 8, no.4, pp. 819-822.

[87] Vargas Olmos Cecilia, *Procesamiento de imágenes con métodos de ondeleta*, Tesis de Maestría en Ciencias Aplicadas. UASLP. San Luis Potosí, 2010.

[88] Vergara, A., Martinelli, E., Huerta, R., D'Amico, A. y Di Natale, C. Orthogonal decomposition of chemo-sensory cues. En: *Sens. Actuators B*. 2011, vol. 159, no. 1, pp. 126-134.

[89] Vergara, A., Calavia, R., Vázquez, R. M., Mozalev, A., Abdelghani, A., Huerta, R., Hines, E. H. y Llobet, E. Multifrequency Interrogation of Nanostructured

Gas Sensor Arrays: A Tool for Analyzing Response Kinetics. En: *Anal. Chem.* 2012, vol. 84, no. 17, pp. 7502-7510.

[90] Vetterli, Martin y Kovacevic, Jelena. *Wavelets and subband coding*. Englewood Cliffs NJ: Prentice Hall, 1995.

[91] Vijayaraghavan, R., Sathya, S., Raajan N. R. Encryption for an image using circular budge on bit-planes. En: *International Journal of Applied Engineering Research*. 2014, vol. 9, no. 2, pp. 153-160.

[92] Wang, Fan; Liao, Deng-wen; Li, Jin-wei y Liao, Gui-ping. Two-dimensional multifractal detrended fluctuation analysis for plant identification. En: *Plant Methods. BioMed Central*. 2015, vol. 11.

[93] Xue, X. y Zhang, X. Feature extraction and classification with wavelet transform and support vector machines. En: *Proceedings IEEE IGARSS (2005)*, 2005, pp. 3795-3798.

[94] Yeh, R. G., Lin, C. W., Abbod, M. F. y Shieh, J. S. Two-Dimensional Matrix Algorithm Using Detrended Fluctuation Analysis to Distinguish Burkitt and Diffuse Large B-Cell Lymphoma. En: *Comput. Math. Meth. Med.* 2012, vol. 2012.

[95] Yin, Y., Yu, H. y Zhang, H. A feature extraction method based on wavelet packet analysis for discrimination of Chinese vinegars using a gas sensor array. En: *Sensors and Actuators B*. 2008, vol. 134, pp. 1005-1009.

[96] Yuan, Yuan; Guo, Qun y Lu, Xiaoqiang. Image quality assessment: A sparse learning way. En: *Neurocomputing*. 2015, vol. 159, pp. 227-241.

[97] Zhou, Y., Leung, Y. y Yu, Z. G. Relationships of exponents in two-dimensional multifractal detrended fluctuation analysis. En: *Phys. Rev. E*. 2013, vol. 87.

[98] Zunino, L., Soriano, M. C., Figliola, A., Pérez, D. G., Garavaglia, M., Mirasso, C. R. y Rosso, O. A. Performance of encryption schemes in chaotic optical communication: A multifractal approach. En: *Opt. Commun.* 2009, vol. 282, pp. 4587-4594.