Análisis del Desempeño de un Algoritmo de Esteganografía de Imágenes Basado en la Transformada Discreta Wavelet

Federico Francisco Alberto Benítez González
Bernardo García Osorio

Directora: MsC. María Manuela Silva Zambrano
Codirector: PhD(c). Siler Amador Donado

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de Nuevas Tecnologías en Telecomunicaciones – GNTT
Procesamiento Digital de Señales

Popayán, 2023

AGRADECIMIENTOS

Queremos expresar nuestros agradecimientos a las siguientes personas que han sido fundamentales en el proceso de investigación, desarrollo y redacción de este trabajo de grado:

A nuestra directora de tesis, la MsC. María Manuela Silva Zambrano, Por su apoyo incondicional y animo investigativo, que nos imbuyo a lo largo de este proceso, además de su espíritu curioso siempre en busca de aprender algo nuevo nos permitió cambiar nuestra perspectiva ante muchos problemas que parecían imposibles.

También agrademos a nuestro codirector, el PhD(c). Siler Amador Donado, por sus aportes claves, para poder evaluar el algoritmo desde puntos de vista que eran ajenos a nosotros.

Federico Benítez:

Querida Madre, quiero agradecerte por todo tu apoyo y aliento durante mi trabajo de grado. Tú has sido una fuente constante de motivación y tu ayuda ha sido invaluable para mí.

Desde el principio, me apoyaste en cada paso del proceso, me ayudaste a organizarme, a hacerme preguntas importantes y a encontrar recursos útiles. Me enseñaste la importancia de la perseverancia y la paciencia, y me diste el empujón que necesitaba para continuar incluso en los momentos más difíciles.

No puedo expresar con palabras cuánto significó para mí tenerte a mi lado en este viaje. Tu amor y tu dedicación me han ayudado a llegar hasta aquí, y por eso quiero agradecerte desde lo más profundo de mi corazón.

Gracias por ser mi madre, mi amiga y mi consejera. Siempre estaré agradecido por todo lo que has hecho por mí.

Con todo mi amor.

Querido Hermano, quiero agradecerte desde lo más profundo de mi corazón por todo el apoyo y el amor que me has brindado durante mi trabajo de grado. Desde que era pequeño, siempre has sido mi héroe y mi modelo a seguir.

También quiero agradecerte por tu ejemplo de amor y compromiso con la familia. Siempre has estado ahí para apoyarnos en todo lo que necesitamos. Me siento muy afortunado de tener un hermano como tú, y espero seguir contando con tu amor y tu apoyo en el futuro.

Gracias por ser mi hermano, mi amigo y mi mentor. Siempre te llevaré en mi corazón, y espero que puedas sentir todo el amor y la gratitud que tengo por ti.

Con todo mi cariño,
También tengo un agradecimiento especial a Juliana Sánchez, quien fue un apoyo inquebrantable en todo este proceso, ya que siempre estuvo ahí cuando la necesite, brindándome ánimos en todos los días y noches que tomó esta ardua tarea, además de darme la seguridad y confianza en que el objetivo iba a ser conseguido pasara lo que pasara.

Gracias de todo corazón

Bernardo García Osorio:

"Quiero dedicar este logro a las personas que me han apoyado incondicionalmente. En primer lugar, a mi mamá porque ha sido mi mayor motivación para este logro. A mi papá por su inimaginable apoyo durante en todo este proceso. A mi tío Juan Pablo por todo lo que ha significado para mí durante toda mi vida. A mi prima Anytha por ser mi compañera de aventuras, ya que la vida nos ha premiado con la oportunidad de vivir y compartir juntos logros muy importantes. A la RAMA Estudiantil IEEE porque con ellos pasé inolvidables momentos, viajes y experiencias que hacen que sean lo mejor de mi paso por la universidad. A Federico porque sus aptitudes técnicas, su perseverancia e insaciable búsqueda de realizar cada tarea de la mejor manera, lo convierten en el mejor compañero de tesis que pude haber escogido. Por último, agradecer a todas las personas que fueron parte de mi vida en estos últimos años porque cada una de ellas ha contribuido a mi crecimiento y felicidad personal."

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ACRÓNIMOS

BPCS	*Bit-Plane Complexity Segmentation, Segmentacion de la Complejidad del Plano de Bits.*
DCT	*Discrete Cosen Transform, Transformada Discreta Coseno.*
DWT	*Discrete Wavelet Transform, Transformada Wavelet Discreta.*
FIR	*Finite Impulse Response, Respuesta Finita al Impulso.*
FT	*Fourier Transform, Transformada de Fourier.*
HSV	*Human Visual System, Sistema Visual Humano.*
IDWT	*Inverse Discrete Wavelet Transform, Transformada Inversa Discreta Wavelet.*
LSB	*Least Significative Bit, Bit Menos Significante.*
LWT	*Lifting Wavelet Transform, Transformada Lifting Wavelet.*
LZWT	*Lazy Wavelet Transform, Transformada Perezosa Wavelet.*
PSNR	*Peak Signal-to-Noise Ratio,* Relación Señal a Ruido Máxima.
ROI	*Regions Of Interest, Regiones De Interes*
STFT	*Short Time Fourier Transform, Transformada de Fourier de Tiempo Corto.*
WT	*Wavelet Transform, Transformada Wavelet.*

CAPÍTULO 1: ESTEGANOGRAFÍA

1.1. Sistemas de Seguridad Informática

La digitalización de la información y el uso de un repositorio abierto como el internet, trajo consigo una nueva área de investigación: la seguridad digital, la cual tiene como finalidad garantizar la comunicación segura entre dos usuarios. La seguridad en la información es actualmente imprescindible en cualquier sistema de telecomunicaciones, es por ello que con el pasar de los años se han hecho avances significativos para garantizar la seguridad de la información, dando como resultado dos grandes grupos de acciones: el cifrado y el ocultamiento de la información; aunque estas técnicas buscan el mismo objetivo, existen algunas diferencias entre ellas: como el tipo de datos que ocultan, la forma en la que brindan la seguridad o el tratamiento dado a la información sensible.

El cifrado se encarga de codificar la información utilizando diferentes algoritmos, proporcionando confidencialidad y autenticidad a los datos, de esta manera se modifican y se vuelven ilegibles para un tercero, tal como se ejemplifica en la Figura 1.1.

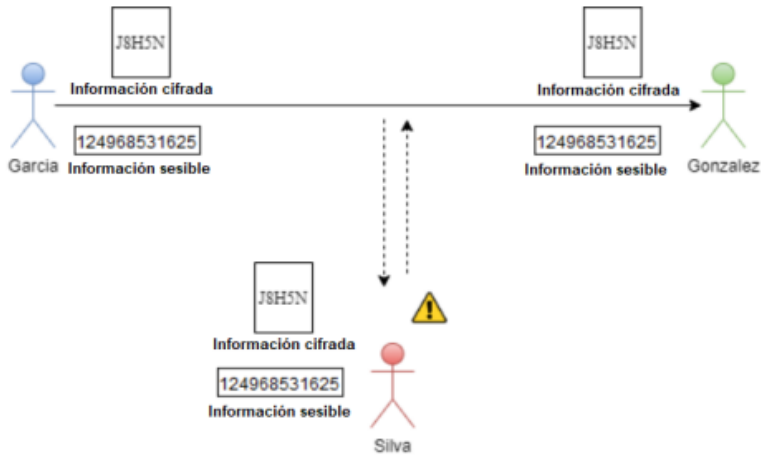


Figura 1.1. Transmisión de datos con un algoritmo de cifrado.

Una desventaja de los algoritmos de cifrado es la apariencia caótica del mensaje transmitido, la cual advierte la existencia de la información que está siendo protegida; en consecuencia, un tercero puede intentar recuperarla con el uso de diferentes algoritmos [1]. En la sección 1.4.4 se habla con mayor detalle de los algoritmos de cifrado y cómo puede trabajar en conjunto con la esteganografía.

Para suplir las desventajas presentadas anteriormente, se puede hacer uso de los métodos para ocultar información, los cuales engloban todas aquellas alternativas para esconder datos sensibles dentro de otro medio portador, e.g. ocultando la información sensible dentro de una imagen tal como se muestra en la Figura 1.2.

Con estos métodos se logra que el ocultamiento de los datos sea indetectable, de tal manera que un tercero sólo perciba el medio portador y no realice esfuerzos por descifrar la información oculta [2].

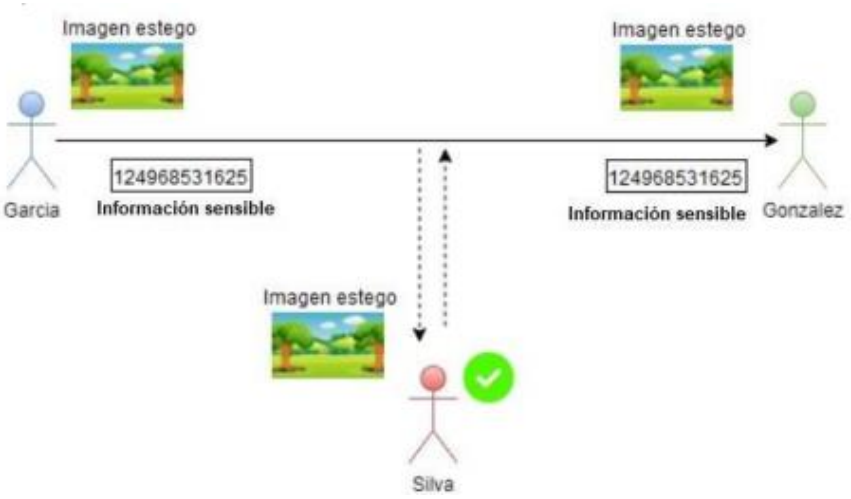


Figura 1.2. Transmisión sistema para ocultar información.

Los métodos para ocultar información cuentan con diversas maneras de ejecución, por ello es posible clasificar sus variaciones tal como se muestra en la Figura 1.3 [3], asimismo, se encuentra resaltado en color naranja el enfoque que se toma en el presente trabajo de grado.

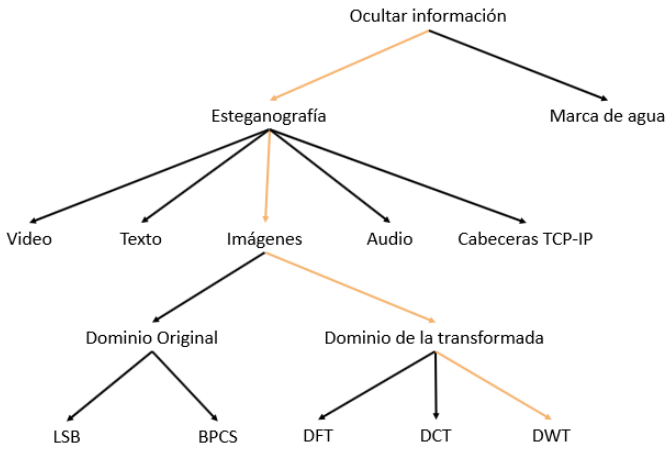


Figura 1.3. Clasificación de sistemas de para ocultar información. Tomado de [2].

Dentro de los métodos para ocultar información se encuentran dos principales enfoques, los sistemas de marca de agua y los sistemas de esteganografía. El objetivo de los sistemas de ocultación de marca de agua es proteger la propiedad intelectual de los archivos digitales y así evitar la duplicidad no ética de los ficheros multimedia [3]; esto se logra al incrustar información de menor tamaño que incluye registros de los derechos de autor del contenido digital como los datos del autor o metadatos de una fotografía o un video.

Por el contrario, el objetivo de un algoritmo de esteganografía es ocultar información secreta dentro de otro medio portador, es decir, la información oculta no tiene relación alguna con el medio utilizado. Como se muestra en la Figura 1.3, en la esteganografía se pueden usar varios tipos de archivos como medio portador: videos, imágenes, audio, texto o cabeceras TCP-IP. Teniendo en cuenta la naturaleza de estos archivos, se debe realizar un preprocesamiento a los datos sensibles antes de incrustarlos. Por ejemplo, si se usa una imagen, un audio digital o un video, los datos a ocultar se deben procesar como bits.

1.2. Esteganografía

La esteganografía es un método de ocultamiento de la información que se utiliza ampliamente en diversas aplicaciones de seguridad de la información. Esta técnica consiste en esconder datos sensibles de tipo texto, audio o imágenes, empleando un soporte multimedia como *Medio de cobertura* [4].

1.2.1. ¿Por qué usar esteganografía?

Una de las principales diferencias entre la esteganografía y el cifrado, es que los métodos de cifrado envían información inentendible que puede alertar a un atacante que hay datos protegidos en el mensaje, por el contrario, en los algoritmos de esteganografía el resultado final es un archivo que no levanta mayor sospecha para un tercero.

La esteganografía es un área en constante evolución, desde hace algunos años se han propuesto diferentes métodos y variaciones buscando un mejor rendimiento en el sistema, dando como resultado múltiples posibilidades de implementación.

Independientemente del método utilizado, los algoritmos de esteganografía buscan 3 objetivos principales, mostrados en la Figura 1.4 [2].

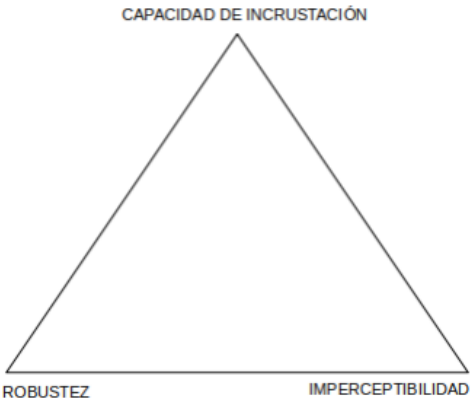


Figura 1.4. Triángulo de la esteganografía. Tomado de [2].

Los vértices del triángulo de la figura anterior, no se pueden satisfacer de forma simultánea, para entender mejor la razón por la cual son mutuamente excluyentes, se realiza la definición de estos 3 parámetros:

- Imperceptibilidad[1]: facultad de no generar sospecha alguna de la presencia de la información escondida.
- Capacidad de incrustación: cantidad de información secreta que se puede introducir en un medio portador.
- Robustez a los ataques: capacidad para mantener la integridad de los datos secretos y para recuperar la información secreta cuando ocurran daños por terceros.

Generalmente, los algoritmos de esteganografía buscan alcanzar un rendimiento representado en un equilibrio entre la capacidad de incrustación, la imperceptibilidad en la imagen estego y la robustez del sistema. Se debe tener en cuenta que aumentar la capacidad de incrustación reduce la imperceptibilidad, ya que el medio portador se altera en mayor medida y, por consiguiente, podría ser más evidente que se ha escondido información, aumentando la probabilidad de que un tercero tome medidas para acceder a los datos secretos y, por ende, afectando la robustez del sistema.

Un algoritmo de esteganografía balanceado se representa en la Figura 1.5, en la cual, el punto de color verde dentro del área del triángulo indica su rendimiento. Idealmente, se debería tener un máximo rendimiento en las 3 aristas, pero dado a que esto no es posible, generalmente se escoge un enfoque que prioriza una arista en particular.

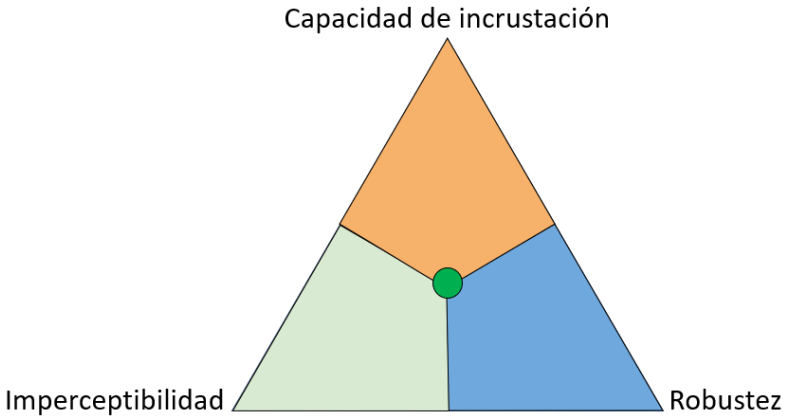


Figura 1.5. Rendimiento ideal en esteganografía de imágenes.

La búsqueda del equilibrio entre las tres aristas del triángulo no se alcanza de una sola forma, debido a la gran cantidad de variaciones posibles en los algoritmos esteganográficos y la inclusión de procesos opcionales en los sistemas modernos,

[1] Este parámetro se mide en la Relación Señal a Ruido Máxima (PSNR, *Peak Signal-to-Noise Ratio*).

por lo que existen muchos métodos que han demostrado obtener resultados óptimos [5].

El propósito principal de la esteganografía es la transmisión segura de archivos digitales mediante la red, pero su potencial ha llevado a que se encuentren otros usos, en los que no siempre lo deseable es ubicar el punto de rendimiento en el centro; ya que, esto puede variar según el contexto en el que se esté aplicando el algoritmo esteganográfico. Por ejemplo, en la transmisión de imágenes médicas se busca una mayor capacidad de incrustación debido al gran tamaño de estas imágenes [6]. Asimismo, en sistemas de seguridad militar se prioriza la robustez del algoritmo, debido a la naturaleza de la información a transmitir, mientras que en sistemas con aplicaciones en fotomontajes el enfoque principal es la imperceptibilidad [7].

1.2.2. Algoritmos de esteganografía según el medio de cobertura

En el proceso esteganográfico se encuentran dos vías de ejecución según el medio de cobertura utilizado: la esteganografía lingüística y la esteganografía técnica; la diferencia más significativa entre ellas es que la esteganografía lingüística utiliza como medio de cobertura el texto plano y la esteganografía técnica utiliza otro tipo de portador como las imágenes, audios o videos. Además de esto, la esteganografía lingüística presenta desventajas notorias frente a las estrategias de esteganografía técnica, ya que su medio de cobertura no provee una gran capacidad para incrustar información secreta y su método de ocultamiento puede ser burlado con relativa facilidad [8]. Teniendo en cuenta lo anterior, la Figura 1.6 revela un acercamiento gráfico al rendimiento de un algoritmo de esteganografía lingüística.

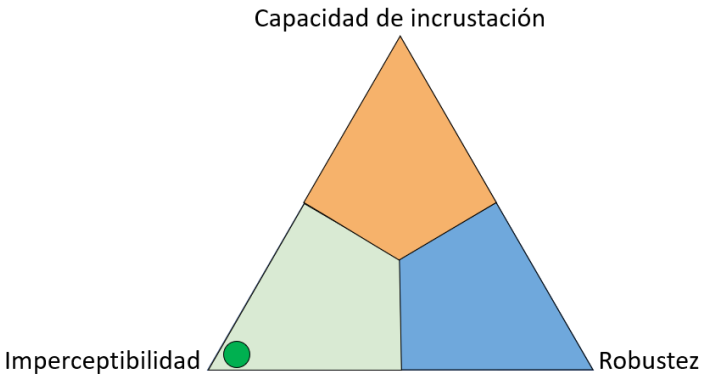


Figura 1.6. Rendimiento de un algoritmo de esteganografía lingüística.

Dado que la información se encuentra inmersa en los caracteres, los algoritmos de esteganografía lingüística alcanzan niveles óptimos en imperceptibilidad, tal como se muestra en la Figura 1.6; no obstante, el uso de texto plano genera poca capacidad de incrustación y deficientes niveles de robustez.

Por otra parte, el uso de archivos multimedia en los algoritmos de esteganografía técnica, abren la posibilidad para realizar un procesamiento más elaborado a los datos secretos y conseguir mejores niveles de rendimiento al compararlo con la esteganografía lingüística[2].

1.2.3. Esteganografía de dominio original

En un algoritmo de esteganografía, se tiene un medio de cobertura el cual se modifica para ocultar los datos secretos, esta modificación se puede realizar de dos modos: cambiando directamente la información (dominio original), o variando la manera en la que se representan los datos (dominio transformado) [9].

Los métodos de esteganografía de dominio original ocultan la información sensible aplicando una manipulación directa de los datos del medio portada, esto genera simplicidad en la implementación, cortos tiempos de ejecución y menores exigencias sobre el hardware. El método más utilizado es el reemplazo en el Bit Menos Significativo (LSB, *Least Significative Bit)*, este método permite una gran capacidad de incrustación, pero con un precio a pagar en la imperceptibilidad; además, no presenta seguridad para enviar los datos, afectando la robustez del sistema [4]. Con relación a las desventajas presentadas anteriormente, a lo largo de los años, en la literatura se han propuesto diversos algoritmos con procesos complementarios para suplir esas falencias [10].

Un algoritmo de esteganografía de dominio original (sin ningún proceso adicional) obtiene valores sobresalientes en capacidad de incrustación, valores aceptables en imperceptibilidad y resultados mejorables en cuanto a robustez, tal como se muestra en la Figura 1.7 [4].

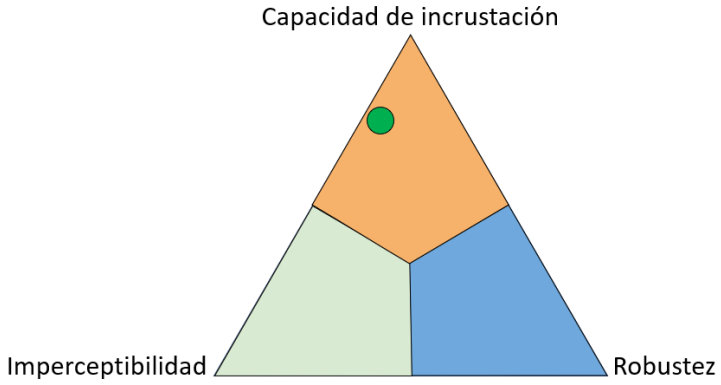


Figura 1.7. Rendimiento de algoritmo de dominio original.

[2] En la actualidad la mayoría de los algoritmos de esteganografía corresponden a esteganografía técnica, como en el caso de este trabajo de grado. Al hablar de esteganografía en este trabajo de grado se considera que es esteganografía técnica.

1.2.4. Esteganografía de dominio transformado

El uso de un dominio transformado en esteganografía conlleva a una modificación en la representación de los datos del medio portada. Lo anterior implica la inclusión de procesos adicionales al algoritmo, los cuales pueden producir mejoras en la imperceptibilidad y/o robustez para una capacidad de incrustación dada, si se compara con algoritmos de dominio original [11]. La modificación de los datos se puede realizar con distintas transformadas lineales, como la Transformada de Fourier (FT, *Fourier Transform)*, la Transformada Discreta de Coseno (DCT, *Discrete Cosen Transform)* y la Transformada Discreta Wavelet (DWT, *Discrete Wavelet Transform)*, las cuales presentan ventajas y desventajas según el método utilizado [10].

En el presente trabajo de grado se hace uso de la DWT, puesto que presenta ventajas frente a las otras transformadas en cuanto a imperceptibilidad y robustez [4]. En la sección 1.3.2 se plantea con mayor detalle la forma en la que se utiliza esta transformada dentro del algoritmo de esteganografía.

1.2.5. ¿Por qué usar imágenes como medio de cobertura?

Las imágenes como medio de cobertura[3] son seleccionadas en gran parte de los algoritmos de esteganografía, debido a sus características de alta capacidad de procesamiento y nivel de redundancia, además de su diversidad en tamaños, colores y formatos. Estas características no sólo originan una elevada capacidad de compresión, sino también una facilidad de representación y modificación de sus propiedades. Es así, como el uso de imágenes puede hacer posible conseguir niveles de rendimiento esperados en un algoritmo de esteganografía, ya que el Sistema Visual Humano (HSV, *Human Visual System*) presenta una baja sensibilidad a los pequeños cambios en pixeles adyacentes dentro de una imagen [12].

En función de lo planteado, son claras las ventajas del uso de las imágenes como medio portador en la esteganografía, por esta razón, es el medio de cobertura escogido para el algoritmo seleccionado en el presente trabajo de grado.

1.2.6. Composición de una imagen digital

En términos matemáticos, una imagen se define como una función en dos dimensiones $g(x,y)$, donde x y y corresponden a coordenadas en un espacio plano y g representa la intensidad de color en esa coordenada[4]. En este orden de ideas, se denomina una imagen digital cuando x,y y g son cantidades finitas y discretas.

---

[3] En esteganografía, cuando el medio de cobertura es una imagen, se le denomina *Imagen portada* y una vez se haya incrustado la información secreta, se denomina *Imagen estego* [1].

[4] A cada $g(x,y)$ en una imagen digital se le denomina un pixel.

$$\begin{bmatrix} g\ (0,0) & g\ (0,1) \\ g\ (1,0) & g\ (1,1) \end{bmatrix}$$

De esta manera, es posible representar una imagen digital como una matriz de $N \times M$, donde N y M son enteros positivos y cada posición de la matriz es un pixel de la imagen.

Por otra parte, los niveles de intensidad de los pixeles que conforman una imagen vienen dados por $L = 2^k$, donde k es un número entero. Generalmente, a k se le asigna un valor de 8, por lo que se cuenta con 256 niveles de intensidad de color[5].

El ojo humano presenta una sensibilidad mayor a los cambios en los colores rojo (R, *Red*), verde (G, *Green*) y azul (B, *Blue*), es por ello que todos los colores se pueden ver como una combinación de valores en estos tonos (conocido como el modelo RGB). Es decir que, al usar 8 bits en cada uno de estos colores, se producen:

$$RGB = 256 \times\ 256 \times\ 256$$

$$= 16'777.216 \text{ colores}$$

El algoritmo planteado, trabaja con el modelo RGB usando imágenes de 8 bits por pixel, soportados en el hecho de que el HVS sólo puede distinguir alrededor de un millón de colores.

1.3. Algoritmos de Esteganografía en Imágenes

Existen múltiples algoritmos de esteganografía en imágenes, con diversos enfoques y propuestas para alcanzar los objetivos en imperceptibilidad, robustez y capacidad de inserción; desde una perspectiva general, los principales procesos implementados en estos algoritmos son los mostrados en la Figura 1.8.

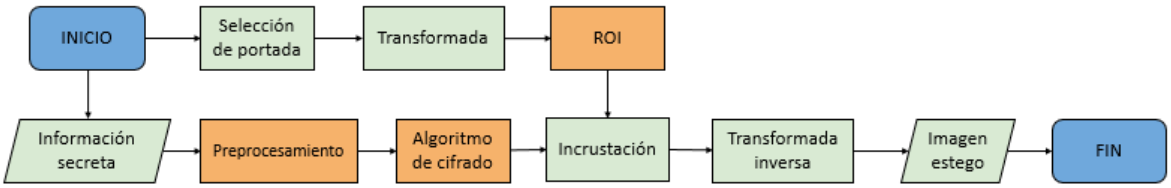


Figura 1.8. Diagrama de bloques de un algoritmo de esteganografía en imágenes.

[5] Antiguamente se trabajaba con 4 bits y en la actualidad se pueden encontrar aplicaciones que hacen uso de 16 y 32 bits.

La Figura 1.8 indica paso a paso la serie de bloques ejecutados en un algoritmo de esteganografía en imágenes, desde la selección de portada hasta la obtención de la imagen estego. Este diagrama de bloques presenta el procesamiento efectuado tanto a la imagen portada como a la información secreta (en el presente trabajo de grado, el tipo de información incrustada es una imagen) antes de la incrustación de los datos. Cada uno de los procesos de color verde cumple una función indispensable para llevar a cabo el algoritmo, por otra parte, los procesos de color naranja son opcionales, es decir que su no implementación no afecta el funcionamiento del algoritmo, pero su inclusión puede aportar a un mejor rendimiento.

Cada bloque del algoritmo se puede ver como un área de investigación independiente[6]; por ello, es pertinente que a lo largo de esta sección se profundice en cada uno de los bloques, con el fin de mostrar las principales características, modos de ejecución e investigaciones que han resultado en avances significativos.

1.3.1. Imagen portada

La imperceptibilidad en un algoritmo de esteganografía en imágenes viene muy ligada a la imagen portada utilizada, de allí que en los últimos años se hayan adelantado diversas investigaciones en torno al efecto de las características de luminosidad, la composición y el formato de compresión de las imágenes en usos esteganográficos [11], [13], [14].

Dentro de estas investigaciones, se resaltan algunas que han demostrado que al ocultar la información en imágenes con: mayor contraste, menor correlación, menor uniformidad, mayor nivel de detalle y alta homogeneidad; se alcanza altos valores de PSNR [11].

Por otra parte, resulta claro que, una vez extraída la información secreta, no es necesario un proceso de reconstrucción para la imagen portada; no obstante, existen algoritmos que permiten la restauración de esta imagen, se les conoce como *Algoritmos de esteganografía de imagen reversible. S*u implementación permite que, una vez reconstruida la imagen portada, se pueda verificar si la imagen estego ha intentado ser vulnerada, de manera que es especialmente útil para campos como la telemedicina, el arte y la milicia [6], [14]. Sin embargo, su aplicación origina pérdidas en la capacidad de incrustación y mayor complejidad con respecto a algoritmo de imagen no reversible [15].

La selección de portada ha pasado a ser un proceso crucial en la esteganografía en imágenes [16], ya que puede aportar al algoritmo planteado mejoras notorias en imperceptibilidad, sin que se vea afectada la capacidad de incrustación. En este orden de ideas, tomando como ejemplo la Figura 1.7 y agregando una imagen

[6] El algoritmo planteado gira entorno a la transformada.

portada óptima, una representación del rendimiento para un algoritmo de esteganografía, es el mostrado en la Figura 1.9.

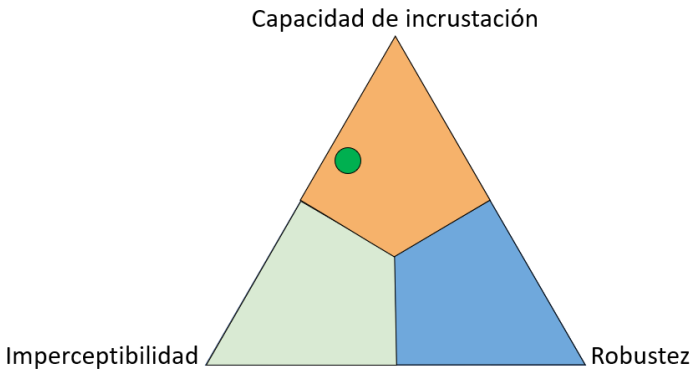


Figura 1.9. Rendimiento de algoritmo de dominio original con una imagen portada óptima.

La Figura 1.9 indica que no se alcanzan niveles óptimos de imperceptibilidad, debido a que en secciones posteriores se demuestra que, al utilizar métodos adicionales, se obtienen mejores niveles de PSNR.

1.3.2. Transformada

El propósito de una transformación lineal en esteganografía de imágenes[7], es cambiar la representación de la información de la imagen portada, con la intención de que, al incrustar la información secreta, las modificaciones ocasionadas sean poco perceptibles.

La DWT es una de las transformadas con mayor despliegue en algoritmos de esteganografía [4], [11], [17], debido a sus ventajas frente a otras transformadas y a los algoritmos de dominio original. Además, esta transformación se puede implementar a través de una gran cantidad de familias de Wavelets, por lo que es posible aumentar la aleatoriedad del algoritmo y así mejorar su robustez.

[7] La inclusión de un proceso de transformada convierte un algoritmo del dominio original al dominio transformado, sin embargo, es posible utilizar los mismos procesos de incrustación de la información en ambos dominios.

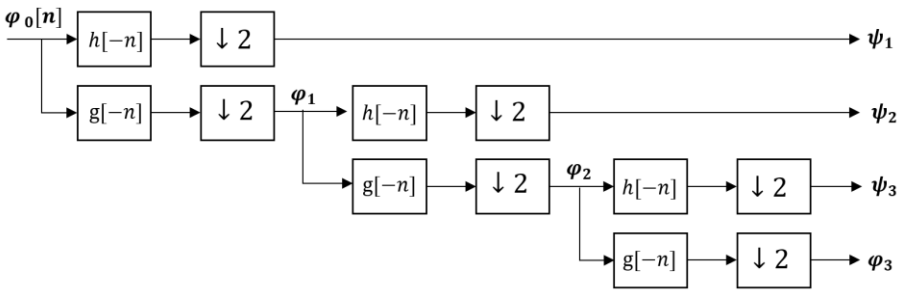


Figura 1.10. Algoritmo de Mallat. Tomado de [18].

Las investigaciones adelantadas en [18], afirman que al realizar la DWT a una señal, $\boldsymbol{\varphi_0}$, se obtienen coeficientes de aproximación, $\boldsymbol{\varphi_1}$, y coeficientes de detalle, $\boldsymbol{\psi_1}$. A este proceso se le conoce como transformación Wavelet a un nivel de descomposición. Es posible tomar nuevamente los coeficientes de aproximación, para repetir el proceso varias veces y obtener unos nuevos coeficientes, $\{\boldsymbol{\varphi_2}, \boldsymbol{\psi_2}\}$, para dos niveles de descomposición y $\{\boldsymbol{\varphi_3}, \boldsymbol{\psi_3}\}$ para tres niveles de descomposición, tal como se muestra en la Figura 1.10.

Para efectos de la esteganografía, tener diferentes conjuntos de coeficientes permite guardar la información secreta en cualquiera de éstos. Teniendo en cuenta que, mientras menor sea el nivel de descomposición en el que se encuentre la información secreta, mayor es su tamaño y por lo tanto se tiene una mayor capacidad de incrustación; sin embargo, se ven afectadas la imperceptibilidad y la robustez del sistema. Por otro lado, si se usa un nivel de descomposición mayor, se ve afectada la capacidad de incrustación, pero el resultado es un algoritmo robusto y con mejores valores de imperceptibilidad [19].

Tomando en cuenta lo anterior, la Figura 1.11 muestra una estimación del rendimiento de un algoritmo de esteganografía en imágenes, asumiendo una buena imagen portada y haciendo uso de la DWT a distintos niveles.

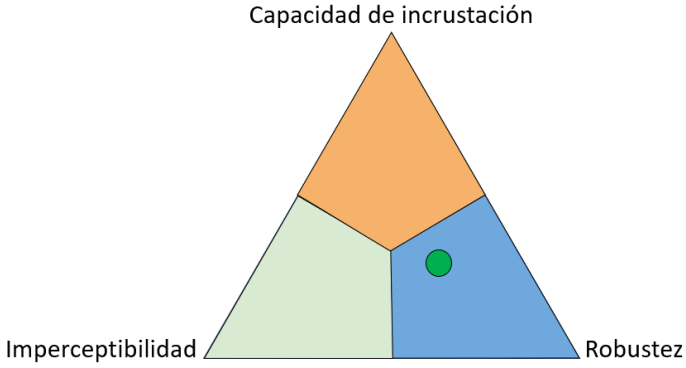


Figura 1.11. Rendimiento de un algoritmo de esteganografía usando la DWT.

Una vez culminado este proceso, la imagen portada se encuentra en un dominio Wavelet[8], es por ello que después de incrustar la información secreta, se requiere realizar la reconstrucción (IDWT, *Inverse Discrete Wavelet Transform*), para regresar la imagen a su dominio original y obtener la imagen estego [4].

1.3.3. Regiones de interés

La detección de Regiones de Interés (ROI, *Regions Of Interest*), es un proceso opcional que se agrega al algoritmo de esteganografía, en el cual se buscan las áreas, posiciones o grupos de pixeles idóneos para ocultar la información secreta. Una de las principales ventajas de la implementación de ROI, es que se puede realizar indistintamente si el algoritmo es de dominio original o de dominio transformado. En particular, su uso, en conjunto con la DWT proporciona mayor nivel de robustez frente a ataques de tipo visual y estadístico, puesto que, al insertar la información en uno de los conjuntos de coeficientes, la distorsión de la imagen portada es pequeña, ya que se altera solo una parte de la información. Además, tiene ventajas contra ataques estructurales, debido a que una modificación en la información de la imagen estego, implica también una modificación en la información sensible.

Las desventajas presentadas frecuentemente por el proceso ROI, se deben a que las técnicas más utilizadas requieren una mayor carga computacional [20] y pueden resultar en menores capacidades de incrustación, si se compara con algoritmos que no lo incluyen [21].

Los avances en esta área se han enfocado principalmente en la detección [22] y uso de los contornos de las imágenes portada, dado que se ha demostrado que el HSV es menos susceptible a los cambios en los bordes [12], [23].

Con la inclusión de este proceso, el algoritmo planteado adquiere resultados sobresalientes en imperceptibilidad y robustez, tal como se representa en la Figura 1.12.

[8] Dado que al aplicar una transformación lineal se cambia la representación de la información, se tiene que al aplicar la DWT el dominio en el que está representada esta información es el dominio Wavelet.

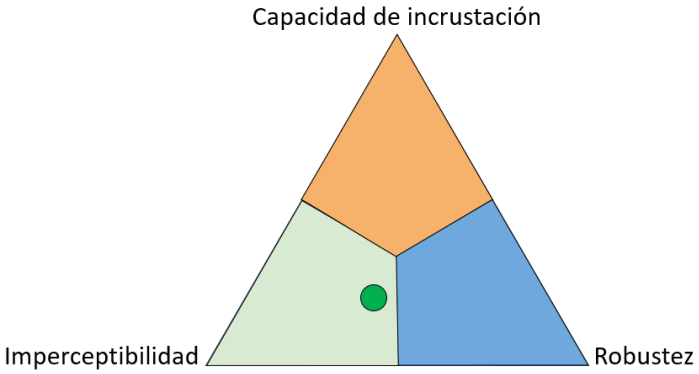


Figura 1.12. Rendimiento de un algoritmo de esteganografía usando ROI.

1.3.4. Información secreta

En un algoritmo de esteganografía en imágenes, es posible ocultar cualquier información que pueda ser representada como una combinación de bits, e.g. para un texto, basta con convertir la información a un sistema de codificación de caracteres binarios, como el código ASCII. Así mismo, un audio puede ser digitalizado para obtener un flujo de bits en una dimensión y una imagen, que corresponde a una serie de valores discretos organizados en matrices de $N \times M$, puede ser codificada para obtener una representación binaria. Una vez la información secreta y la imagen portada están representadas por medio de una secuencia de unos y ceros, es posible continuar con el proceso esteganográfico.

1.3.5. Preprocesamiento

Se trata de un proceso opcional previo al ocultamiento de la información, que busca aplicar un tratamiento a los datos secretos, con el fin de aumentar el rendimiento del sistema. Por ejemplo, al usar un método de *compresión* se requiere menor cantidad de bits para representar la información, logrando que afecte en menor medida a la imagen portada y sea posible mejorar la imperceptibilidad de la imagen estego.

1.3.6. El cifrado

El cifrado se encarga de codificar la información utilizando diferentes algoritmos, para generar una secuencia aparentemente caótica que proporcione confidencialidad y autenticidad a los datos. La recuperación de la información se logra aplicando de manera inversa dichos algoritmos, con ayuda de una llave o clave secreta [1].

Los métodos de cifrado se dividen en sistemas de cifrado simétricos y asimétricos. El cifrado simétrico, hace uso de una clave única para cifrar y descifrar los datos ocultos. Una de las ventajas de este método, es la simpleza en implementación y

ejecución, no obstante, si la clave compartida es interceptada, el sistema queda obsoleto. Por otra parte, el cifrado asimétrico hace uso de dos claves, una clave pública (usada para cifrar los datos) y una clave privada (usada para descifrar los datos). Este sistema presenta una mayor robustez frente al cifrado simétrico, dado que no se requiere la distribución de las claves; sin embargo, incrementa la complejidad de implementación y uso del sistema [24]

Los algoritmos de cifrado y los algoritmos esteganográficos pueden ser complementarios, esto se logra al realizar un proceso de cifrado antes de incrustar la información secreta en el medio de cobertura. Por consiguiente, si un atacante pudiera extraer la información de la imagen estego, ésta seguiría siendo inentendible y por lo tanto inaccesible para él.

La inclusión de un proceso de cifrado aumenta la carga computacional y la complejidad de un algoritmo de esteganografía, pero su uso aporta los niveles esperados de robustez en el sistema [9].

Teniendo en cuenta lo anterior, la Figura 1.13 muestra un ejemplo del rendimiento de un algoritmo de esteganografía, al incluir un sistema de cifrado.

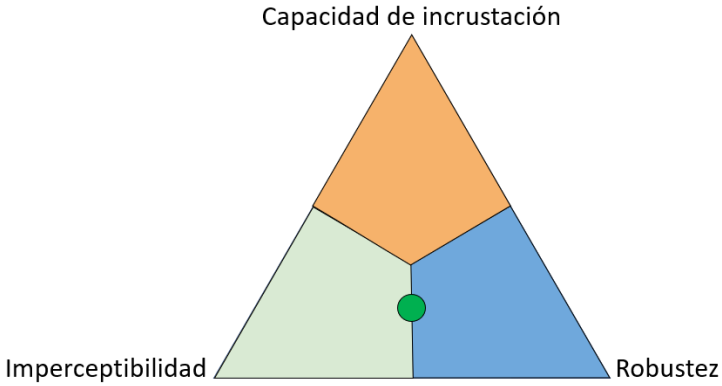


Figura 1.13. Rendimiento de un algoritmo esteganográfico con algoritmo de cifrado.

1.3.7. Incrustación de la información

Es el proceso que se encarga de ocultar la información secreta dentro de la imagen portada; para ello, se busca que el método a utilizar permita la incrustación de los datos, sin afectar la imperceptibilidad de la imagen estego.

Los dos métodos más usados en esteganografía para la incrustación de la información son el LSB y la Segmentación de Complejidad del Plano de Bits (BPCS, *Bit-Plane Complexity Segmentation*) [2].

1.3.7.1. BPCS

En este método se descompone la imagen en distintos planos de bits y se reemplaza la información secreta en los *planos complejos* de la imagen [25]. La característica que determina el nivel de complejidad en cada uno de estos planos es la homogeneidad de la imagen, es decir, la cantidad de cambios entre valores de uno y cero que presente un área determinada. Los planos de baja complejidad se encuentran en áreas de la imagen con intensidad de color uniforme o que contengan formas simples. En cambio, los planos complejos son resultado de áreas de la imagen con ruido alto, o zonas con múltiples cambios entre uno y cero en bits adyacentes.

Teniendo en cuenta que el HVS no percibe cambios en la información en un patrón binario complicado, se pueden sustituir los planos complejos de la imagen por la información secreta [26].

1.3.7.2. LSB

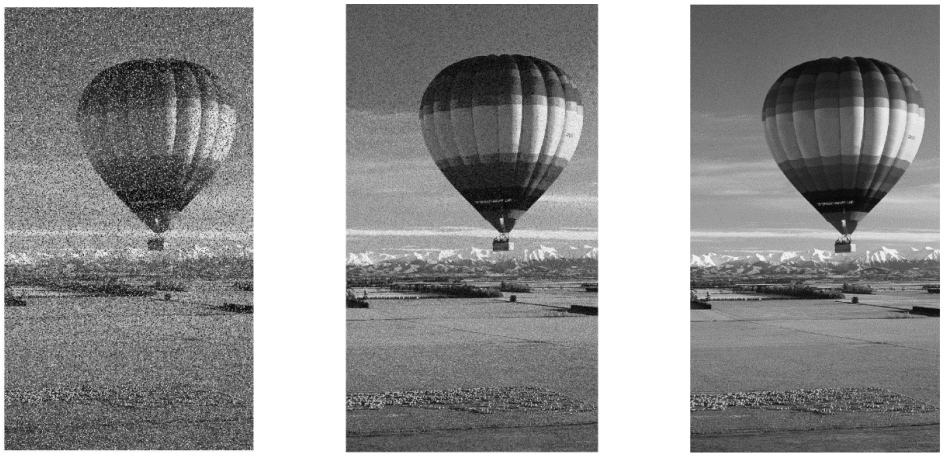
En este método, se reemplaza la información en uno o varios bits de cada pixel de la imagen, priorizando el reemplazo en los últimos bits de la secuencia, los que son menos significativos. Por ejemplo, si se tiene una imagen codificada a 8 bits (1 byte) y se usan 3 LSB para insertar la información secreta, entonces cada byte de la imagen estego estaría dado por: 1 0 0 1 1 0 1 1, siendo los bits de color negro los bits que no se modifican y los bits de color rojo en los que se oculta la información secreta.

Existe una relación directamente proporcional entre la capacidad de incrustación de información y el número de bits usados con el método LSB, sin embargo, aumentar el número LSB, disminuye la imperceptibilidad de la imagen estego. Para ilustrar lo anteriormente mencionado, se han generado 3 imágenes estego con la misma imagen portada[9], usando diferentes números de LSB para incrustar la información de una imagen secreta[10]; los resultados obtenidos se muestran a continuación.

La Figura 1.14, muestra tres imágenes estego en la que se han reemplazado 8, 5 y 3 LSB para incrustar la información secreta. En el primer caso, el uso de los 8 bits genera que la imperceptibilidad de la imagen estego se vea afectada de manera notoria. Lo anterior significa que, a pesar de su óptima capacidad de incrustación, el uso de 8 LSB no es recomendable para aplicaciones en esteganografía. Mientras que, al ocultar la información en 5 LSB, la imperceptibilidad de la imagen estego mejora considerablemente en comparación con la de 8 LSB, además, su capacidad de incrustación no se ha visto mayormente afectada. Sin embargo, en ciertas zonas de la imagen se puede apreciar un cambio en la intensidad del color de algunos bits, especialmente en la zona del cielo. De esta manera, se concluye que el uso de 5 LSB genera un equilibrio entre la capacidad de la incrustación y la imperceptibilidad.

[9] Imagen portada con un tamaño de 1920 x 1080.
[10] Imagen secreta con un tamaño de 554 x 650.

Ahora bien, se puede apreciar visualmente que en la imagen estego con 3 LSB, la imperceptibilidad no se ha afectado; pero el costo a pagar es una disminución en la capacidad de la incrustación, si se compara con las variaciones de 5 y 8 LSB. Por esta razón, el uso de 3 LSB en un algoritmo de esteganografía es usado en aplicaciones en las que se favorece la imperceptibilidad sobre la capacidad de incrustación.



8 LSB 5 LSB 3 LSB

Figura 1.14. Imagen estego “Globo Aerostático” reemplazando 8,5 y 3 LSB.

1.3.8. Tipos de ataques en esteganografía

La imperceptibilidad y la robustez son características fundamentales para los algoritmos de esteganografía, debido a que la imagen estego puede enfrentarse a distintos ataques. Estos ataques intentan encontrar indicios de que la imagen ha sido modificada y, de ser así, tratar de vulnerar la información oculta dentro de ella. Comúnmente, para poner a prueba el rendimiento de los algoritmos de esteganografía en imágenes, se hace uso de ataques visuales y ataques estadísticos.

1.3.8.1. Ataques visuales

En este tipo de ataques, visualmente se buscan fallas o indicios de que la imagen ha sido manipulada para ocultar información. Lo anterior quiere decir que este método está limitado por el HVS, el cual es proclive a pasar por alto detalles sutiles dentro de las imágenes [12], no obstante, es el tipo de análisis más común y el que primero se efectúa.

Uno de los objetivos principales de la esteganografía es que la imagen estego no levante sospechas, por lo que como mínimo los algoritmos deben poder superar este tipo de ataques y, dado que con la mayoría de los algoritmos se alcanzan niveles altos de imperceptibilidad, los ataques visuales resultan poco efectivos si se quiere detectar una imagen estego, por lo que se recurre a los ataques estadísticos [8].

1.3.8.2. Ataques estadísticos

En general, los ataques de tipo estadístico hacen uso de métodos matemáticos para buscar patrones, indicios o señales de que la imagen ha sido modificada para ocultar información en ella. Este tipo de ataques aprovechan las falencias que presentan algunos métodos comúnmente utilizados en esteganografía, por ejemplo, si la imagen estego tiene formato *.jpg*, se pueden buscar indicios de bits perdidos causados por el redondeo en el proceso de compresión. Además, se podrían atacar las regiones del borde de la imagen, ya que estas áreas son frecuentemente escogidas como ROI [8].

Los métodos de ataques estadísticos se pueden aplicar de manera general a todos los algoritmos de esteganografía, pero debido a la aleatorización que genera la variedad de procesos y subprocesos utilizados, los métodos de estegoanálisis genéricos presentan resultados deficientes. Sin embargo, el estegoanálisis estadístico moderno se enfoca en realizar métodos específicos para cada algoritmo, no obstante, quebrantar un algoritmo de esteganografía robusto toma un tiempo considerable y capacidades computacionales altas [8]

CAPÍTULO 2: TRANSFORMADA WAVELET

2.1. ¿De Dónde Provienen las Wavelets?

Las Wavelets nacen como producto del desarrollo continuo que ha existido en el análisis de señales, tanto en frecuencia como en el tiempo, debido a las deficiencias mostradas por la Transformada de Fourier. La FT muestra cómo cualquier señal se puede ver como la suma ponderada de señales sinusoidales, gracias a lo cual es posible conocer las frecuencias que componen a dicha señal, pero tiene como limitación que no es posible relacionar el comportamiento de la señal en instantes de tiempo concretos con los componentes de frecuencia que estén ocurriendo en esta ventana de tiempo.

Es importante resaltar que el principio de incertidumbre de Heisenberg impide tener conocimiento perfecto de lo que ocurre en un instante en el tiempo y la frecuencia, por lo que una buena resolución en la frecuencia implica una mala resolución en el tiempo. Por el contrario, una buena resolución en el tiempo implica una mala resolución en la frecuencia. La Transformada de Fourier de Tiempo Corto (STFT, *Short Time Fourier Transform*) parte de este principio, por lo cual toma como base la idea de un análisis de la señal con una ventana de tiempo específico, generando dos posibles resultados al aplicar un marco de referencia con respecto a la frecuencia de ese instante de tiempo [27]–[29]:

1. Si la ventana tiene una duración muy amplia, los detalles de la información en frecuencia tienden a ser abundantes, dando una buena idea de lo que ocurre en el dominio de la frecuencia, aun así, se pierde la capacidad de ubicar instantes de tiempo concretos asociados a las componentes de frecuencia. En la Figura 2.1 se busca ejemplificar esta restricción por medio de un espectrograma [27].

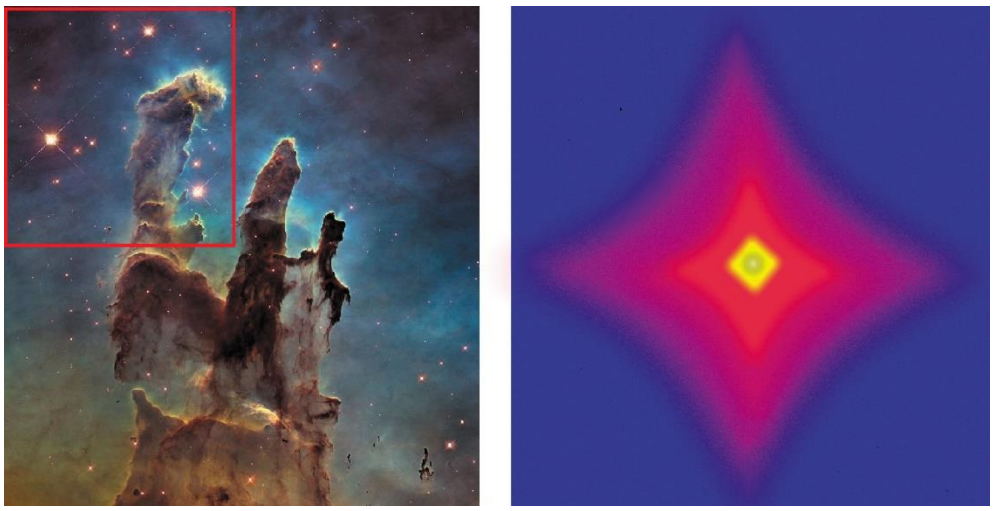


Figura 2.1. STFT con una ventana 4 veces menor que la imagen.

2. Si la ventana tiene una duración muy corta, se puede conocer de manera más clara lo que sucede en ese instante de tiempo, pero se pierde resolución de lo que sucede en el dominio de la frecuencia [27]. Lo anterior se puede apreciar en la Figura 2.2.

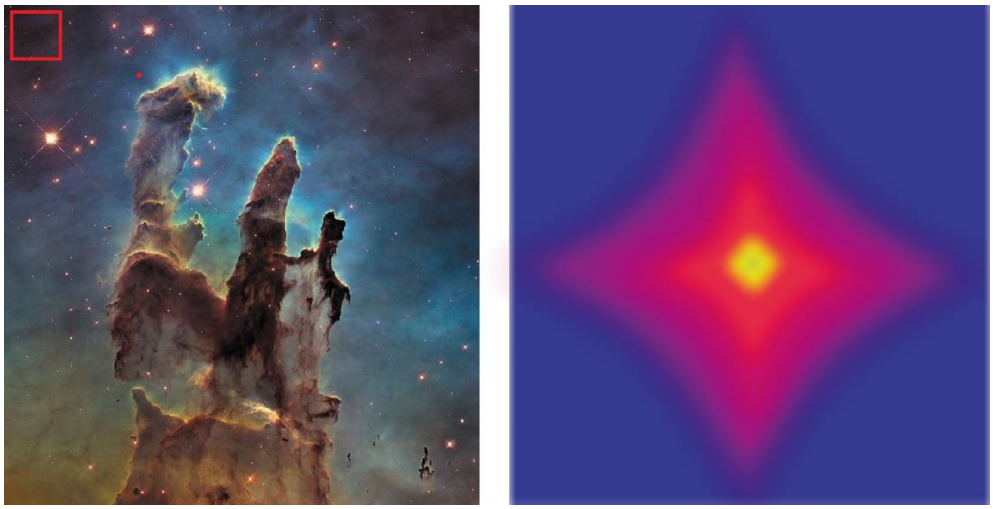


Figura 2.2. STFT con una ventana 8 veces menor que la imagen.

Aunque la STFT relaciona lo que ocurre en los dominios del tiempo y la frecuencia, para su aplicación es necesario determinar el tamaño y el tipo de la ventana. La Transformada Wavelet (*WT, Wavelet Transform*) surge como una evolución de la STFT, es decir, es consecuencia directa a la necesidad de facilitar la forma de relacionar el comportamiento de una señal en el tiempo y la frecuencia [27].

En un principio, Jean Morlet definió de forma teórica la transformada Wavelet, en la cual se correlaciona a la señal con versiones modificadas de una señal de duración finita en el tiempo (ventana), las modificaciones consisten en generar versiones desplazadas y escalonadas de la ventana, por lo que esta transformación es biparámetrica. Esta transformada constituye una compensación entre las resoluciones que se tienen en el tiempo y la frecuencia; sin embargo, según su formulación se deben considerar infinitos valores de desplazamiento y escala que hacen inviable su aplicación práctica [27], [30].

2.2. Definición Matemática de una Wavelet

Morlet nombró las Wavelets como *ondelettes*, cuya traducción al inglés es *Wavelets* y al español como *onditas*, indicando que son ondas de duración finita en el tiempo. El conjunto de funciones Wavelet se obtiene a partir de la Wavelet madre, la cual se denotada como $\psi(t)$ [30], [31]. No obstante, para que una onda sea clasificada como una Wavelet, debe cumplir con tres características (*condiciones de admisibilidad*) [27]:

1. Área bajo la curva igual a cero:

$$\int_{-\infty}^{\infty} \psi(t)dt = 0.$$

2. Duración finita:

$$\psi(t) = 0, \forall\, t \notin [t1, t2],$$

donde $-\infty < t1 < t2 < \infty$. Luego, su energía finita se puede calcular de la forma:

$$\mathcal{E}_{\psi} \approx \int_{t1}^{t2} |\psi(t)|^2 dt\,, \qquad \mathcal{E}_{\psi} < \infty.$$

3. Buena localización espectral:

$$\mathcal{E}_{\psi} \approx \int_{f1}^{f2} |\Psi(f)|^2 df\,, \qquad -\infty < f_1 < f_2 < \infty.$$

A partir de las características mostradas anteriormente, se han creado diferentes tipos de familias Wavelets, las cuales proporcionan diversos efectos a la hora de interactuar con una señal, esto ha originado un sin número de aplicaciones en diferentes áreas. La familia Wavelet creada a partir de la Wavelet madre se nota como $\psi_{a,b}(t)$, la cual es un conjunto de versiones escaladas y trasladadas de la función original [27].

2.3. Transformada Wavelet de Tiempo Continuo

En la Figura 2.3 muestra un ejemplo de cómo una Wavelet (color naranja), a una escala dada, se traslada y se correlaciona con una señal seno (color azul), en este caso la Wavelet ha recorrido una distancia λ (No confundir con la longitud de onda de la función seno), no obstante, se considera un desplazamiento continuo, es decir, la diferencia entre valores consecutivos del parámetro encargado del desplazamiento tiende a cero [27].

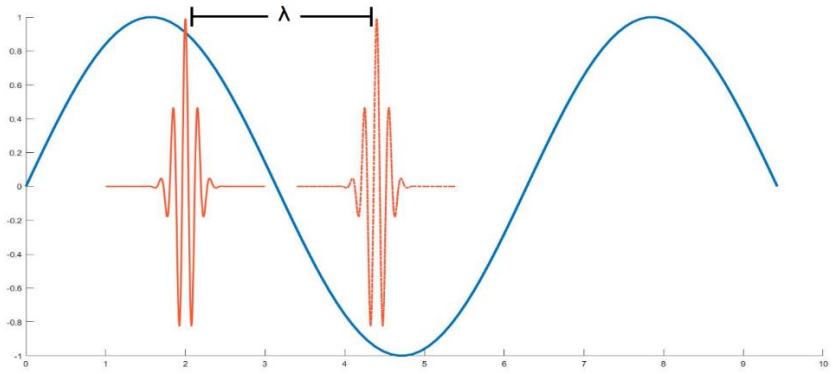


Figura 2.3. Transformada Wavelet continua, traslación de la Wavelet.

Además del desplazamiento en la WT se considera la variación de la escala, la cual permite variar el nivel de descomposición. Las versiones escaladas también se deben trasladar, por lo que, siguiendo el ejemplo de la Figura 2.3, se obtiene el resultado mostrado en la Figura 2.4. Como se aprecia en la Figura 2.4, la Wavelet ha reducido su duración en el tiempo, pero a su vez ha aumentado su amplitud, con lo que se mantiene constante el valor de $\mathcal{E}_{\psi}$.

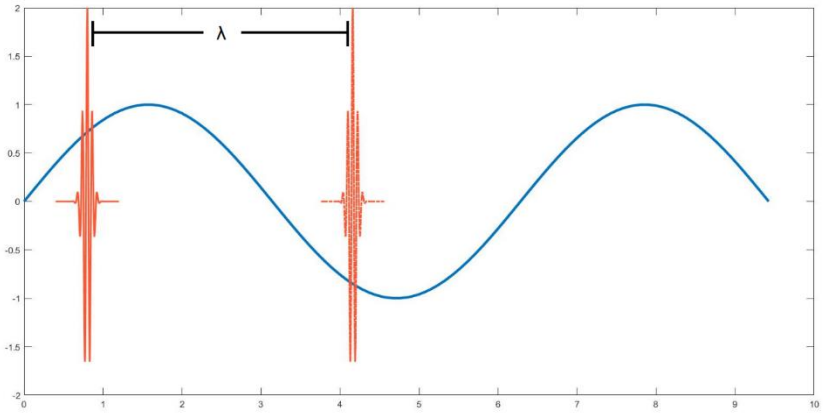


Figura 2.4. Transformada Wavelet continua, cambio de la resolución.

El conjunto generado por la traslación y el escalado, se puede captar desde frecuencias bajas hasta frecuencias altas. Matemáticamente los coeficientes resultantes son de la forma [27], [31], [32]

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

siendo,

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

donde,

a es el parámetro de escala.
b es el parámetro traslación.

Así mismo, es posible recuperar la señal original a partir de los coeficientes Wavelet.

$$x(t) = C \int_{0}^{\infty} \int_{-\infty}^{\infty} W_x(a,b)\psi_{a,b}(t)\, db\, da,$$

donde C es un valor constante asociado a la familia Wavelet utilizada, pero no tiene mucha relevancia en los coeficientes resultantes.

De manera analítica, el problema de la WT en tiempo continuo es que su aplicación práctica es imposible, ya que posee una cantidad infinita de valores tanto de desplazamiento como de escala. La WT de tiempo continuo genera una gran cantidad de coeficientes, los cuales tienen información redundante y por lo tanto pueden ser omitidos; de esta manera, surge la DWT [27].

2.4. Transformada Wavelet Discreta

Una señal limitada en banda que se discretiza en tiempo cumpliendo con la tasa de muestreo de Nyquist no sufre pérdida de información. En este caso la frecuencia máxima que podría contener la señal es la mitad de su frecuencia de muestreo, según el análisis implementado, por lo que la DWT debe poder analizar este rango de frecuencias respetando la fidelidad de la información contenida en la señal y eliminando la información redundante. Para esto, tanto la traslación como el escalado deben estar relacionados, de modo que se definen dos nuevos parámetros, j como el nivel de descomposición y k como el nivel de traslación que va a tener la señal; por lo tanto, a y b quedan de la forma [27]

$$\begin{aligned} a &= 2^{-j}, \qquad j \in \mathbb{Z}. \\ b &= 2^{-j}k, \qquad k \in \mathbb{Z}. \end{aligned}$$

Al remplazar respectivamente los nuevos valores de a y b se obtiene

$$\psi_{j,k}(t) = \frac{1}{\sqrt{2^{-j}}}\,\psi\left(\frac{t - 2^{-j}k}{2^{-j}}\right),$$

$$= 2^{\frac{j}{2}}\psi\left(2^{j}t - k\right).$$

Por ende, la señal resultante con su forma discreta es

$$w_x^j(k) = 2^{\frac{j}{2}} \int_{-\infty}^{\infty} x(t)\, \psi\left(2^j t - k\right) dt.$$

Para recuperar la señal original se tiene que

$$x(t) = \sum_{j=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} 2^{\frac{j}{2}} w_x^j(k) \psi\left(2^j t - k\right).$$

Lo anterior, indica que cada señal se puede ver como la unión de los diferentes niveles de descomposición obtenidos por la familia con la que interactúa. En la Figura 2.5 se aprecia la descomposición según la resolución que se tiene [27], [31], [32]. El escalado de la DWT genera múltiples resoluciones para analizar la señal, tanto en el dominio del tiempo como en el dominio de la frecuencia [27].

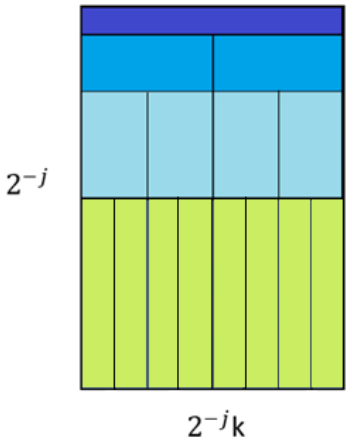


Figura 2.5. Descomposición de una señal.

Gracias a que las Wavelets son funciones pasa banda, el cambio de escala genera también un desplazamiento en frecuencia. Con la DWT se logra que las diferentes escalas generen ventanas de observación en la frecuencia que no se traslapan; sin embargo, para llegar a las frecuencias ubicadas cerca del origen se deben considerar infinitos valores de escala. El límite superior de las frecuencias no es un inconveniente dado que, como se explicó anteriormente, se tiene una frecuencia máxima igual a la mitad de la frecuencia de muestreo [27], dicho inconveniente se puede apreciar en la Figura 2.6 (a)

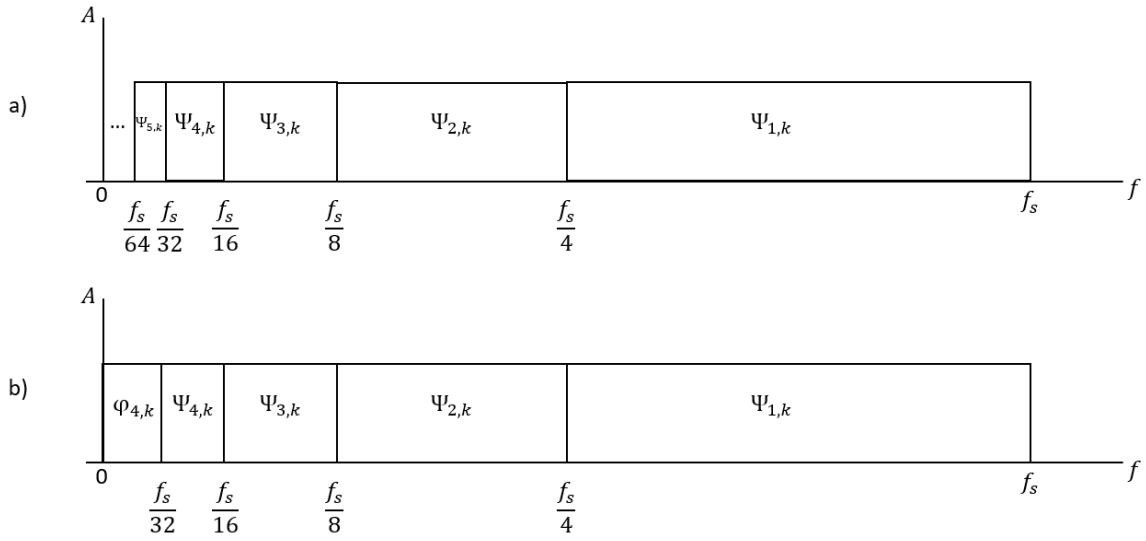


Figura 2.6. Descomposición Wavelet con y sin Scaling.

El análisis multiresolución complementa la definición inicial de la DWT definiendo una nueva función llamada Scaling, $\varphi(\mathrm{t})$. Esta función se acopla al esquema planteado de la Wavelet, debido a su ubicación en banda base [27], [32], i.e., su área bajo la curva no es cero, no obstante, el espacio de acción de una función Scaling se enfoca en la información de baja frecuencia, como se observa en la Figura 2.6 (b), la cual contiene gran cantidad de datos de la señal a analizar. En algunos textos, las funciones Scaling son llamadas coeficientes de aproximación, mientras que las funciones Wavelet se nombran coeficientes de detalles [33], [34].

2.4.1. Descomposición con la DWT

Para garantizar el cumplimiento del teorema de la energía de Rayleigh, i.e., que se conserve la información de la señal sin que exista redundancia, se deben utilizar familias Wavelet ortogonales [27], [32]. Así, para dos niveles de descomposición diferentes, j y m, se cumple que [32]

$$\psi_{j,k} \cap \psi_{m,k} = \emptyset, \qquad j \neq m,$$

donde, $\psi_{j,k}$ y $\psi_{m,k}$ son los subespacios generados por la Wavelet en las escalas j y m. En la Figura 2.7 se muestra gráficamente el aporte de cada uno de los subespacios cuando se asume que la familia Wavelet es ortogonal.

Por otro lado, como se muestra en la Figura 2.7 la Wavelet $\psi_{j,k}$ y su Scaling φ_j[11] generan subespacios que no se traslapan, dado que el producto interno entre las

[11] Las dos funciones se encuentran en una escala j, es decir, se encuentran en el mismo nivel de descomposición.

dos es cero y, por ende, son ortogonales. No obstante, la Scaling φ_j no es ortogonal con la Wavelet $\psi_{j-1,k}$, dado que la Wavelet está contenida dentro de la Scaling.

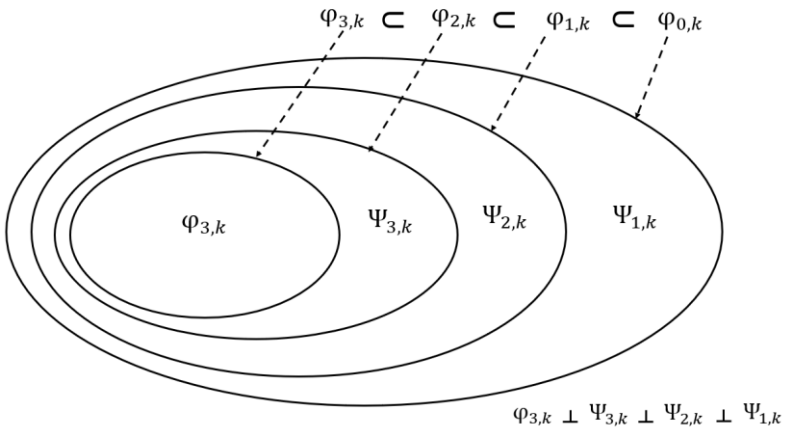


Figura 2.7. Subespacios Wavelet y Scaling.

Una forma más intuitiva de abordar la descomposición en subespacios alcanzada con la DWT es a partir de las gráficas del espectro. En la Figura 2.6 parte b[12] se muestran superpuestos los espectros de magnitud de una Scaling y de Wavelets a diferentes escalas, gracias a lo cual se observa que cada una de estas funciones se encuentra en un rango de frecuencias diferente y, por lo tanto, aporta información complementaria para la caracterización de una señal.

Lo anterior implica que para reconstruir una señal se debe contar con los coeficientes Scaling del nivel de descomposición j y los coeficientes Wavelet de los niveles menores o iguales a j. Así, en una descomposición a tres niveles la señal reconstruida se obtiene a partir de [27], [32] $\left((\varphi_3 \cup \psi_3) \cup \psi_2\right) \cup \psi_1$.

2.5. Algoritmo de Mallat

Para la implementación práctica de la DWT es utilizado el algoritmo de Mallat [27], [35], el cual a través de un banco de filtros de Respuesta al Impulso Finita (FIR, *Finite Impulse Response*) crea un algoritmo con estructura de árbol (iterativo) capaz de generar la descomposición a múltiples escalas [27], [36]

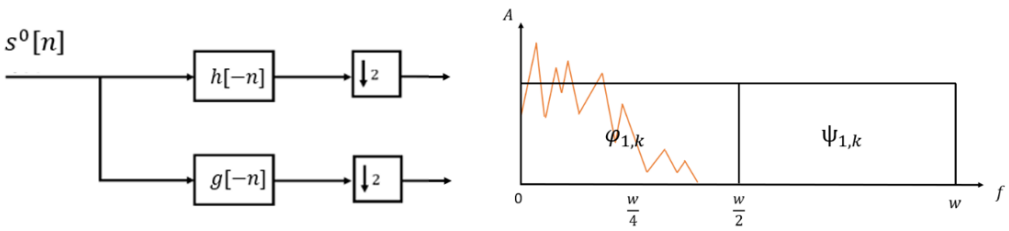


Figura 2.8. Algoritmo de Mallat y partición del espectro para un nivel de descomposición.

[12] Para la construcción de esta figura se normalizaron los espectros por facilidad.

La estructura básica del algoritmo a un nivel de descomposición se muestra en la Figura 2.8, donde $s_o[n]$ es la señal por analizar, $h[-n]$ es el filtro que utiliza como base la Wavelet a esa escala y $g[-n]$ es el filtro asociado a la Scaling. Los coeficientes resultantes para los k desplazamientos de la Wavelet de primer nivel, son representado con $\psi_{1,k}$ y para la Scaling con $\varphi_{1,k}$. Como se observa, para un nivel de descomposición el espectro se divide a la mitad, donde las frecuencias altas van a ser captadas por la Wavelet y las bajas por la Scaling.

El carácter iterativo del algoritmo de Mallat[13] permite obtener las funciones Wavelet y Scaling de un nivel de descomposición $j+1$ a partir de la Scaling del nivel j. Por lo anterior, a la señal de entrada se le suele considerar como coeficientes Scaling a un nivel de descomposición 0, $s_o(n)$ [27]. Los coeficientes Scaling se conocen también como coeficientes de aproximación y los coeficientes Wavelet como coeficientes de detalles.

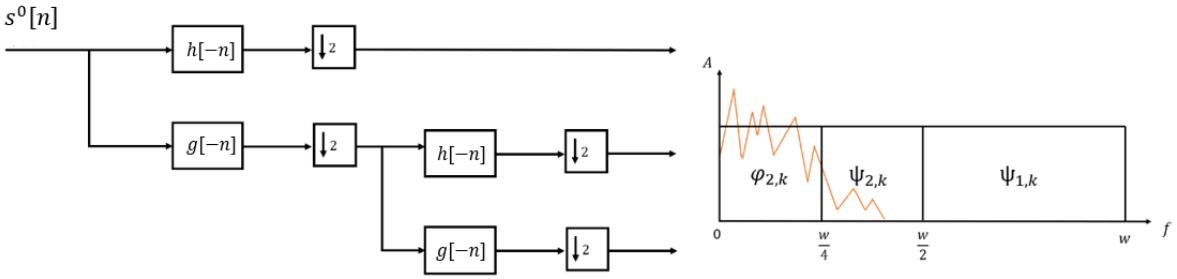


Figura 2.9. Algoritmo de Mallat y partición del espectro para dos niveles de descomposición.

En la Figura 2.9 se muestra el algoritmo de Mallat para dos niveles, a partir de la cual se observa que la división del espectro ocurre cada vez más cerca al origen. Esta nueva división no afecta a los coeficientes Wavelet de primer nivel, $\psi_{1,k}$, sino que a partir de los coeficientes Scaling $\varphi_{1,k}$ genera los coeficientes $\psi_{2,k}$y $\varphi_{2,k}$ de segundo nivel. Lo anterior muestra el carácter iterativo de la DWT [27].

La estructura del algoritmo de Mallat es adaptable para analizar señales de dos dimensiones (2D), para lo cual se genera un leve cambio, i.e., se realiza el proceso primero sobre las filas y posteriormente sobre las columnas de la matriz que representa a la señal 2D, de esta forma se obtienen 4 coeficientes diferentes [37], como se apreciar en la Figura 2.10, donde:

CD: coeficientes diagonales.
CV: coeficientes verticales.

[13] Existen variaciones sobre la estructura clásica del algoritmo de Mallat, las cuales conducen a diferentes divisiones del espectro. *Los paquetes Wavelet* es una de las modificaciones más conocida del algoritmo de Mallat.

CH: coeficientes horizontales.
CA: coeficientes de aproximación.

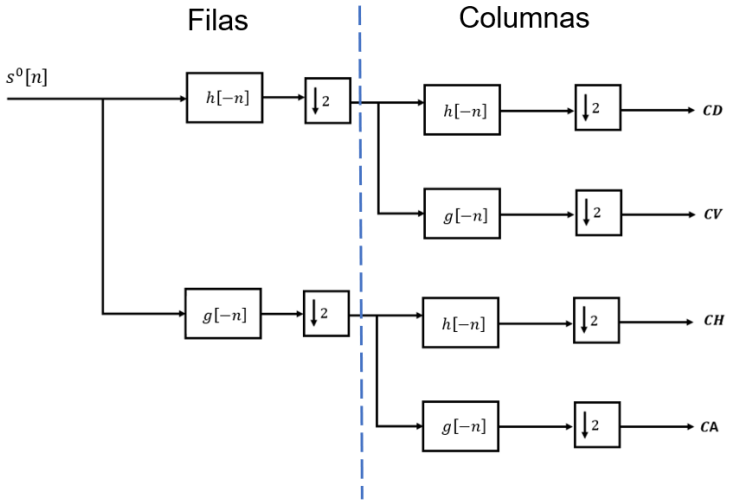


Figura 2.10. Algoritmo de Mallat en 2 dimensiones.

En la Figura 2.11 se muestra el resultado de aplicar el algoritmo de Mallat sobre una imagen.

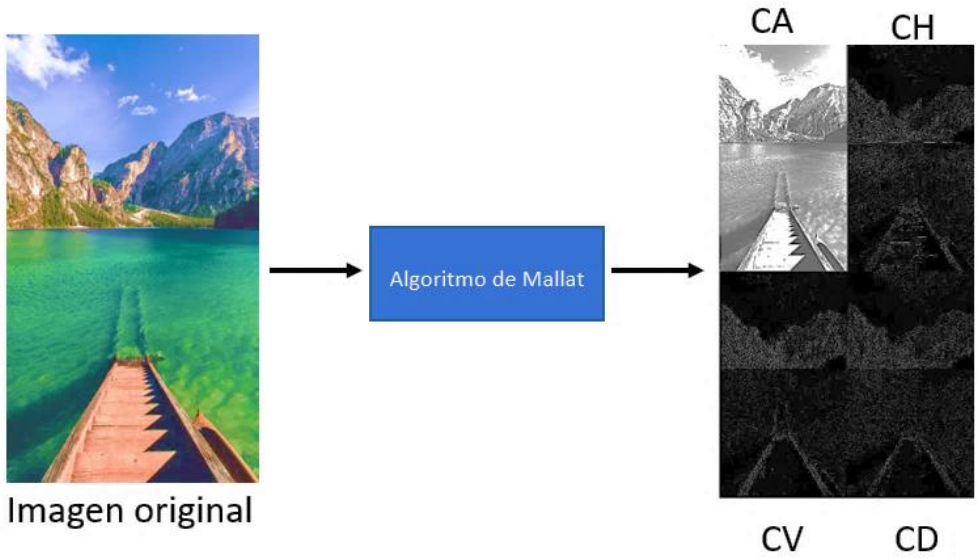


Figura 2.11. Algoritmo de Mallat aplicado en una imagen.

Como se observa en la Figura 2.11, los coeficientes de aproximación (CA) que se obtienen al descomponer la imagen son aquellos que poseen la mayor cantidad de información de la señal, sirviendo como un punto clave para aplicar de manera reiterativa el algoritmo. Algo para tener en cuenta es que la operación representada gráficamente como ↓2 en la Figura 2.10, hace referencia a realizar una disminución de la cantidad de muestras a la mitad, como esto ocurre tanto en filas como en

columnas, en este caso, cada grupo de coeficientes es la cuarta parte del tamaño de la imagen original. En consecuencia, a medida que se aumenta el número de niveles de descomposición, i.e., se descomponen los CA, se obtienen grupos de coeficientes cada vez más pequeños.

2.6. Limitaciones del Algoritmo de Mallat

2.6.1. Alta capacidad de memoria

Debido a la manera en la que las Wavelets interactúan con las señales, los coeficientes resultantes poseen valores que tienden a ser decimales, los cuales requieren una mayor cantidad de memoria para ser almacenados [38]. Modificar estos decimales genera pérdidas en la información, lo que se traduce en la aparición de ruido o distorsión en la señal recuperada. Por ello, para garantizar una mayor precisión en los valores de los coeficientes resultantes se requiere de un aumento en la capacidad de memoria [39], [40].

2.6.2. Alta capacidad de procesamiento

Debido a que la construcción de las funciones Wavelet y Scaling se realiza a partir de filtros, la DWT basa su funcionamiento en convoluciones sucesivas, por lo que, en su implementación se debe considerar el tiempo que toma calcular los coeficientes de dichos filtros y el manejo de la respuesta transitoria de éstos [38],[40].

En conclusión, aunque la DWT es una herramienta muy potente y versátil para el análisis de señales, gracias a la construcción de familias Wavelet de segunda generación[14], existen alternativas para su implementación que solventan las limitaciones del algoritmo de Mallat y, por lo tanto, brindan mejoras tanto en rendimiento como en su forma de aplicación.

2.7. Lifting Wavelet Transform

Al igual que el algoritmo de Mallat, la Transformada Wavelet Discreta usando Lifting (LWT, *Lifting Wavelet Transform*) pretende encontrar una manera de implementar la DWT y, con esto, encontrar los coeficientes del dominio Wavelet, además de brindar ciertas ventajas en comparación a Mallat, como son sus cortos tiempos de ejecución, el costo computacional, mayor facilidad para construir familias, análisis de bordes y la posibilidad de implementar la transformada Wavelet entera, lo cual le da un manejo más amigable al analizar los coeficientes, los cuales guardan de manera intrínseca la información de la señal original.

[14] Se hace referencia a Wavelet biortogonales

Si el conjunto de funciones base es ortogonal, se cumple que la energía permanece invariante, i.e., se conserva la información de la señal sin que exista pérdida o redundancia, por ello a partir del algoritmo de Mallat se crearon familias Wavelets ortogonales [41], [42],[43]. En la parte (a) de la Figura 2.12 se muestran las divisiones sobre el espacio de la señal, las cuales, en este caso, resultan de implementar tres niveles de descomposición y familias Wavelet ortogonales; mientras que en la parte (b) de la Figura 2.12 se muestran las divisiones en caso de usar familias Wavelet que no son ortogonales, las áreas sombreadas corresponden al traslape existente entre las divisiones, lo cual genera que la señal en el dominio Wavelet tenga información redundante y, por lo tanto, tenga más energía que la señal en el dominio original.

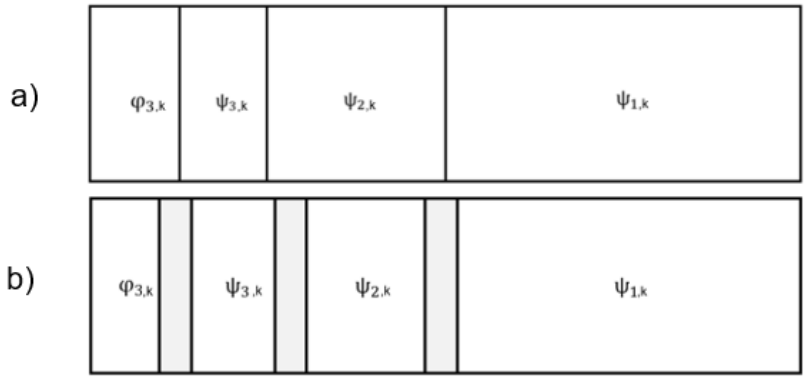


Figura 2.12. Distribución ortogonal y no ortogonal del espectro.

Crear los filtros para construir familias Wavelet que sean ortogonales es un proceso muy dispendioso dadas las restricciones impuestas por el algoritmo de Mallat, no obstante, las familias Wavelet construidas para ser implementadas de esta forma son llamadas Wavelet de primera generación [44]. En la Figura 2.13 se muestra que en el algoritmo de Mallat se hace uso de filtros acoplados para la descomposición y síntesis de la señal.

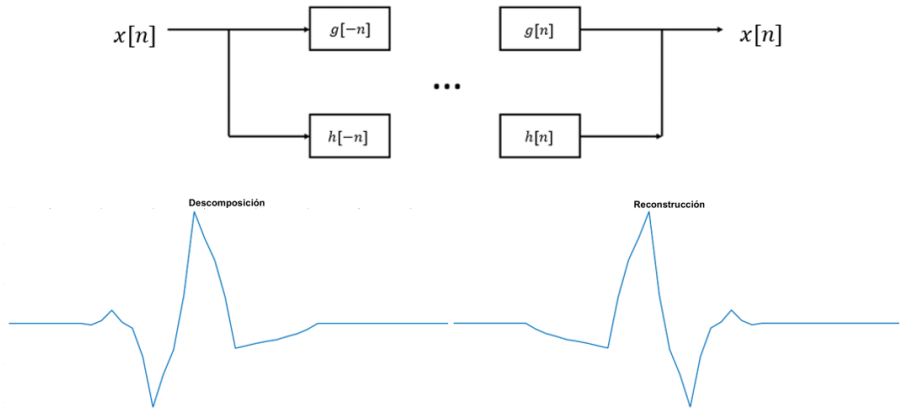


Figura 2.13. Algoritmo Mallat simplificado.

Con el fin de flexibilizar las restricciones de las familias Wavelet ortogonales nacen las Wavelets de segunda generación, las cuales se conocen como Wavelets biortogonales. La diferencia estriba en que con las familias biortogonales se tienen dos pares distintos de funciones, para la descomposición y la síntesis la señal original [41]. En la Figura 2.14 se ejemplifica el funcionamiento de las familias biortogonales, a partir de la cual se obtiene que la flexibilización de la segunda generación radica en que para la descomposición se cumple que $g[n]$ y $h[n]$ son ortogonales, pero para la síntesis se tienen funciones diferentes, $\tilde{g}[n]$ y $\tilde{h}[n]$, las cuales deben cumplir únicamente la ortogonalidad entre ellas [41].

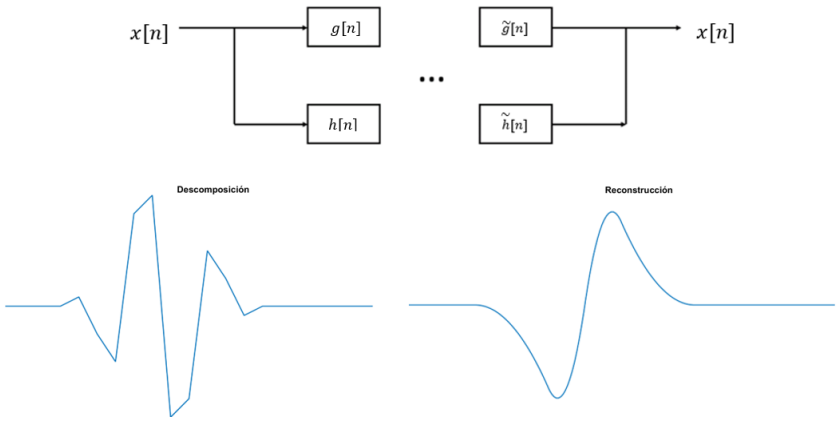


Figura 2.14. Señales biortogonales.

Dado el caso anterior, surge la alternativa al algoritmo de Mallat, para poder implementar aquellas Wavelets que son biortogonales.

2.7.1. Transformada perezosa Wavelet

La Transformada Perezosa Wavelet (LZWT, *Lazy Wavelet Transform*), es un proceso que separa las muestras pares de la señal de las muestras impares, por medio de submuestreos [45].

2.7.2. Algoritmo de predicción (P)

Los coeficientes Wavelet, $\boldsymbol{d^1}$, se obtienen a partir del algoritmo de predicción, $\boldsymbol{P}$, el cual se basa en la gran correlación existente entre las muestras pares e impares que arroja la LZWT [45].

2.7.3. Algoritmo de actualización (U)

La Scaling surge como un complemento de las Wavelets en el análisis multiresolución, por lo que en el algoritmo Lifting se hace uso de $\boldsymbol{U}$ para obtener los coeficientes Scaling, $\boldsymbol{s^1}$, a partir de las muestras impares y los coeficientes $\boldsymbol{d^1}$ [45].

2.7.4. Esquema general

El algoritmo LWT se fundamenta en los tres algoritmos mencionados anteriormente, los cuales se encargan de calcular los coeficientes en los que se descompone la señal [39], [45]. El diagrama que define el algoritmo Lifting se aprecia en la Figura 2.15, en el cual los valores que definen a $\boldsymbol{P}$ y $\boldsymbol{U}$ son los que determinan la familia Wavelet con la que se va a trabajar.

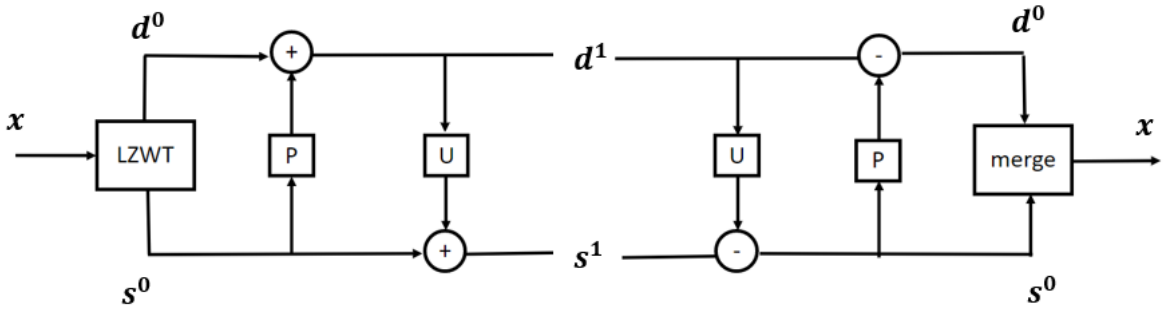


Figura 2.15. Estructura algoritmo Lifting.

Con el fin de presentar de forma más clara el funcionamiento del algoritmo LWT se procede a realizar un ejemplo conciso con los pasos a seguir, para esto se trabaja con los valores de $\boldsymbol{P}$ y $\boldsymbol{U}$ asociados a la Wavelet de Haar [41]. La primera sección es la LZWT, así, la señal

$$\boldsymbol{x} = [7,2,9,5,3,1,0,4],$$

se separa en dos vectores, los cuales contienen las muestras pares, $\boldsymbol{d^0}$, y las impares, $\boldsymbol{s^0}$, así

$$\boldsymbol{d^0} = [2,5,1,4],$$

$$\boldsymbol{s^0} = [7,9,3,0].$$

Para obtener $\boldsymbol{d^1}$ se debe utilizar $\boldsymbol{P}$, el cual para el caso de la Wavelet de Haar es una constante igual a -1, así

$$\boldsymbol{d^1} = \boldsymbol{d^o} - \boldsymbol{s^o}.$$

Por su parte, $\boldsymbol{U}$ en este caso también es una constante, pero con valor igual a 0.5, por lo que para obtener $\boldsymbol{s^1}$ se tiene que

$$\boldsymbol{s^1} = \boldsymbol{s^o} + \frac{1}{2}\boldsymbol{d^1},$$

$$= \frac{1}{2}(\boldsymbol{d^0} + \boldsymbol{s^0}).$$

El proceso anteriormente descrito se puede condensar por medio de su representación matricial, i.e.,

$$\begin{bmatrix} 1 & 1/2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} \boldsymbol{s^0} \\ \boldsymbol{d^0} \end{bmatrix} = \begin{bmatrix} \boldsymbol{s^1} \\ \boldsymbol{d^1} \end{bmatrix}$$

$$\begin{bmatrix} 1/2 & 1/2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} \boldsymbol{s^0} \\ \boldsymbol{d^0} \end{bmatrix} = \begin{bmatrix} \boldsymbol{s^1} \\ \boldsymbol{d^1} \end{bmatrix}$$

$$\begin{bmatrix} \frac{1}{2}(\boldsymbol{d^0} + \boldsymbol{s^0}) \\ \boldsymbol{d^0} - \boldsymbol{s^0} \end{bmatrix} = \begin{bmatrix} \boldsymbol{s^1} \\ \boldsymbol{d^1} \end{bmatrix}$$

Esta variación del análisis es lo que permite que se optimice el algoritmo en sí, ya que se cambia el enfoque de aplicar un conjunto de pasos de manera secuencial, por un grupo de multiplicaciones matriciales.

Con el fin de validar la equivalencia de las diferentes formas de descomposición se usa un caso práctico, en el cual se calculan tanto los coeficientes Wavelet como los Scaling, para esto en MATLAB se implementan: el sistema de ecuaciones de $\boldsymbol{P}$ y $\boldsymbol{U}$, el método matricial del algoritmo Lifting, la función de descomposición Lifting y el algoritmo de Mallat[15]; los resultados se muestran gráficamente en las Figuras 2.16 y 2.17.

[15] Herramientas propias de MATLAB.

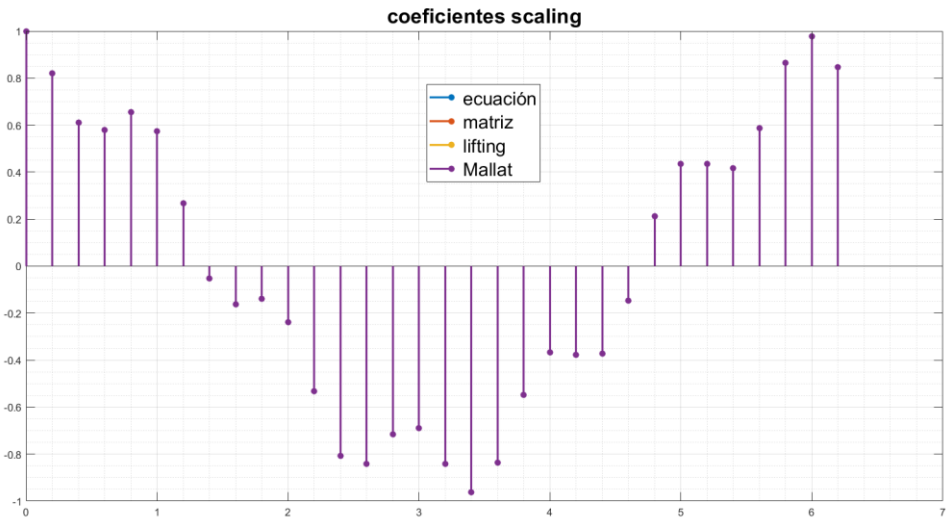


Figura 2.16. Coeficientes Scaling obtenidos por ecuaciones, matrices, algoritmo Lifting y Mallat.

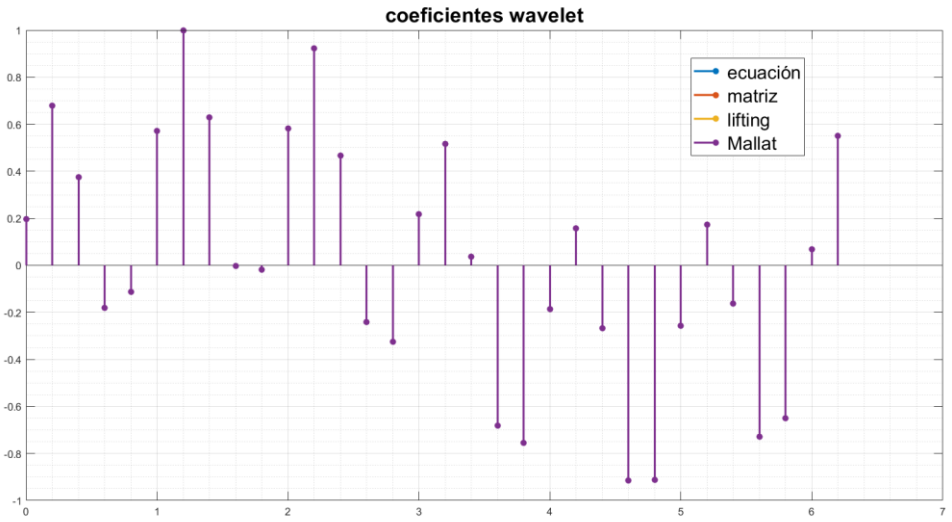


Figura 2.17. Coeficientes Wavelets obtenidos por ecuaciones, matrices, algoritmo Lifting y Mallat.

Como se aprecia en las Figuras 2.16 y 2.17, para los 4 casos no se presentan variaciones en los valores de los coeficientes Scaling y Wavelet, mostrando que para el caso de la familia Wavelet de Haar es indistinto el mecanismo por medio del cual se decida hacer la implementación de la DWT.

Un punto clave para tener en cuenta en el algoritmo Lifting es que éste permite implementar la transformada Wavelet entera, la cual, por motivos de optimización y mejora en su manejo, se implementa ajustando los valores que caracterizan tanto a $\boldsymbol{P}$ como a $\boldsymbol{U}$, permitiendo que los coeficientes de la señal, $\boldsymbol{d^1}$ y $\boldsymbol{s^1}$, sean

exclusivamente números enteros. Los ajustes sobre $\boldsymbol{P}$ y $\boldsymbol{U}$ también se verían reflejados en las dos matrices que representan la respuesta del sistema.

Finalmente, la DWT contempla la posibilidad de variar el número de niveles de descomposición, para lo cual el algoritmo Lifting básico se debe aplicar de forma iterativa, así, en la Figura 2.18 se representa al bloque LWT como el ensamble de los algoritmos LZWT, $\boldsymbol{P}$ y $\boldsymbol{U}$.

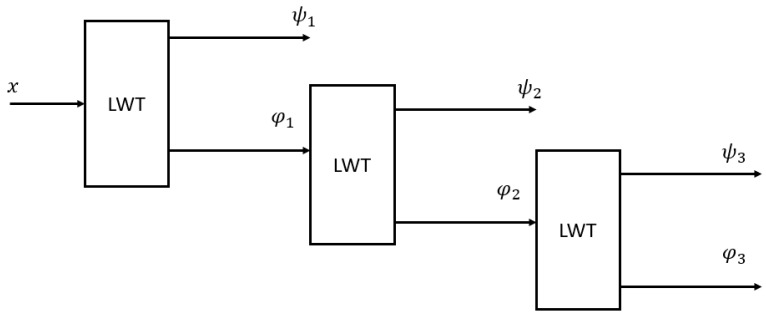


Figura 2.18. Algoritmo Lifting en cascada.

Gracias a lo previamente mencionado, el paralelo entre el algoritmo de Mallat en 2D y el algoritmo LWT en 2D se representa en la configuración mostrada en la Figura 2.19.

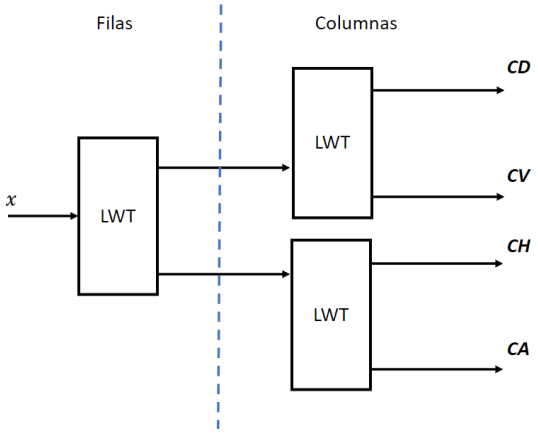


Figura 2.19. Algoritmo de Mallat con LWT.

CAPÍTULO 3: DISEÑO

3.1. Metodología

La metodología utilizada para poder llevar a cabo el desarrollo de este trabajo de grado se conoce como *tres ciclos de la investigación* [46]. Esta metodología se basa en la implementación simplificada de tres secciones o ciclos. El primer ciclo, o ciclo de relevancia, se encarga de dar el enfoque necesario para reunir los requerimientos y métodos de evaluación; el segundo ciclo, conocido como ciclo de rigor, busca la apropiación del conocimiento necesario para poder cumplir dichos requisitos; finalmente, el ciclo de diseño se apoya en los otros dos con el fin de obtener los mejores resultados. En este trabajo de grado se propone la realización de tres iteraciones de los tres ciclos de investigación, en pro de trabajar en paralelo la implementación de las actividades planteadas. El diagrama de la metodología *tres ciclos de la investigación* es mostrado en la Figura 3.1.

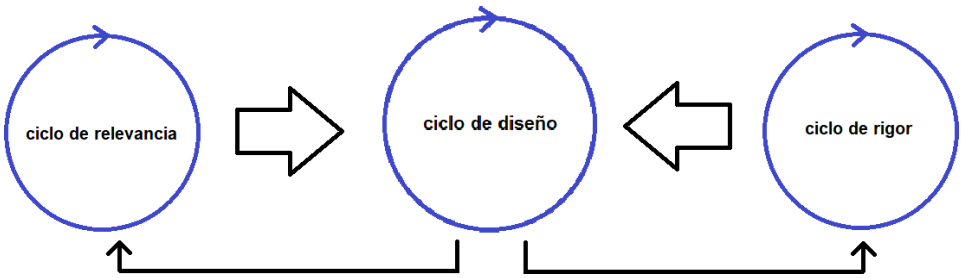


Figura 3.1. Diagrama de la metodología Tres ciclos de la investigación.

El capítulo 3 se organiza con base en el diagrama de bloques de un algoritmo de esteganografía en imágenes (ver Figura 3.2), detallando sobre cómo se lleva a cabo la implementación de cada uno de estos procesos.

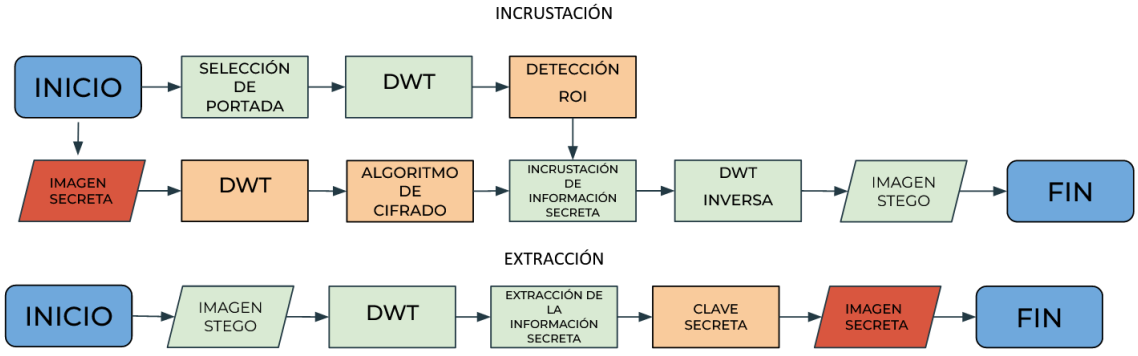


Figura 3.2. Algoritmo de esteganografía para inserción y extracción de la información.

Cabe resaltar que dicha implementación no fue realizada en el orden presentado por el diagrama de la Figura 3.2, sino que, de acuerdo con la metodología utilizada, se han realizado los procesos en paralelo y de manera modular[16]. Por otra parte, los resultados obtenidos en algunos procesos se han iterado a procesos previos o posteriores a fin de obtener mejores resultados.

3.2. Selección de la Imagen Portada

En esta sección se analiza el impacto de la imagen portada en el proceso de esteganografía desde un punto de vista funcional, es decir, se realizan variaciones de la imagen portada y se verifica la integridad de los datos de la imagen secreta recuperada, por lo que es necesario realizar los pasos del diagrama mostrado en la Figura 1.8 y sus procesos inversos. Además de esto, es importante aclarar que la comparación a realizar se efectúa entre la imagen secreta antes de incrustarla en la imagen portada y la imagen resultante de extraer la imagen secreta de la imagen estego, es decir, la integridad de los datos en estas pruebas indica la similitud entre la información secreta enviada (imagen secreta antes de incrustar) y la información obtenida al finalizar el proceso (imagen resultante tras extracción). Cabe aclarar que la medida utilizada para evaluar dicha integridad es la comparación pixel a pixel, esto es, el porcentaje de igualdad obtenido al comparar los valores de los pixeles de la imagen secreta antes y después de incrustarla en la imagen portada. A continuación, se muestra un ejemplo de una comparación pixel a pixel entre estas dos imágenes.

Tabla 3.1. Matrices Imagen secreta original e Imagen secreta tras extracción.

Imagen Secreta Original	Imagen secreta tras extracción

[16] Las funciones no dependen de otras.

255	120	255	110
100	0	100	0

La Tabla 3.1 muestra las matrices de las imágenes a utilizar, cada una de ellas de 2×2 pixeles, los cuales se concatenan en un vector, como se ve en la Tabla 3.2.

Tabla 3.2. Vectores columna de Imagen secreta original e Imagen secreta tras extracción.

Vector Imagen Secreta Original	Vector Imagen secreta tras extracción
255	255
100	100
120	110
0	0

La comparación lógica se realiza entre cada una de las posiciones de los vectores, es decir, si los pixeles son iguales, se suma un 1 al conteo. Una vez finalizado el proceso, se divide el valor de ese conteo con el número de pixeles de la imagen portada y se multiplica por 100 para obtener el porcentaje de igualdad, el cual, para este ejemplo, es de 75%.

Con el algoritmo planteado se pretende obtener un porcentaje del 100% de igualdad, o valores muy cercanos, lo cual indica una recuperación total de la imagen secreta. Para alcanzar el objetivo anterior, es indispensable utilizar una imagen portada que permita un ocultamiento con mínimas pérdidas, es por ello por lo que, para llevar a cabo la selección de las imágenes portada, se han realizado pruebas[17] teniendo en cuenta los siguientes criterios:

- Tamaño en pixeles.
- Propiedades de la imagen:
  1. Contraste.
  2. Saturación.
  3. Exposición.

3.2.1. Tamaño en pixeles

El tamaño de una imagen se determina de a partir de su cantidad de pixeles, es decir, el número de elementos de la matriz $N \times M$, e.g., para las imágenes de la Figura 3.2 se tiene que la imagen 1 tiene 1'048.576 pixeles y la imagen 2 tiene 262.144 pixeles.

[17] Estas pruebas se realizan con 3 LSB.

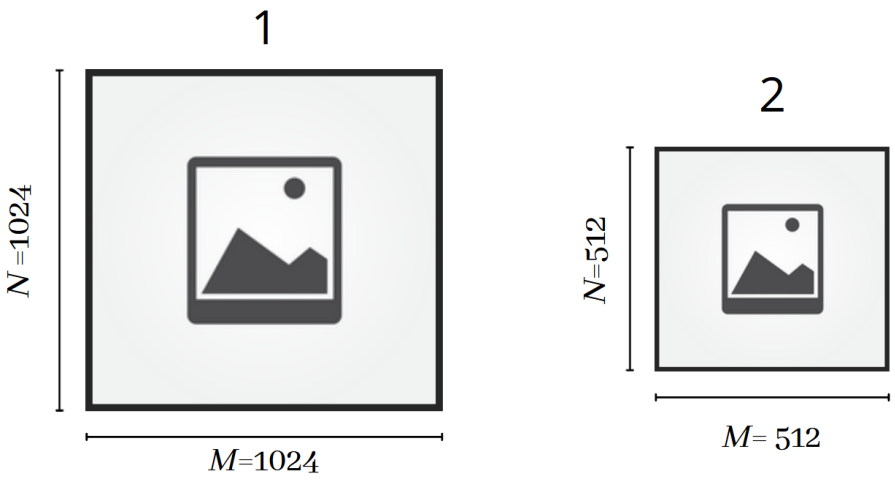


Figura 3.3. Tamaños de imagen.

En el ejemplo mostrado en la Figura 3.3 se tiene que la imagen 2 es la cuarta parte de la imagen 1, por lo que para hacer la inserción se tendría que modificar completamente un cuarto de los pixeles de la imagen 1 o los últimos dos bits de todos los pixeles de la imagen 1. Cabe resaltar que entre mayor sea la diferencia de tamaños entre estas dos imágenes mayor será la imperceptibilidad de las alteraciones de la imagen estego, por lo que en la sección 3.5.3 se busca determinar la relación entre los tamaños de la imagen portada y la imagen secreta, para garantizar una alta capacidad de incrustación sin afectar los resultados de imperceptibilidad.

3.2.2. Propiedades de la imagen

Para determinar la influencia de cada una de la saturación, el contraste y la exposición en la selección de la imagen portada, se realizan pruebas variando cada una de estas propiedades en la imagen portada; y, tras realizar el proceso esteganográfico, se compara la imagen secreta resultante con la imagen secreta original, estas pruebas se detallan en el Apéndice A.

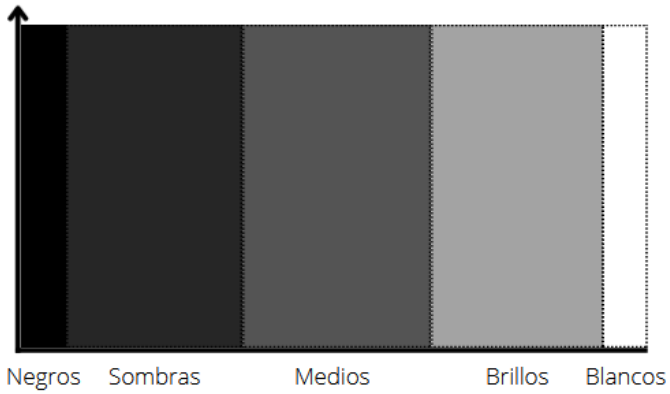


Figura 3.4. Distribución de tonos en una imagen en escala de grises.

Los resultados encontrados muestran que, para el algoritmo planteado, se busca que la imagen portada tenga un bajo contraste, es decir, que sus pixeles tengan valores intermedios (sombras, medios y brillos), evitando los tonos blancos (valores cercanos a 255) y negros (valores cercanos a 0). La distribución de pixeles de una imagen en escala de grises se muestra de manera gráfica en la Figura 3.4.

Así, para las pruebas de este trabajo de grado se seleccionan 6 imágenes portada con distintos niveles de grises (ver Tabla 3.3), la Figura 3.5 muestra las imágenes portadas a utilizar.

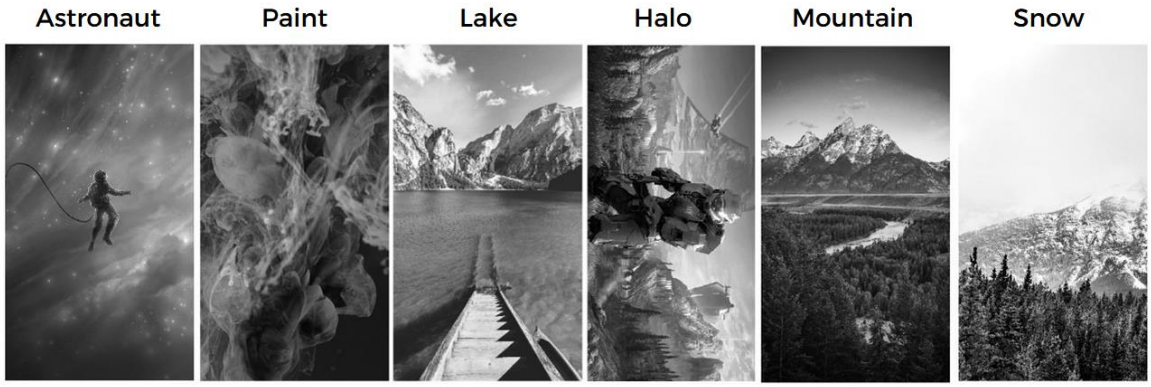


Figura 3.5. Imágenes Portada utilizadas.

La Tabla 3.3 muestra la distribución de los tonos de las 6 imágenes portadas, las cuales poseen porcentajes de grises desde 82.31% (imagen *Snow)* hasta 99.97% (imagen *Astronaut*).

Tabla 3.3. Distribución de pixeles de las imágenes portada.

Nombre de la imagen Portada	% Gris	% Negro	% Blanco
Astronaut	99.9777	0.0033034	0.0190
Halo	96.8034	2.7859	0.4107
Lake	97.8941	0	2.1059
Mountain	97.9826	2.0169	0.0005
Paint	99.9616	0.038436	0
Snow	82.3121	4.2726	13.4154

3.3. Selección de Imagen Secreta

Con el fin de determinar las características que deben tener las imágenes secretas para ser usadas con el algoritmo planteado, se realiza una prueba que consiste en determinar si es posible recuperar 6 imágenes secretas de 225×225 (ver Figura 3.6), a partir de 6 imágenes estego. Para esto se utiliza la combinación de 6

imágenes[18] portada de 2160×3840 (ver Figura 3.5) y las 39 familias Wavelets[19] a dos niveles de descomposición.

Figura 3.6. Imágenes Secretas utilizadas.

3.3.1. Análisis respecto a la imagen portada

Para realizar un análisis con mayor objetividad, se utilizan las 6 imágenes portada seleccionadas, con el fin de determinar si esta característica influye en la integridad de los datos de las distintas imágenes secretas; las Figuras 3.4 y 3.5 muestran las imágenes a utilizar.

Inicialmente, se guarda cada una de las 6 imágenes secretas en cada una de las 6 imágenes portada utilizando cada una de las posibles combinaciones de las 39 familias Wavelet a dos niveles de descomposición. En la Figura 3.6 se muestra el promedio de porcentaje de igualdad resultante para cada imagen portada y para cada imagen secreta, tras la comparación bit a bit de las imágenes secretas.

[18] El algoritmo planteado convierte las imágenes a escala de grises, al promediar el valor de cada pixel en cada una de sus tres matrices R, G y B. Esto se realiza con el fin de optimizar el tiempo de ejecución de las pruebas realizadas.
[19] Se usan las 39 familias Wavelet con las que se puede trabajar en MATLAB bajo el algoritmo Lifting.

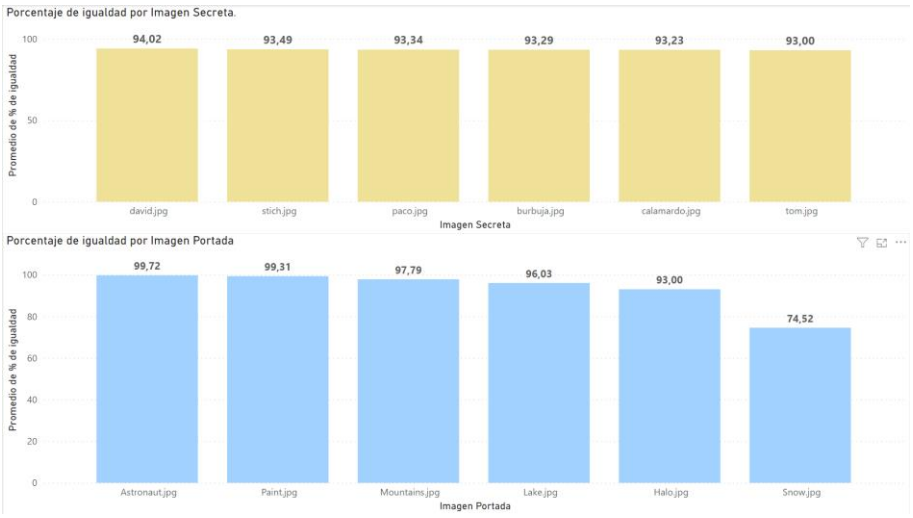


Figura 3.7. Porcentajes de igualdad promedio para imágenes portada e imágenes secretas.

La Figura 3.7 muestra que los porcentajes de igualdad promedio en las imágenes secretas no presentan variaciones significativas entre ellas. Por el contrario, el promedio de porcentaje de igualdad para las imágenes portada es directamente proporcional al nivel de grises presente en cada imagen.

A continuación, se analiza el comportamiento del porcentaje de igualdad en las imágenes secretas, cuando se grafican los resultados obtenidos para una imagen portada en particular. Como primer ejemplo, se selecciona la imagen *Astronaut*, la cual es la que mantiene en mayor medida la integridad de los datos entre las 6 imágenes portada (99,72%) y se aprecia que el promedio de igualdad para cada imagen secreta se mantiene entre 99,68% y 99,75%, tal como se muestra en la Figura 3.8.

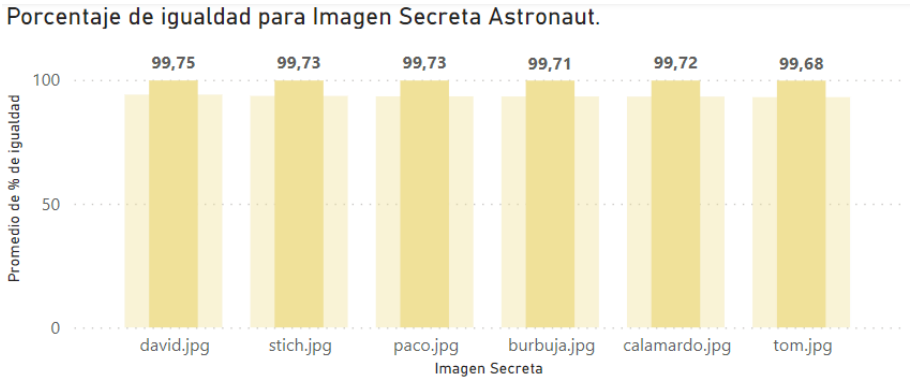


Figura 3.8. Promedios de porcentaje de igualdad para la portada *Astronaut*.

En seguida, se toma como ejemplo la imagen portada *Lake*, que tiene un promedio de igualdad de 96,03% y al graficar los promedios de igualdad por imagen secreta (Figura 3.9) se observa que este porcentaje varía entre 95,76% y 96,45%, lo cual

se considera una variación mínima teniendo en cuenta la cantidad de datos analizados.

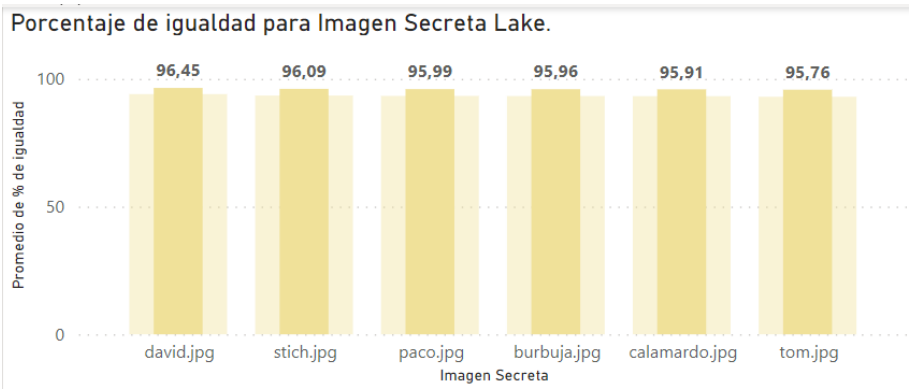


Figura 3.9. Promedios de porcentaje de igualdad para la portada *Lake*.

Para finalizar, se observan los resultados obtenidos en porcentaje de igualdad en las imágenes secretas tras usar *Snow* como imagen portada, la cual es la imagen portada con menor nivel de integridad entre las 6 imágenes portada usadas.

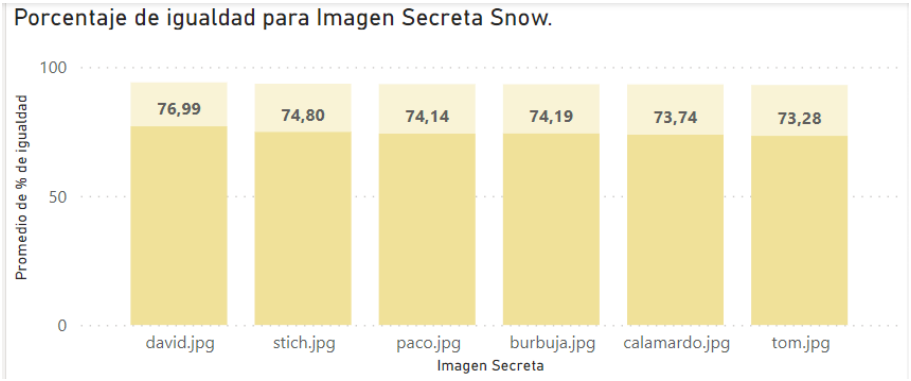


Figura 3.10. Promedios de porcentaje de igualdad para la portada *Snow*.

Los resultados mostrados en la Figura 3.10, indican que, aunque la imagen portada *Snow* presenta el promedio de porcentaje de igualdad más bajo que las demás imágenes portada, esta característica no representa una variación significativa en la integridad de los datos si se analizan las imágenes secretas individualmente.

Lo planteado anteriormente muestra que tras realizar pruebas con imágenes portada que entregan distintos resultados en porcentajes de igualdad, no se presentan variaciones significativas en la integridad de los datos de las 6 imágenes secretas. Por lo tanto, la integridad de los datos depende de la correcta selección de la imagen portada y es independiente de la selección de la imagen secreta, con lo cual se tiene un algoritmo esteganográfico que no impone limitaciones sobre las características de la información que se quiere proteger.

3.3.2. Análisis respecto a familias Wavelet

En esta sección se busca analizar los cambios en la integridad de la información de las imágenes secretas, respecto a la variación de la familia Wavelet. La implementación del algoritmo de esteganografía se realiza en la herramienta de simulación MATLAB, para la obtención de los coeficientes Wavelet se utiliza el algoritmo Lifting, dentro del cual es posible utilizar 39 familias Wavelet diferentes. Adicionalmente, con el fin de aumentar la aleatoriedad del algoritmo de esteganografía se realiza una variación al planteamiento original de la DWT, en la cual se cambia el tipo de familia para cada nivel de descomposición, por lo que en estas pruebas no es obligatorio que la familia utilizada en el primer nivel sea la misma para el segundo nivel.

En la Figura 3.11 se muestran los resultados promedio de igualdad en las imágenes secretas de acuerdo con la familia Wavelet utilizada en el primer nivel.

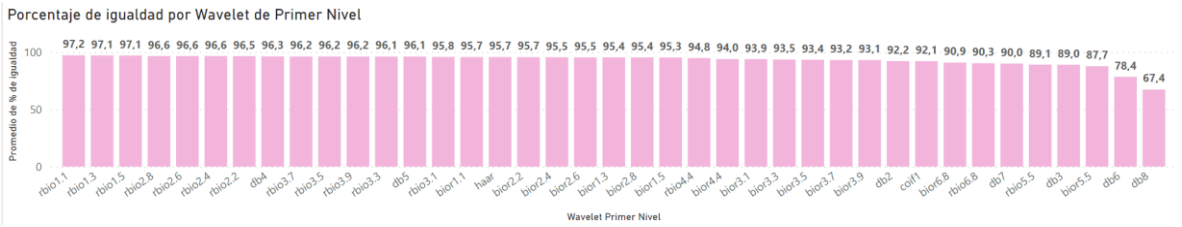


Figura 3.11. Porcentajes de igualdad promedio para Wavelets de primer nivel.

A continuación, se analiza los cambios en el promedio de igualdad de cada imagen secreta al tomar como ejemplo una Wavelet de primer nivel. Inicialmente se observan los porcentajes de igualdad tras usar la Wavelet *db7* en el primer nivel de descomposición, esta Wavelet presenta un promedio de porcentaje de igualdad de 90,1%. Teniendo esto en cuenta, se aprecia que la integridad de los datos en las imágenes secretas varía entre 90,15% correspondiente a la imagen *david* y 89,98% en la imagen *tom*, como se observa en la Figura 3.12, por lo que se puede afirmar que la integridad de los datos no es afectada de manera significativa al usar esta Wavelet.

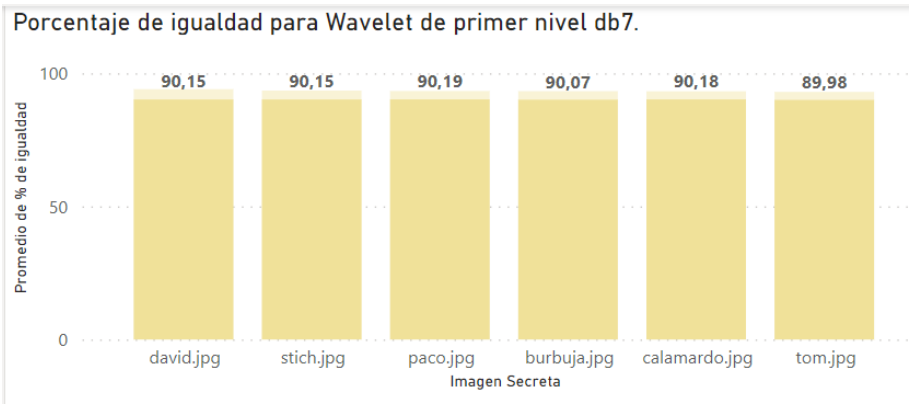


Figura 3.12. Promedio de porcentaje de igualdad en imágenes secretas usando db7.

De la misma manera, se analiza la familia Wavelet *Rbio1.1* para el primer nivel de descomposición, la cual presenta un promedio de igualdad de los datos secretos de 97,2%. En este caso, tras observar los porcentajes de igualdad de las imágenes secretas, se nota una fluctuación del porcentaje de igualdad entre 97,59% y 97,10% (ver Figura 3.13), es decir, las imágenes secretas no sufren cambios pronunciados cuando se usa esta Wavelet.

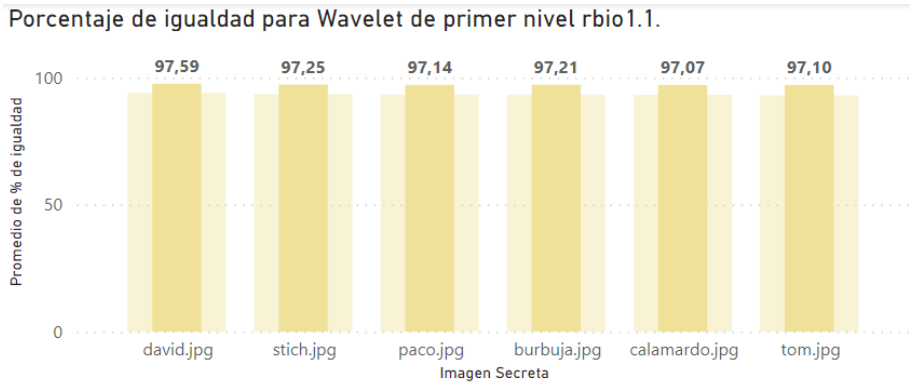


Figura 3.13. Promedio de porcentaje de igualdad en imágenes secretas usando Rbio1.1.

Tras determinar que ninguno de los dos ejemplos de las Wavelet de primer nivel representa cambios significativos en el porcentaje de igualdad de las imágenes secretas, se analiza el efecto de la familia Wavelet del segundo nivel de descomposición por medio de la misma comparación anterior; en la Figura 3.14 se ve representado el porcentaje de igualdad promedio tras usar cada una de las Wavelets de segundo nivel.

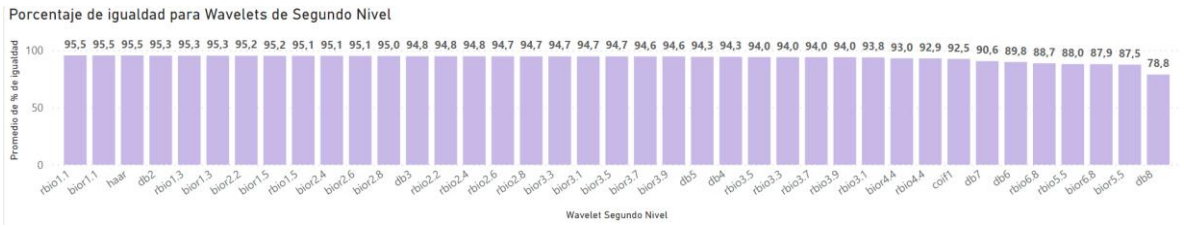


Figura 3.14. Porcentajes de igualdad promedio para Wavelets de segundo nivel.

Como primer ejemplo de Wavelet de segundo nivel, se toma el caso de la familia *Coif1*, la cual presenta un 92,5% de promedio en porcentaje de integridad de los datos secretos. La Figura 3.15 muestra que las imágenes secretas presentan cerca de 1% de diferencia en el porcentaje de igualdad entre el valor más alto (*david)* y el valor más bajo (*tom)*, este porcentaje se interpreta como bajo, i.e., ninguna de las imágenes secretas muestra un nivel de integridad diferente al de las otras imágenes secretas tras el uso de esta Wavelet.

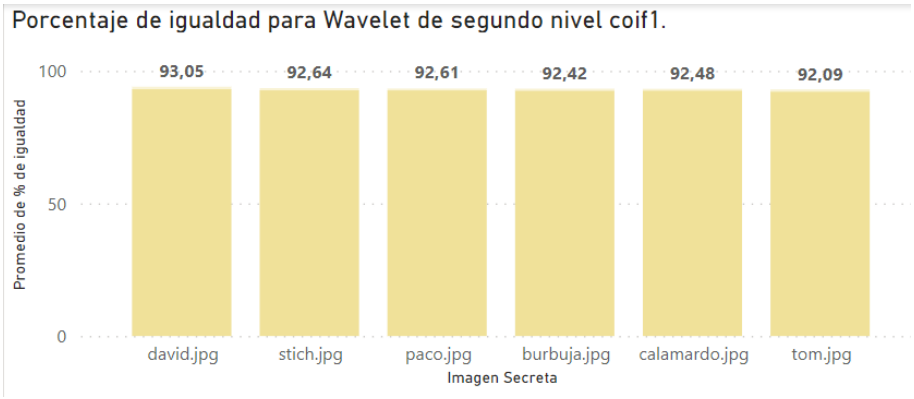


Figura 3.15. Promedio de porcentaje de igualdad en imágenes secretas usando Coif1.

Por último, se analizan los resultados de la Wavelet *Bior1.1* en segundo nivel, en este caso, el porcentaje de igualdad entre las imágenes secretas tienen una variación no superior al 0,9%, esto se evidencia de manera gráfica en la Figura 3.16.

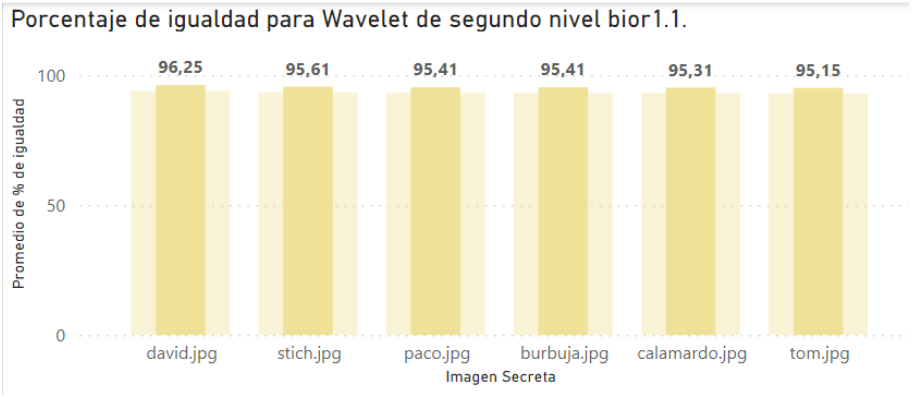


Figura 3.16. Promedio de porcentaje de igualdad en imágenes secretas usando Bior1.1.

Tras analizar cada una de las familias Wavelets de primer y segundo nivel de descomposición, se determina que para Familias Wavelets con porcentajes de igualdad promedio mayores al 90%[20] en el primer o el segundo nivel de descomposición, el porcentaje de igualdad promedio en las imágenes secretas no varía en más del 2%. Por lo tanto, la información a ocultar no afecta el desempeño del algoritmo en términos de integridad de la información cuando se varía entre uno y dos niveles de descomposición. No obstante, la elección de familias sí presenta un impacto en el porcentaje de igualdad de la imagen recuperada, por ello, en la sección 4.1, se realizan pruebas para determinar las combinaciones de familias Wavelets aptas para utilizar con el algoritmo planteado.

[20] Las familias que presentan promedios de igualdad menores al 90% no fueron tomadas en cuenta para este caso, ya que se considera ese porcentaje como un valor bajo.

3.4. Módulo Wavelet

En la implementación de la descomposición Wavelet, y al tener en cuenta lo explicado en las secciones 2.6 y 2.7, se opta por realizar un análisis comparativo entre el algoritmo de Mallat y el algoritmo Lifting, con el fin de tener una mayor certeza sobre la selección del algoritmo para implementar la DWT. Para poder darle una continuidad y utilidad de las posibilidades de cada algoritmo, se tienen en cuenta las siguientes directrices:

1. Recursividad: El algoritmo debe ser iterativo sobre los coeficientes de aproximación resultantes, y así adentrarse en un nivel más profundo.

2. Idoneidad: Los valores resultantes de los coeficientes de la descomposición deben ser adecuados para el módulo de inserción LSB.

3.4.1. Recursividad

Para implementar en MATLAB la DWT sobre imágenes utilizando el algoritmo de Mallat existe la función *dwt2*, la cual entrega en arreglos tipo celda los coeficientes resultantes de la descomposición.

$$COEFICIENTES = [CH_1, CV_1, CD_1, CA_1] \rightarrow 1\ NIVEL$$

$$COEFICIENTES = [CH_1, CV_1, CD_1, CH_2, CV_2, CD_2, CA_2] \rightarrow 2\ NIVEL$$

$$COEFICIENTES = [CH_1, CV_1, CD_1, CH_2, CV_2, CD_2, CH_3, CV_3, CD_3, CA_3] \rightarrow 3\ NIVEL$$

Para la manipulación de estos coeficientes se construye el módulo *dwt_multi_level*, dentro del cual se encuentra la función propia llamada *show_wav_decomposition*, la cual permite mostrar gráficamente los valores de los coeficientes, tal como se ejemplifica en la Figura 3.17. Adicionalmente, se valida que se pueda reconstruir la imagen original a partir de sus coeficientes.

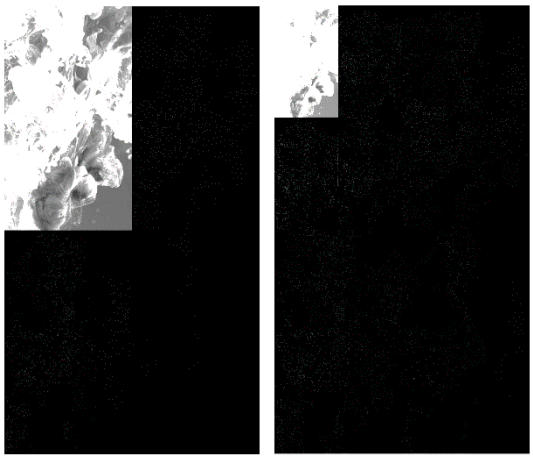


Figura 3.17. Descomposición Wavelet.

Por otro lado, para el uso del algoritmo Lifting, MATLAB cuenta con la función *lwt2*. Para este caso se crea el módulo *ldwt_v2*, el cual funcionaria de forma iterativa. El resultado de la descomposición con este algoritmo se muestra en la Figura 3.18.

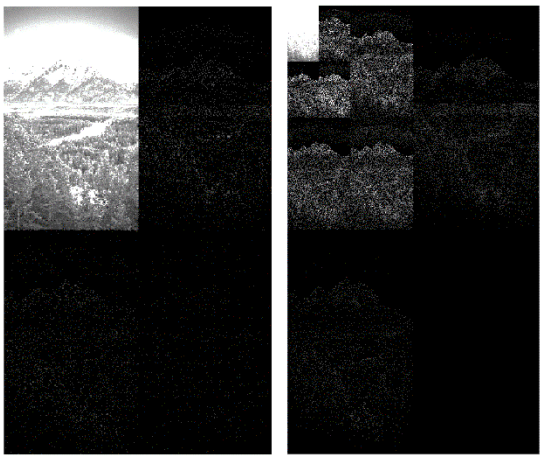


Figura 3.18. Descomposición Lifting.

Al igual que en el caso del algoritmo de Mallat, para el algoritmo LWT se valida que sea posible reconstruir la imagen original a partir de sus coeficientes. Al analizar los valores de estos coeficientes se tiene que, al escoger la opción de la *transformada Wavelet entera*, los valores de los coeficientes resultantes son números enteros exclusivamente.

3.4.2. Idoneidad

Dado que para el ocultamiento de la imagen secreta se utiliza el algoritmo LSB, los valores de los coeficientes resultantes de la descomposición Wavelet se deben representar por medio de una secuencia binaria, lo que implica que el número de valores únicos entre los coeficientes debe ser finito y menor al número de

posibilidades que admite un código de longitud fija L, es decir, 2^L. Por lo anterior, si los valores de los coeficientes son decimales se debe hacer un redondeo para limitar el número de posibles valores, lo que se traduce en un proceso de cuantificación y, por lo tanto, tiene asociado una distorsión sobre la información de la imagen.

En la Tabla 3.4 se muestra el número de coeficientes con valores decimales susceptibles a ser redondeados. Para cada una de las 6 imágenes portada de referencia se calcula el porcentaje de coeficientes que tienen un valor decimal, diferenciando la implementación de la DWT con el algoritmo de Mallat (*dwt2*) y el algoritmo Lifting (*ldwt2*). Los resultados muestran que utilizar la *transformada Wavelet entera* con el algoritmo Lifting evita la presencia de valores decimales y, por ende, del redondeo, facilitando la conversión a binario de estos valores y la posterior implementación del LSB. Por lo anterior, para este trabajo de grado se selecciona el algoritmo Lifting para la implementación de la DWT.

Tabla 3.4. Idoneidad, comparación dwt2 y ldwt2.

	Astronaut		Halo		Lake		Mountain		Paint		Snow	
Algoritmo / coeficientes	dwt2	ldwt2	dwt2	ldwt2	dwt2	ldwt2	dwt2	ldwt2	dwt2	ldwt2	dwt2	ldwt2
CH1	99,7824	0	99,2958	0	98,9781	0	99,7824	0	97,3961	0	97,36	0
CV1	98,4013	0	97,3472	0	97,4031	0	98,4013	0	94,8484	0	95,72	0
CD1	89,5156	0	96,0354	0	97,1775	0	89,5156	0	96,3936	0	94,50	0
CH2	99,8594	0	99,6574	0	99,4834	0	99,8594	0	98,9307	0	99,06	0
CV2	99,8083	0	99,2255	0	99,272	0	99,8083	0	98,5889	0	98,89	0
CD2	99,8038	0	99,403	0	99,3762	0	99,8038	0	98,8110	0	99,05	0
CH3	99,9097	0	99,7978	0	99,7377	0	99,9097	0	99,5147	0	99,66	0
CV3	99,8071	0	99,5332	0	99,706	0	99,8071	0	99,4776	0	99,67	0
CD3	99,5926	0	99,8256	0	99,7469	0	99,5926	0	99,5463	0	99,64	0
CA3	98,5563	0	98,5463	0	98,5343	0	98,5563	0	99,9985	0	99,99	0

3.5. Módulo Inserción de la Información LSB

El objetivo de este módulo es insertar la información en los coeficientes que se obtienen del paso anterior, por ello se crea una función llamada *ocultamientoLSB*, la cual recibe como argumentos: la ROI donde se guarda la información, la imagen secreta y la cantidad de *LSB*. Inicialmente se compara la forma en la que se escogen los coeficientes a modificar, para esto en un primer escenario se realiza una selección consecutiva de los coeficientes y luego en un segundo caso, una selección aleatoria donde cada coeficiente tiene la misma probabilidad de ser seleccionado. Con el fin de que este efecto sea más notorio se toma un valor de LSB igual a 8, es decir, se modifica por completo el valor del coeficiente.

En el primer escenario la información queda localizada en los primeros coeficientes. Como se observa en la imagen estego resultante de alterar los coeficientes CH1[21] de la Figura 3.19, los coeficientes que sufrieron una alteración están ligados a una región de la imagen original, la cual es muy perceptible a simple vista. Por lo tanto,

[21] CH1: Coeficientes horizontales del primer nivel de descomposición.

la modificación secuencial de los coeficientes no es una alternativa viable para la implementación del algoritmo.

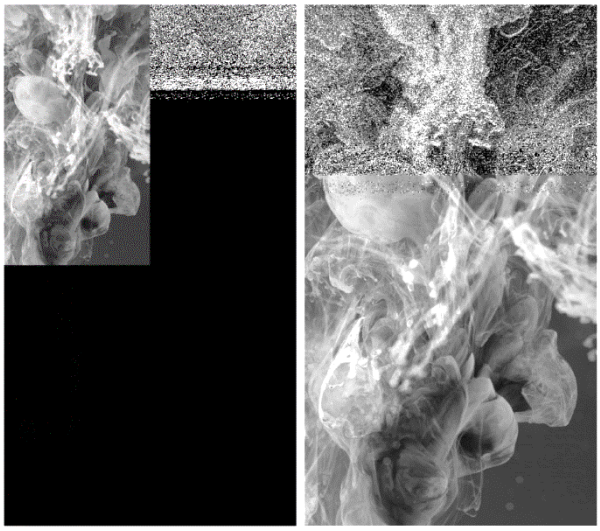


Figura 3.19. Distribución simétrica, *ocultamientoLSB* con 8 bits.

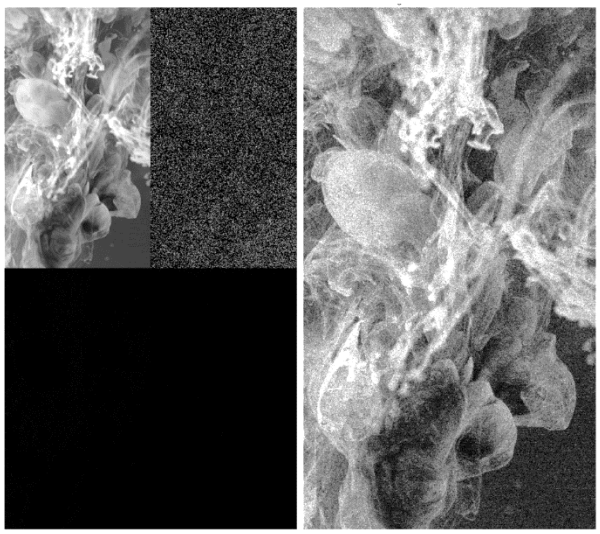


Figura 3.20. Región afectada por el *ocultamientoLSB* con 8 bits con clave.

Mientras que en el segundo escenario con una localización aleatoria se obtiene una distribución uniforme, sobre los coeficientes que pertenecen a CH1, generando una mejor distribución respecto a la primera versión del módulo de inserción, y mejorando la imperceptibilidad y por tanto la robustez (ver Figura 3.20), ya que la ubicación de la información secreta deja de ser predecible. En la imagen estego obtenida se puede ver la distorsión distribuida sobre la imagen y no en una única zona, lo que dificulta el discernimiento sobre si es o no una imagen estego. Por otro lado, para recuperar la imagen secreta se deben conocer los coeficientes modificados, por lo que su elección aleatoria se agrega una capa de cifrado al

proceso de inserción, otorgando complejidad y robustez frente a intentos de revertir el algoritmo sin el conocimiento de esta información.

3.5.1. Cantidad de LSB

Para tener un nivel de imperceptibilidad alto en la imagen estego, la cantidad de LSB no puede ser 8, ya que en este caso la alteración de la información de la imagen portada es muy evidente, debido a que implica reemplazar por completo el valor de uno de los coeficientes Wavelet de la imagen portada. Si el valor de los LSB es 1, entonces se tiene un buen desempeño en cuanto a imperceptibilidad, pero se sacrifica la capacidad de incrustación. La selección en el valor de los LSB implica un equilibrio entre la capacidad de incrustación y la imperceptibilidad; no obstante, en la práctica esta elección también está supeditada a la relación de tamaños de las imágenes portada y secreta, esto es

$$Pp \geq Ps \times 8,$$

donde Pp y Ps corresponden al número de pixeles de la imagen portada y la imagen secreta, respectivamente.

Según la anterior relación se puede determinar la cantidad de pixeles de la imagen portada varía según los LSB

$$Pp \geq \frac{Ps \times 8}{LSB}.$$

para poder determinar los posibles valores que pueden tomar los LSB se realiza el siguiente análisis:

1. Suponiendo que se tiene una imagen portada compuesta por cp columnas y fp filas y una imagen secreta compuesta por cs columnas y fs filas, como se ve en la Figura 3.21. Cada imagen tiene una cantidad pixeles dada por

$$Pp = fp\, cp,$$

$$Ps = fs\, cs.$$

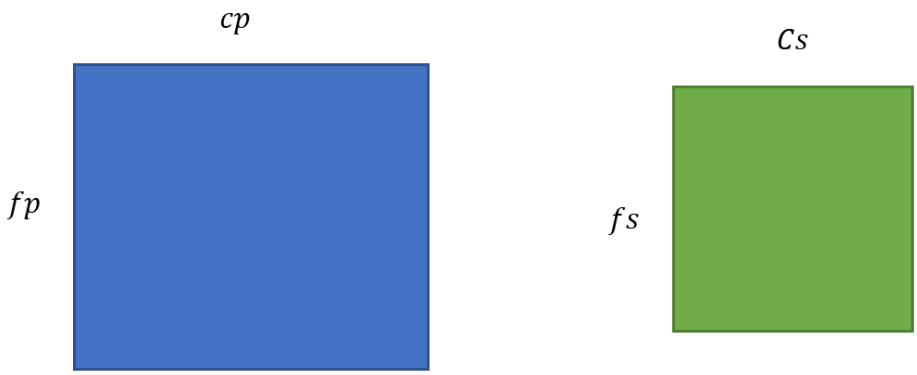


Figura 3.21. Variables imagen portada e imagen secreta.

2. Las longitudes de las cadenas bits necesarias para representar cada imagen son

$$bp = 8\,Pp,$$

$$bs = 8\,Ps.$$

3. Al realizar la comparación de los tamaños de las dos imágenes se tiene que

$$P = \frac{Pp}{Ps},$$

donde un valor de $P > 1$ indica que la imagen portada es más grande que la imagen secreta. $P \leq 1$ implica que no es posible realizar el proceso de ocultar la información.

4. Dado que cada coeficiente se está representando por medio de 8 bits, los LSB pueden tomar valores entre 8 bits y un porcentaje de éstos, para ser más exactos

$$\left\lceil \frac{8}{P} \right\rceil \leq LSB \leq 8,$$

donde el límite inferior de esta desigualdad implica la modificación de un mayor número de coeficientes, mientras que el límite superior indica el número mínimo de coeficientes que deben ser modificados. Si Pp y Ps son iguales se cumple el caso donde los LSB solo pueden tomar el valor de 8. Así, entre mayor sea el valor de Pp, se tiene una mayor flexibilidad para los LSB, siendo el rango máximo de 1 a 8 bits.

3.5.2. Análisis cantidad LSB

Para finalizar las pruebas relacionadas con el funcionamiento y diseño del algoritmo de esteganografía planteado en este trabajo de grado, se busca analizar el efecto de los LSB en la integridad de la información, así como también en la

imperceptibilidad de la imagen estego generada, por lo que, se realizan pruebas con cada una de las 39 familias Wavelets utilizando desde 1 hasta 8 LSB y se compara el porcentaje de igualdad de la imagen secreta original con la imagen secreta recuperada, además del cálculo de la PSNR de la imagen estego utilizando como referencia la imagen portada. Los resultados obtenidos se muestran en la Figura 3.22.

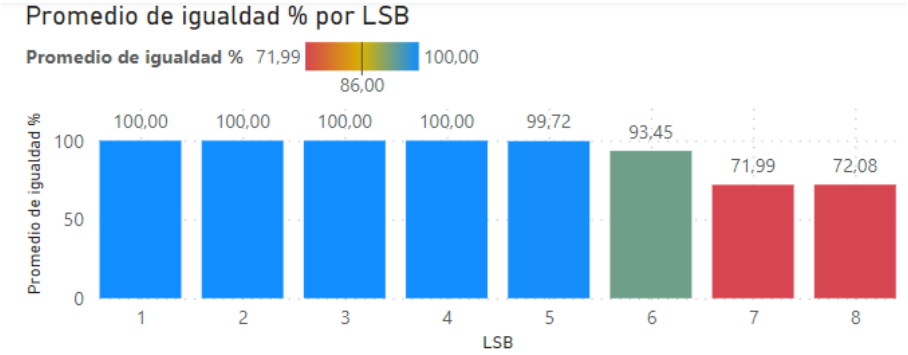


Figura 3.22. Promedio % de igualdad imagen secreta.

Tras analizar los resultados obtenidos, en la Figura 3.22, se evidencia la inviabilidad de usar 5, 6, 7 y 8 LSB, debido a la pérdida de información que demuestra su implementación.

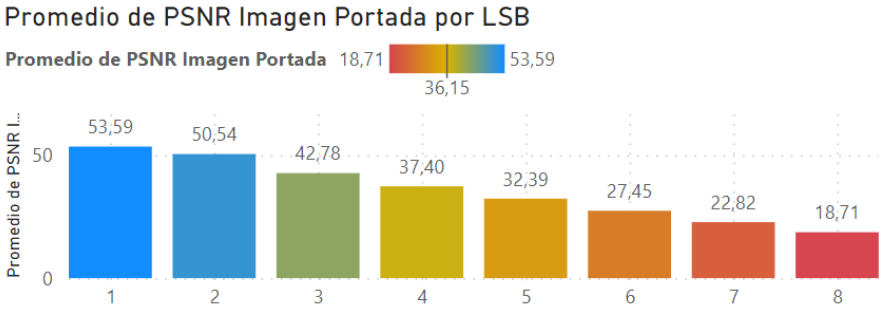


Figura 3.23. Promedio de PSNR imagen estego.

De igual manera, con los resultados obtenidos de PSNR, que se observan en la Figura 3.23, se puede concluir que los valores 5, 6, 7 y 8 no cumplen con un valor aceptable de imperceptibilidad, por el grado de afectación que se tiene en la imagen estego.

Para finalizar el análisis, se muestra en la Figura 3.24 la cantidad de pixeles necesarios (color azul) para ocultar 10.000 pixeles secretos (color rojo) según cada valor de LSB.

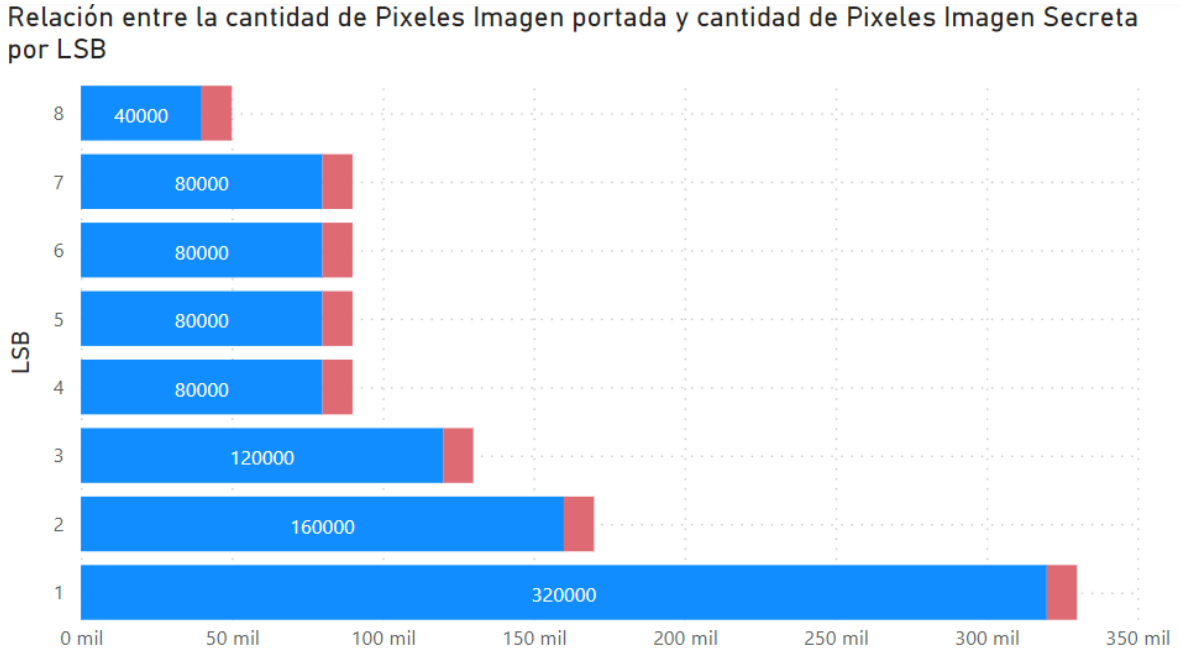


Figura 3.24. Cantidad de pixeles portada necesarios para ocultar 10.000 pixeles secretos.

Los resultados de las Figuras 3.22 y 3.23 muestran que con respecto a la integridad e imperceptibilidad los LSB deben ser menores a 4 y que, en cuanto a estos atributos, lo más recomendable es que el valor de LSB sea lo más pequeño posible; no obstante, los resultados de la Figura 3.24, relacionados con la capacidad de incrustación, permiten concluir que para este atributo lo más recomendable es que el valor de LSB sea lo más grande posible, ya que, por ejemplo, el uso de 1 LSB reduce significativamente la capacidad de incrustación del algoritmo en contraste con 8 LSB.

Comparativamente se tiene que el uso de 3 LSB aumenta un 33% la capacidad de incrustación con respecto a 2 LSB. Por otro lado, un LSB igual a 3 aumenta significativamente la PSNR, en comparación a un LSB de 4. Por lo mostrado anteriormente, se determina que 3 LSB representa el equilibrio buscado para el algoritmo del presente trabajo de grado en términos de imperceptibilidad y capacidad de incrustación, además de que su uso, bajo las condiciones de esta prueba, permite recuperar la información secreta en un 100%.

3.5.3. Proporción imagen portada sobre imagen secreta

Bajo el caso previamente demostrado en la sección anterior con un LSB igual a 3 se lleva a que la relación P sea

$$\left\lceil \frac{8}{P} \right\rceil \leq 3,$$

$$\lceil 2.7 \rceil \leq P,$$

$$3 \leq P,$$

$$3 \leq \frac{Pp}{Ps}.$$

Lo que implica que debe haber una relación de por lo menos 3 a 1, entre los pixeles de la imagen secreta respecto a la portada. Un punto para tener en cuenta es que si se va a hacer uso de una ROI para insertar la información la relación de tamaños cambia, por ejemplo, si se considera como ROI uno de los 4 conjuntos de coeficientes resultantes de un nivel de descomposición con la DWT, como el número de coeficientes de la ROI tiene ¼ del tamaño de la imagen portada original, se tiene que

$$3 \leq \frac{\frac{Pp}{4}}{Ps},$$

$$3 \leq \frac{Pp}{4\,Ps},$$

$$12 \leq \frac{Pp}{Ps}.$$

Lo que hace que la relación entre Pp y Ps sea como mínimo de 12 a 1. Por ejemplo, sobre una imagen portada de 3840 x 2160 pixeles, se pueden guardar imágenes hasta de 691.200 pixeles aproximadamente, como una imagen cuadrada de 831 x 831 pixeles. En la Figura 3.25 se muestra de forma gráfica la diferencia de las escalas de las dos imágenes del ejemplo anterior.

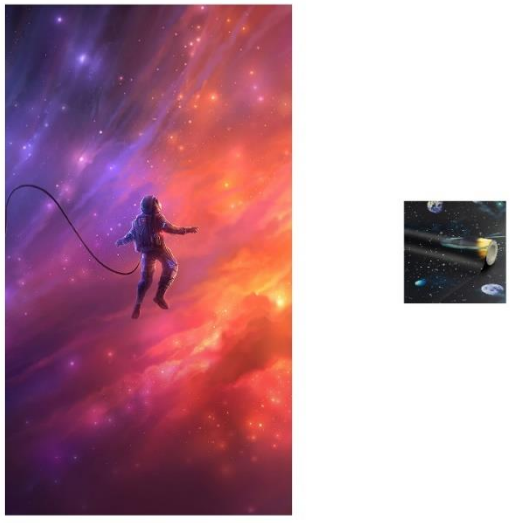


Figura 3.25. Comparación visual de tamaños imagen portada con imagen secreta.

Si se utiliza un solo conjunto de coeficientes como ROI, entonces aumentar el número de niveles de descomposición de la DWT implica que se tengan mayores exigencias en cuanto a la diferencia de tamaños entre la imagen portada y la imagen secreta.

3.5.4. Distribución de la información en la imagen portada

Para poder insertar los bits de la imagen secreta, $8\,Ps$, en los coeficientes de la ROI, se debe calcular el número de coeficientes de la imagen portada que deben ser afectados, o modificados, antes de hacer su selección, el número que se debe modificar, m_p, debe ser menor a la cantidad de pixeles de la imagen portada, Pp, esto es

$$m_p = \left\lceil \frac{8\,Ps}{LSB} \right\rceil \ , \quad m_p \leq Pp.$$

A partir de la cantidad del valor de m_p se realiza una permutación, con el fin de determinar el número de posibilidades en las que se puede hacer la selección de estos valores dentro de los Pp posibles, matemáticamente se tiene que

$$R_p = \frac{Pp!}{(Pp - mp)!}.$$

Teniendo en cuenta lo anterior, a partir de una distribución uniforme se genera un vector de valores con las m_p ubicaciones de los valores de la imagen portada seleccionados para incrustar la información secreta. Dado el carácter aleatorio de este vector, se selecciona una de las R_p posibilidades, a este vector se le denomina c*lave.*

Finalmente, en la Figura 3.26, se presenta el diagrama de flujo que describe el proceso de inserción LSB, el cual utiliza un manejo en paralelo para optimizar el tiempo de procesamiento de este mismo.

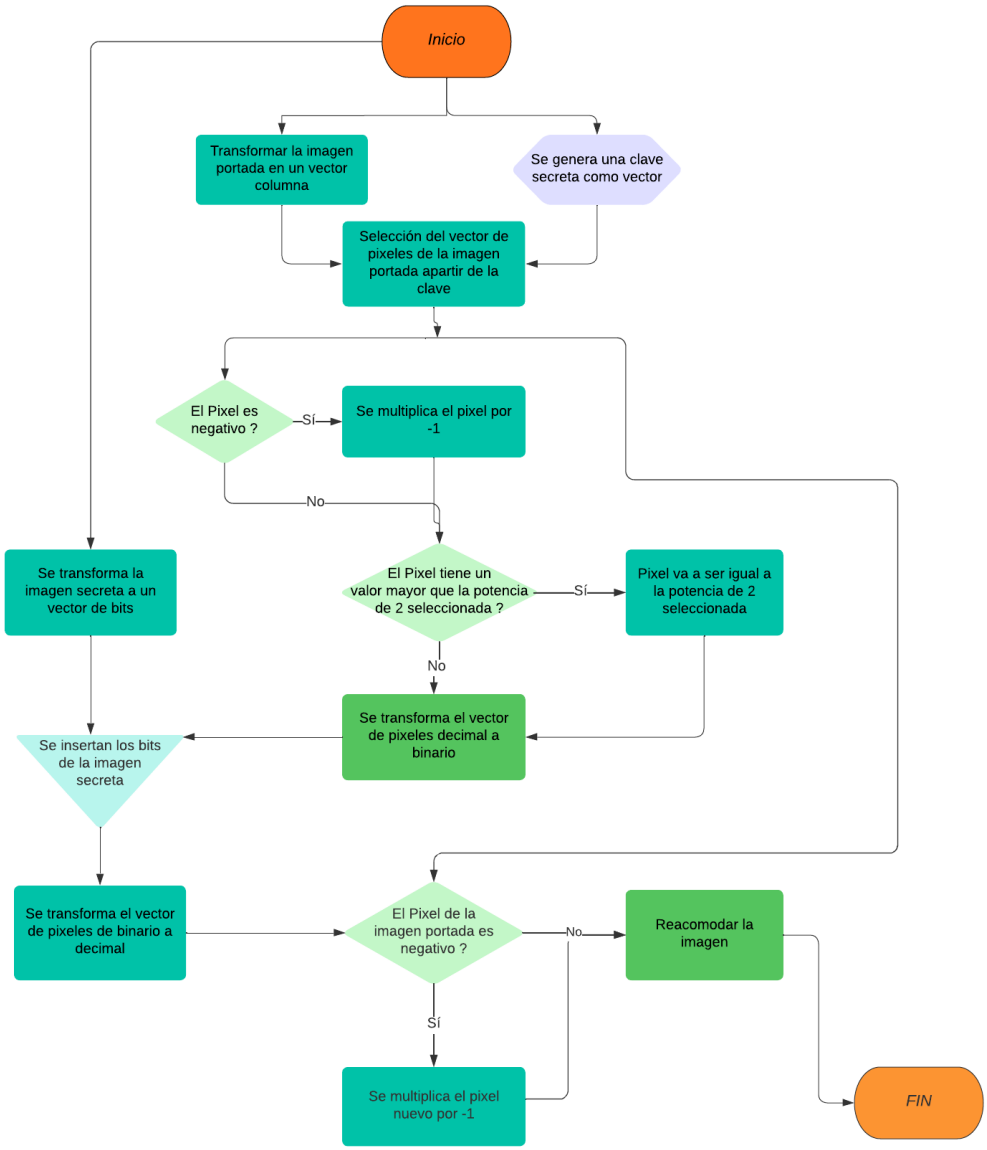


Figura 3.26. Algoritmo de inserción LSB.

3.6. Formato de la Imagen Estego

Para determinar el formato de compresión de las imágenes estego más adecuado para el algoritmo diseñado, se compara la imagen secreta recuperada, cuando la imagen estego es guarda tanto en formato *.jpg* como en *.png*[22].

[22] Se escogen estos dos tipos de formato debido a su popularidad en aplicaciones digitales.

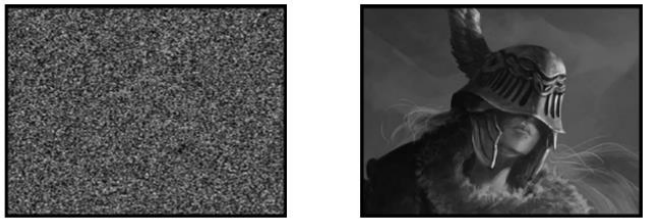


Figura 3.27. Imágenes secretas recuperadas enviando imágenes estego en formato .jpg y .png.

En la Figura 3.27, de manera visual, se aprecia que la imagen estego al ser guardada con formato *.jpg* impide la reconstrucción de la imagen secreta original, además, al realizar la comparación pixel a pixel, el porcentaje de igualdad encontrado es de $0{,}60754\%$. Por otra parte, en la imagen extraída de la prueba con el formato *.png*, se percibe un alto grado de similitud con la imagen secreta original y, tras realizar la comparación pixel a pixel en esta imagen, se obtiene un porcentaje del 100% de igualdad. Lo anterior ocurre debido a que la compresión que se realiza en el estándar *.jpg,* produce pérdidas de información en las imágenes, ocasionadas por redondear los valores de la imagen. Por esta razón se opta por el formato *.png* como el indicado para guardar la imagen estego generada por el algoritmo.

Estas pruebas se validaron por medio de la transmisión de la imagen estego a través de medios comúnmente utilizados, como: *WhatsApp*, *Gmail* y *WeTransfer*. Los resultados fueron consistentes, por lo que se concluye que siempre y cuando se respete el formato de la imagen estego generada (*.png*) será posible realizar la reconstrucción de la imagen secreta.

3.7. Análisis de la Robustez de la Imagen Estego

En esta sección se pretende verificar, por medio de herramientas externas, la robustez del algoritmo, i.e., la facilidad con la que un atacante podría detectar que se ha realizado un proceso estenográfico y/o extraer la información secreta. En el diagrama mostrado en la Figura 3.28 se detallan los caminos que un atacante puede recorrer para obtener la información secreta, por un lado, se tiene un conjunto de pasos que son de utilidad cuando se quiere determinar si la imagen es o no una imagen estego: detectabilidad de la imagen. Por el otro lado, sabiendo que es una imagen estego, se consideran dos caminos para intentar recupera la información, si se conoce el algoritmo se pueden aplicar procesos inversos para tratar de recuperar la imagen secreta: estegoanálisis; si no se conoce el algoritmo se puede realizar una comparación directa con la imagen portada, para analizar las diferencias encontradas; no obstante, para esto se requiere conocer la imagen portada: búsqueda inversa.

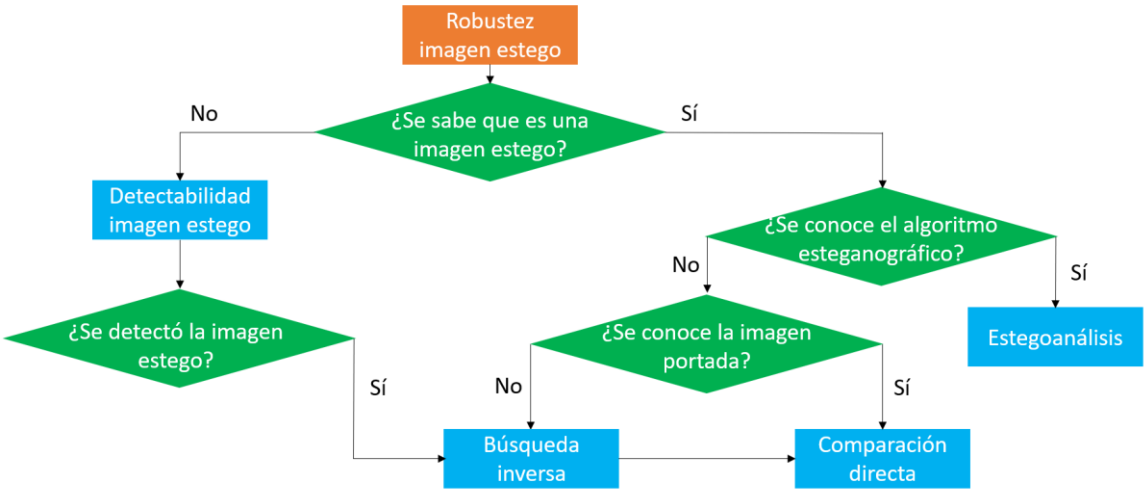


Figura 3.28. Diagrama de flujo detección de información secreta.

3.7.1. Detectabilidad de la imagen estego

Actualmente existen muchas herramientas para detectar alteraciones sobre imágenes o fotografías. En la Figura 3.29 se muestran las herramientas que se probaron en este trabajo de grado. *FotoForesis* es una herramienta conocida por poder identificar aquellos pixeles que tengan alguna modificación o edición. Esta herramienta utiliza un análisis de nivel de error, para poder identificar aquellos pixeles que salen del comportamiento que se espera de toda la imagen. Por su parte, *Forensically* ofrece más posibilidades de análisis y permite una variación al nivel de error que puede presentar la imagen.

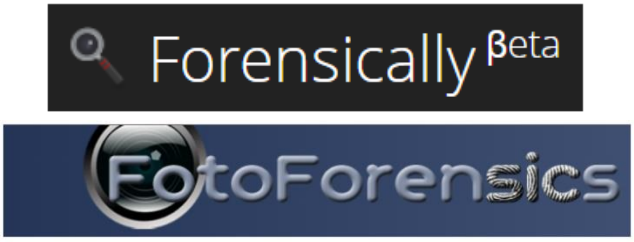


Figura 3.29. Herramientas para analizar la detectabilidad de la imagen estego [47], [48].

Para poder analizar el ver el nivel de afectación que produce el algoritmo propuesto en este trabajo de grado, se tomó como base una imagen nueva, sobre la cual se tiene la certeza de que no ha sufrido ediciones externas, dicha imagen se denomina *gato*. En Figura 3.30 se muestran que los resultados arrojados por *FotoForensics* y *Fotosically* no permiten evidenciar alteraciones en los pixeles de esta imagen.

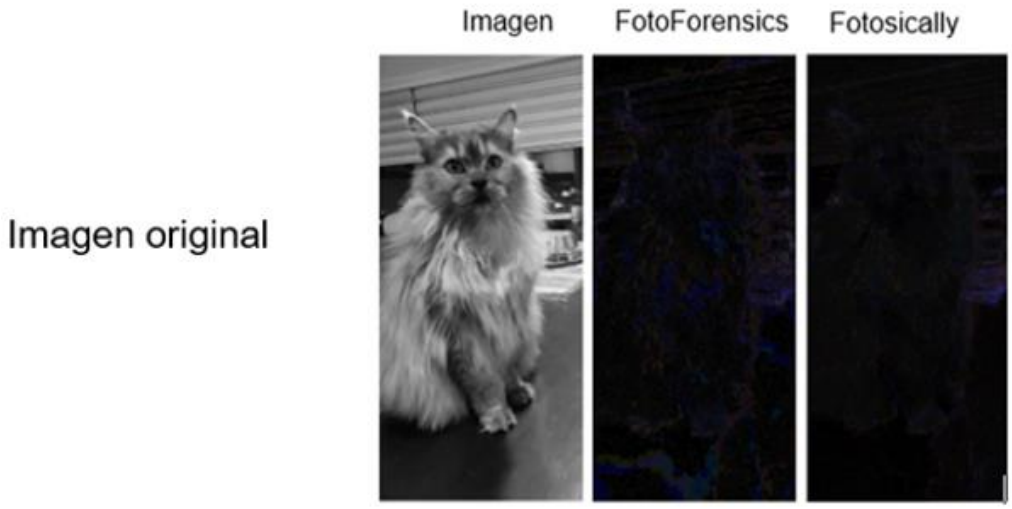


Figura 3.30. Análisis de una imagen sin alteraciones.

De manera intencionada se edita la imagen *gato*, con el fin de determinar si las herramientas utilizadas pueden detectar estas modificaciones. En la Figura 3.31 se evidencia que las dos herramientas resaltaron los elementos que se adicionaron sobre la imagen original.

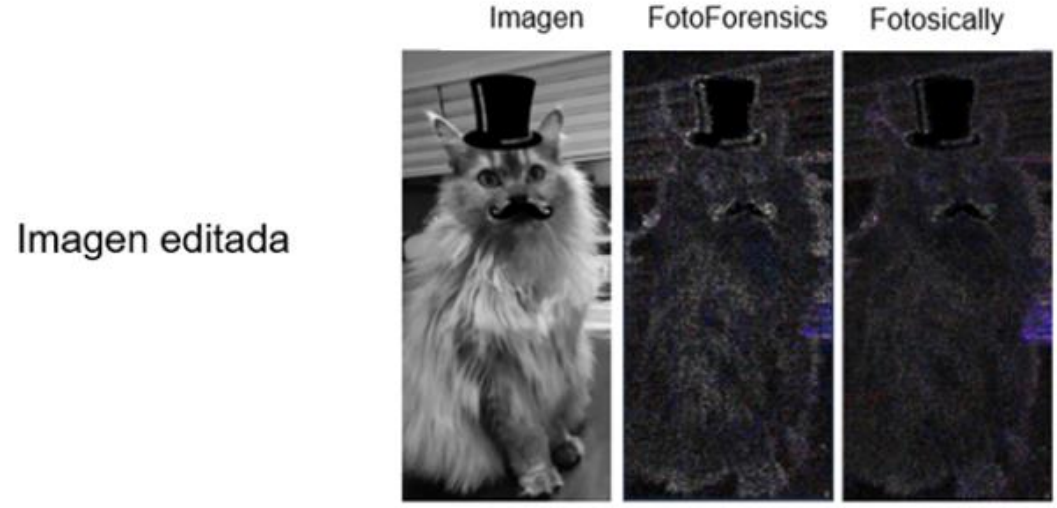


Figura 3.31. Análisis de una imagen editada.

Finalmente, se crea una imagen estego utilizando a *gato* como imagen portada. En la Figura 3.32 se muestran los resultados obtenidos por las dos herramientas al analizar la imagen estego, en los dos casos no se demarcan claramente zonas o pixeles que no coincidan con la imagen, por lo que se concluye que en este caso no es posible determinar que es una imagen estego.

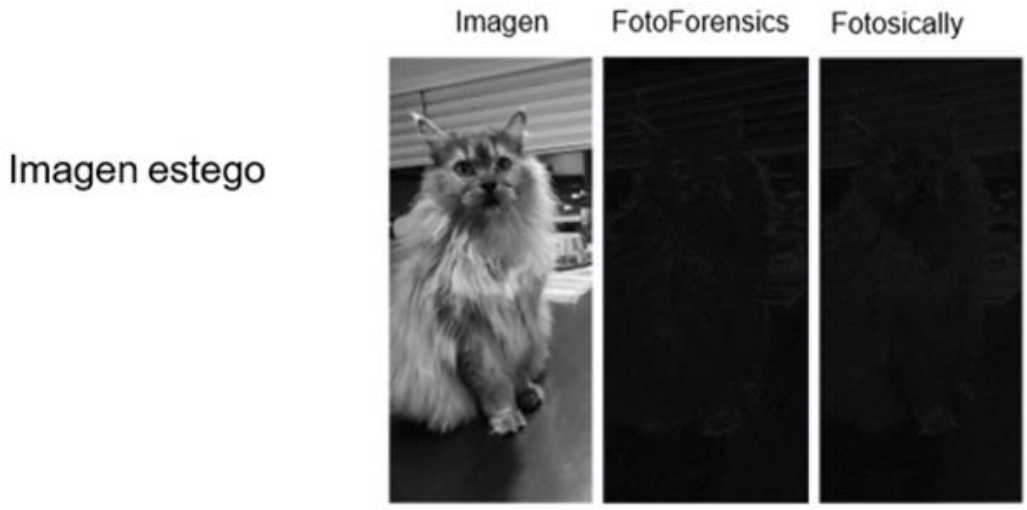


Figura 3.32. Análisis de una imagen estego.

3.7.2. Búsqueda inversa

La búsqueda inversa consiste en utilizar una imagen como referencia para realizar una verificación de coincidencias con imágenes disponibles en la web. Para el análisis de coincidencias se utilizaron herramientas como las que se muestran en la Figura 3.33.

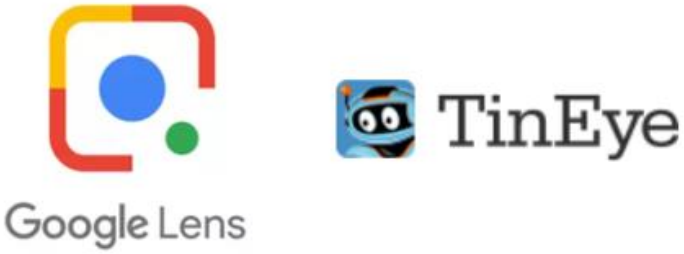


Figura 3.33. Herramientas para realizar la búsqueda inversa [49], [50].

Google Lens es una herramienta muy utilizada para encontrar imágenes iguales o similares a una imagen cargada en la herramienta. Con el fin de validar el proceso de búsqueda realizado por ésta, se utiliza la imagen estego obtenida a partir de la imagen portada *Paint*. En la Figura 3.34 se muestran los resultados obtenidos, los cuales contienen imágenes con patrones similares, pero no se encuentra una coincidencia exacta, por lo que no se puede aplicar una comparación directa entre estas dos imágenes.

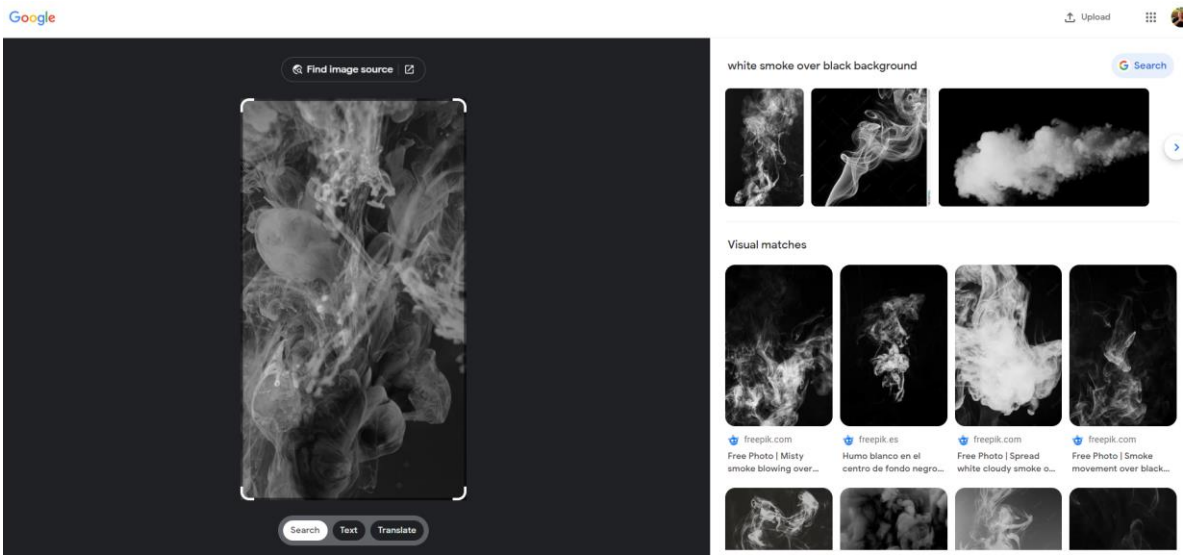


Figura 3.34. Resultados de la búsqueda con *Google Lens*.

Al igual que *Google Lens*, *TinEyes* es una herramienta utilizada para reconocimiento y búsqueda inversa de imágenes a partir de una imagen cargada en esta. En el caso de Paint, la similitud de su búsqueda da múltiples resultados, pero no da una coincidencia exacta, dando a entender que la similitud con su imagen base se ha perdido, lo cual dificulta su identificación para posterior verificación de alteraciones.

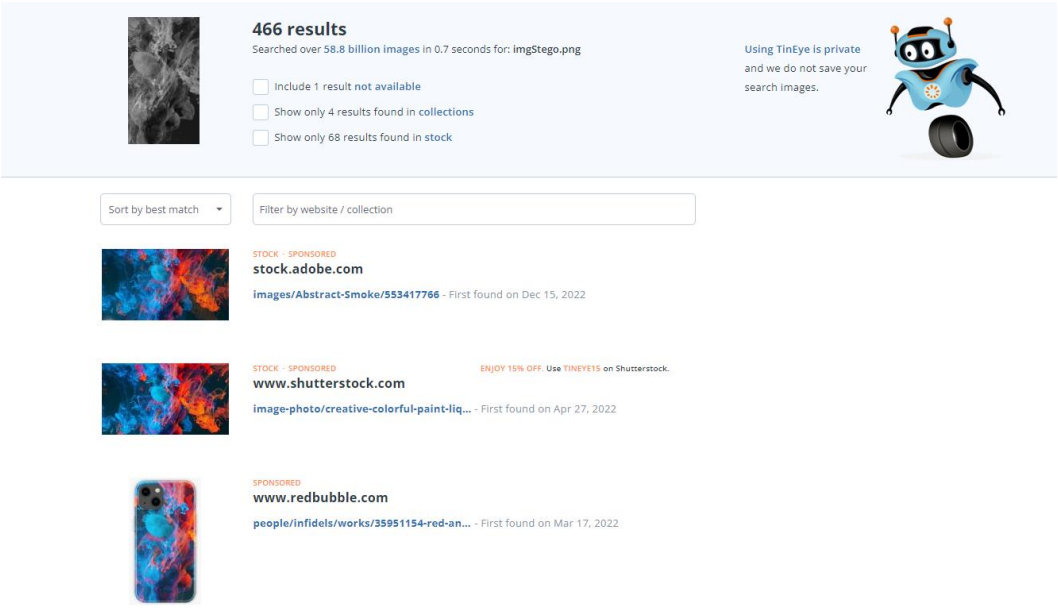


Figura 3.35. Resultados de la búsqueda con *TinEyes*.

Si se logra encontrar la imagen portada se puede intentar encontrar la información secreta por medio de la comparación directa entre la imagen estego y la imagen portada, lo cual conduciría a buenos resultados si la modificación de los LSB se

realiza en el dominio espacial, i.e., directamente sobre la imagen portada, pero no es una garantía si, como en el caso de este trabajo de grado, se han añadido procesos o capas de seguridad para realizar el proceso de incrustación.

3.7.3. Estegoanálisis

El estegoanálisis consiste en el estudio y detección de información secreta oculta por algún proceso de esteganografia, para lo cual existen herramientas software como ***stegosuite, Esteganografía Online*** *y* ***Silenteye***; no obstante, no es posible realizar estas pruebas con el algoritmo propuesto en este trabajo de grado, dado que es un diseño propio que aún no es conocido y por lo tanto ninguno logra ser compatible para poder atacar la imagen estego generada.

En caso de que el atacante decida realizar un ataque por fuerza bruta, es decir, probar todas las posibles combinaciones que se pueden realizar con el algoritmo de esteganografía propuesto en este trabajo de grado de grado, se tiene que el número máximo de intentos que debería realizar es

$$I = f_w \times R_p,$$

donde, R_p describe el número de posibilidades en las que se puede ocultar la información dentro de la imagen portada (ver sección 3.5.4) y f_w indica el número de combinaciones que se pueden obtener con las 39 familias Wavelets, es decir,

$$f_w = \frac{39!}{(39 - ND)!},$$

siendo ND los niveles de descomposición, los cuales se pueden determinar según la relación Pp/Ps.

Este análisis busca mostrar que, hasta el momento según las validaciones hechas, el algoritmo propuesto en este trabajo de grado tiene un buen desempeño en cuanto a robustez, debido a que el número I, incluso para imágenes muy pequeñas, es grande, dificultando la posibilidad de un ataque por fuerza bruta.

CAPÍTULO 4. PLAN DE PRUEBAS

En el presente capítulo se analiza el algoritmo descrito en el capítulo 3, a fin de encontrar las limitaciones que presenta y obtener una claridad sobre su funcionamiento y posibles aplicaciones. Se plantean 3 escenarios para esclarecer las condiciones para el funcionamiento adecuado de este algoritmo.

Para el primer escenario se plantea encontrar las combinaciones de familias Wavelets apropiadas para ocultar la información, es decir, aquellas familias que brinden menores pérdidas en la integridad de la imagen secreta, lo cual implica realizar una comparación pixel a pixel entre la imagen secreta antes y después de ser insertada en la imagen portada.

En el segundo escenario se buscan aquellas ROI que presentan las mejores condiciones para ocultar la información secreta, esto se logra al poner a prueba cada grupo de coeficientes Wavelet a 3 niveles de descomposición usando el 100% de la capacidad de inserción de cada uno de ellos. Se analizan los resultados para encontrar los umbrales adecuados para el algoritmo y determinar las ROI que entregan los mejores porcentajes de igualdad y las PSNR.

En el tercer escenario se evalúa el comportamiento de cada coeficiente al disminuir el porcentaje de inserción a: 25%, 50% y 75%; y encontrar una relación adecuada entre la capacidad de incrustación y la imperceptibilidad.

Finalmente, se realiza un resumen general de los resultados encontrados para mostrar la configuración ideal del algoritmo planteado en este trabajo de grado.

4.1. Escenario 1

Este escenario se divide en tres partes: en la primera parte del escenario se realiza una prueba a un nivel de descomposición, en la segunda parte se utilizan dos niveles de descomposición para finalizar con una prueba con tres niveles de descomposición. Para las pruebas realizadas en este escenario se utilizan las siguientes familias Wavelets[23]:

{bior1.1, bior1.3, bior1.5, bior2.2, bior2.4, bior2.6, bior2.8, bior3.1, bior3.3, bior3.5, bior3.7, bior3.9, bior4.4, bior5.5, bior6.8, coif1, db2, db3, db4, db5, db6, db7, db8, haar, rbio1.1, rbio1.3, rbio1.5, rbio2.2, rbio2.4, rbio2.6, rbio2.8, rbio3.1, rbio3.3, rbio3.5, rbio3.7, rbio3.9, rbio4.4, rbio5.5, rbio6.8}.

Una vez obtenidos los resultados de cada prueba, todas las combinaciones de Wavelets cuyo porcentaje de igualdad sea diferente de 100% son descartadas para la prueba siguiente.

[23] Estas son las 39 familias Wavelet con las que se pueden trabajar en MATLAB con el algoritmo Lifting.

Para el escenario inicial, se guarda una imagen secreta aleatoria de tamaño 225×225 en una imagen portada con niveles adecuados de grises de 2160×3840, usando cada una de las 39 familias a un nivel de descomposición. Los porcentajes de igualdad tras esta prueba son los mostrados en la Figura 4.1.

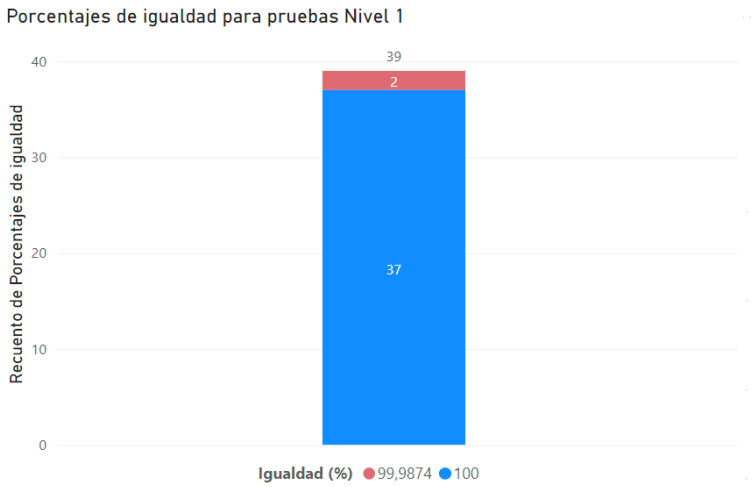


Figura 4.1. Porcentajes de igualdad para Wavelets a 1 nivel de descomposición.

De las 39 familias utilizadas, solamente con dos de ellas no es posible recuperar la totalidad de la imagen secreta; la *rbio5.5* y la *db8*, por lo tanto, estas familias son eliminadas para la siguiente prueba, es decir, que para la prueba de dos niveles se utilizan 37 Wavelets de primer nivel y 39 Wavelets de segundo nivel.

Los resultados de la etapa dos de este escenario (ver Figura 4.2), muestran la cantidad de resultados obtenidos tanto para 100% de igualdad como para valores diferentes de 100%. Tras analizar las familias Wavelets con las que se obtiene un 100% de igualdad en la imagen secreta, se llega a una elección de 22 Wavelets de primer nivel combinadas con 35 Wavelets de segundo nivel. Además, el gráfico circular de la Figura 4.2, muestra en detalle la distribución de los valores diferentes de 100%, revelando que un 79,4% de estos valores son porcentajes de igualdad entre 99% y 100%, lo da a entender que para la mayoría de las combinaciones en una descomposición Wavelet a dos niveles, el algoritmo mantiene la integridad de la información de manera sobresaliente.

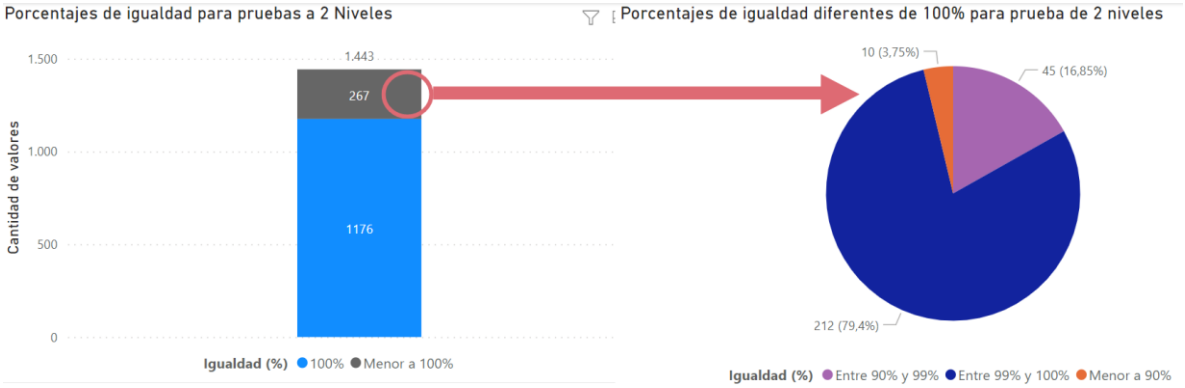


Figura 4.2. Porcentajes de igualdad para Wavelets a 2 niveles de descomposición.

Debido a que el algoritmo está planteado para que funcione hasta con 3 niveles de descomposición, se realiza una tercera prueba en la cual se analizan las 770 combinaciones de familias Wavelets con las que se ha obtenido hasta el momento un 100% de igualdad, i.e., tras el análisis en uno y dos niveles de descomposición[24], agregando en un tercer nivel de descomposición con cada una de las 39 familias Wavelets iniciales.

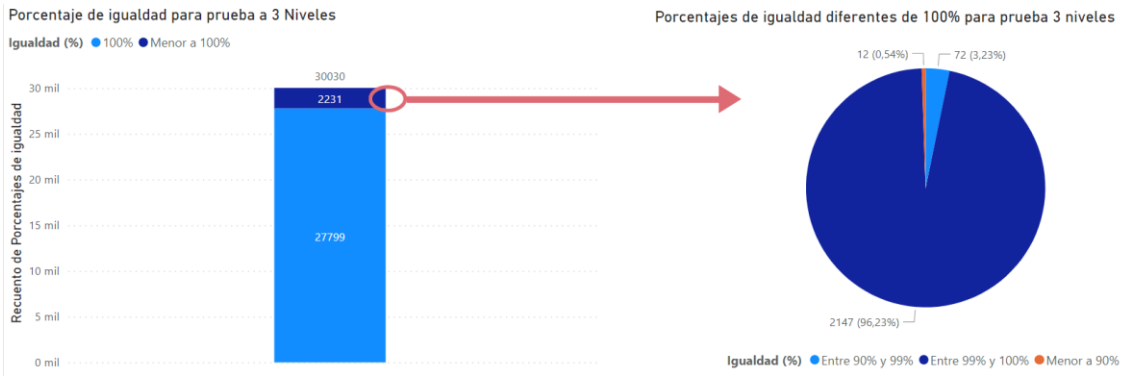


Figura 4.3. Porcentajes de igualdad a 3 niveles de descomposición.

Los resultados obtenidos en la Figura 4.3 muestran que, de las 30.030 combinaciones realizadas, en 27.799 se obtiene un 100% de igualdad en la imagen secreta. Por otra parte, cabe resaltar que de las 2.231 combinaciones con las que no se obtiene un 100%, en 2.147 combinaciones (equivalente al 96,23% de este grupo) se obtienen valores entre 99% y 100%. Lo anterior muestra que, para 3 niveles de descomposición, el algoritmo planteado continúa manteniendo un nivel sobresaliente de integridad de los datos. Lo anterior produce la posibilidad de llegar a una lista de familias Wavelets que pueda ser utilizada en cualquier orden y que con ellas se logre una integridad completa de la información secreta, por ello, para finalizar este escenario, se analizan, en conjunto, todas las pruebas realizadas con el fin de obtener una lista de familias Wavelets que permitan combinaciones con porcentajes de igualdad del 100%.

[24] 22 familias de primer nivel y 35 familias de segundo nivel.

Tras realizar un cruce de los datos y analizar los resultados, se determina que es posible utilizar las siguientes 18 familias Wavelets individualmente o en cualquier combinación desde 1 a 3 niveles de descomposición:

{bior1.1, bior1.3, db4, db5, haar, rbio1.1, rbio1.3, rbio1.5, rbio2.2, rbio2.4, rbio2.6, rbio2.8, rbio3.1, rbio3.3, rbio3.5, rbio3.7, rbio3.9 y rbio4.4}.

Para los escenarios 2 y 3, se utilizan estas 18 Wavelets y todas sus posibles combinaciones.

4.2. Escenario 2

En el escenario 2 se busca evaluar la influencia del uso de diferentes coeficientes Wavelets al usarlas como ROI para insertar información secreta. Con el fin de analizar el caso más crítico para el algoritmo, se plantea realizar una inserción aproximada del 100% de la capacidad de cada coeficiente y de esta manera analizar el nivel de afectación que sufre tanto la PSNR de imagen estego como en la integridad de la imagen secreta recuperada. Para determinar el tamaño de que debe tener la imagen secreta, se debe cumplir que

$$\left\lceil \frac{8}{P/4^{ND}} \right\rceil = 3,$$

$$P_s = \left\lceil \frac{3}{8} \frac{P_p}{4^{ND}} \right\rceil.$$

Es así como tomando como base una imagen portada de dimensiones 4.100×7.290 pixeles y con ayuda de la herramienta *Photoshop,* se obtienen versiones escaladas de esta misma imagen para que funcionen como imágenes secretas, de tal manera que las dimensiones de la imagen se modifican para que tengan el mismo tamaño de cada coeficiente de los 3 niveles de descomposición (ND) de la imagen portada inicial, como se muestra en la Figura 4.4.

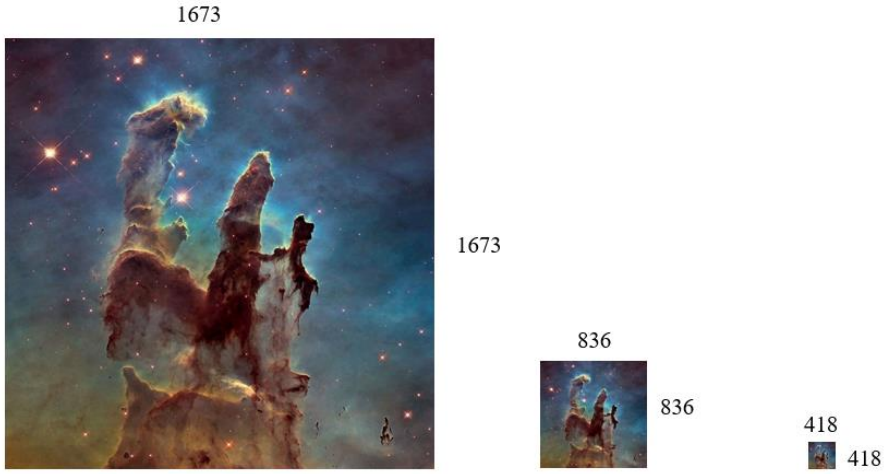


Figura 4.4. Imágenes secretas del tamaño de cada grupo de coeficientes.

La Figura 4.4 muestra las imágenes secretas guardadas en cada nivel, siendo la imagen de 1.673×1.673 la imagen secreta para el primer nivel, la de 836×836 para el segundo nivel y la de 418×418 para el tercer nivel. Por otra parte, el mapa de los coeficientes (Figura 4.5) muestra cada una de las ROI en los que se va a guardar la imagen secreta, siendo:

- CA, los Coeficientes de Aproximación.
- CH, los Coeficientes Horizontales.
- CD, los Coeficientes Diagonales.
- CV, los Coeficientes Verticales.

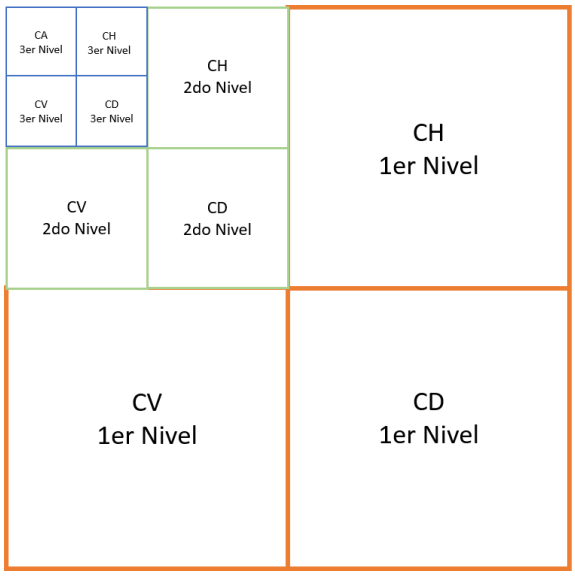


Figura 4.5. Coeficientes a 3 niveles de descomposición.

Teniendo claro lo anterior, se procede a realizar el proceso esteganográfico para cada una de las imágenes secretas, modificando los grupos de coeficientes de cada nivel de descomposición, utilizando las combinaciones de las 18 familias Wavelets escogidas en el escenario 1. Una vez obtenidos los resultados, se realiza un diagrama de caja[25] y un histograma de frecuencia relativa[26], como se muestra en la Figura 4.6.

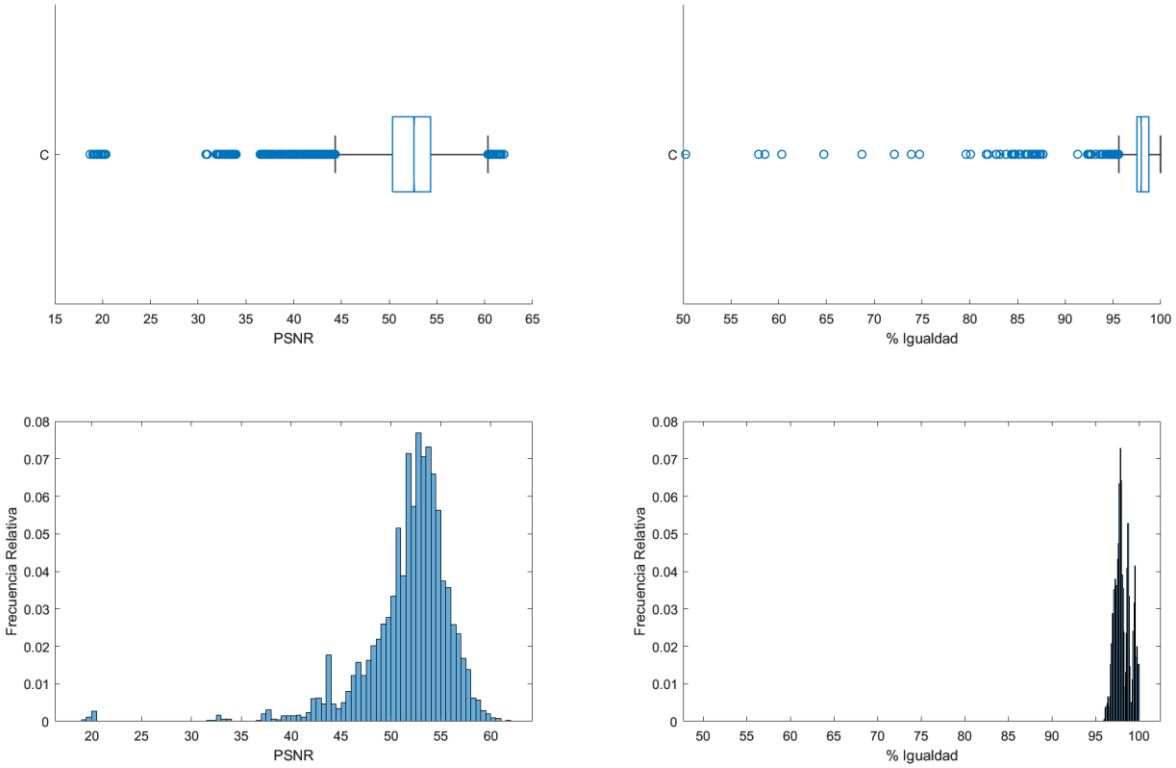


Figura 4.6. Histograma y diagrama de caja para todos los coeficientes.

Lo mostrado en la Figura 4.6, se realiza con el fin de encontrar los datos típicos y atípicos y determinar el valor del bigote inferior para tomar este valor como el umbral tanto en el porcentaje de igualdad como en PSNR. Esto se realiza ya que, a partir de estos puntos, se encuentran la mayoría de los datos de este escenario. Los valores de los bigotes inferiores son: 44,37dB para la PSNR y 95,64% para el porcentaje de igualdad.

Se presenta una mayor variabilidad en los valores del porcentaje de igualdad en comparación con el escenario 1, por lo cual en este escario su valor medio cambia y pasa de 100 a 98, debido a que en el escenario 1 se tiene una menor capacidad de incrustación, puesto que se esconde una imagen de 225×225 en una imagen

[25] El diagrama de caja distribuye la información en cuartiles; los bigotes indican el inicio y el final de los datos típicos.

[26] El histograma de frecuencia relativa muestra la distribución de los valores de amplitud, por medio del conteo del número de valores que se encuentran dentro de cada barra del histograma.

portada de 2160×3840, lo cual corresponde a un grado de inserción del 3,1% para el primer nivel, 9,7% para el segundo nivel y 39% para el tercer nivel; mientras que este escenario se guarda una imagen en la que se deben modificar todos los coeficientes de cada ROI. Esto incrementa la probabilidad de que alguno de los coeficientes tenga un valor inadecuado, implicando que al hacer la transformada inversa se altere este valor y por lo tanto algunos pixeles de la imagen secreta se vean afectados y se produzcan pérdidas.

El siguiente paso en el análisis es filtrar los datos obtenidos para valores menores a los umbrales establecidos anteriormente y observar el rendimiento de cada uno de los conjuntos de coeficientes Wavelets como ROI.

Inicialmente se analiza la integridad de los datos secretos y, tras filtrar los valores del porcentaje de igualdad que están por debajo de 95,64 (ver Figura 4.7), se aprecia que 91 valores no alcanzan esta cifra del umbral y que todos estos casos corresponden a modificaciones realizadas sobre los coeficientes de aproximación del tercer nivel, lo cual se entiende debido a que en este conjunto de coeficientes se encuentra la mayor concentración de la información de la imagen portada. Por otra parte, se aprecia que son combinaciones de las familias Wavelets: Rbio3,1, Rbio3,3, Rbio3,5, Rbio3,7 y Rbio3,9; esto indica que se generan pérdidas en la información si se usa esta ROI con combinaciones de las familias mencionadas anteriormente.

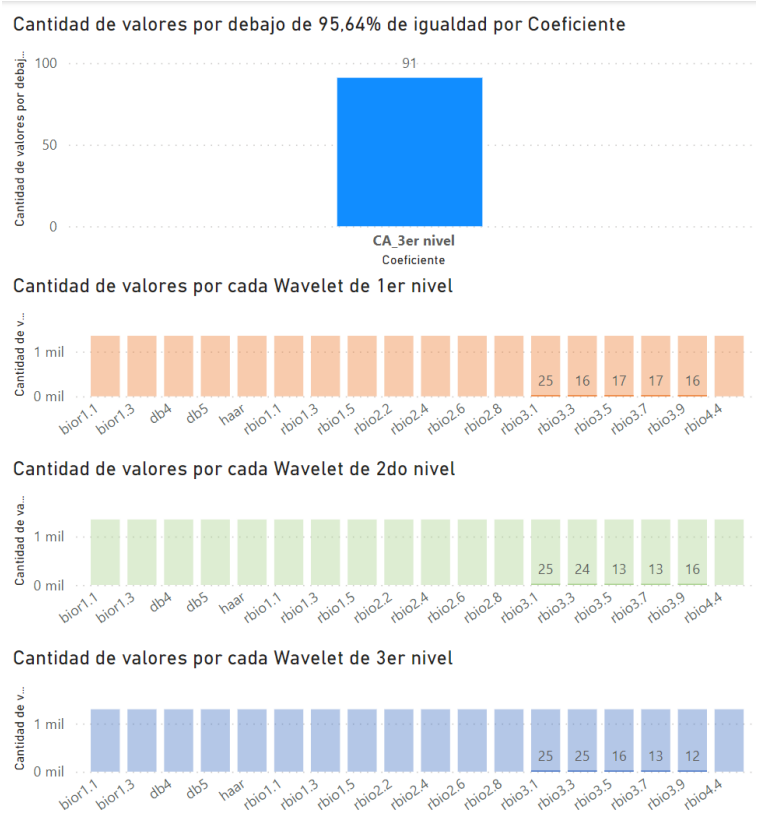


Figura 4.7. Valores por debajo de 95.64% de igualdad.

Posteriormente, se analizan los valores de PSNR tras realizar un filtraje de los valores menores al umbral, 44,37dB, los resultados por coeficientes de estos datos se ven representados en la Figura 4.8.

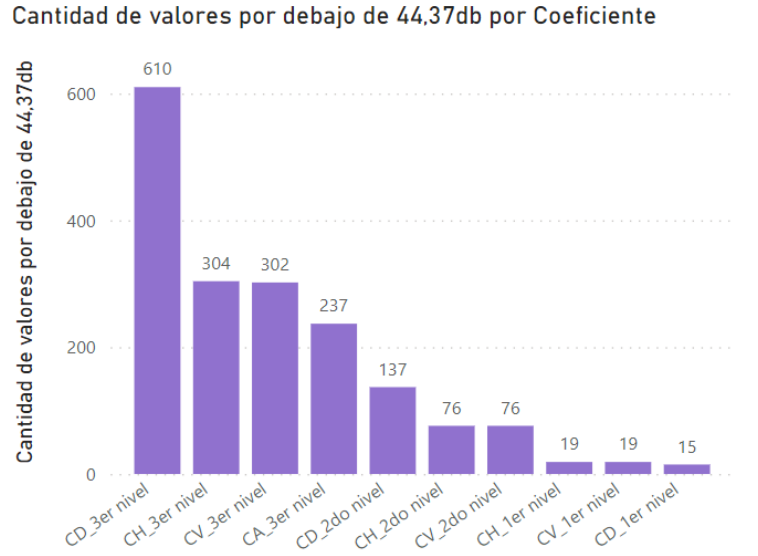


Figura 4.8. Cantidad de valores por debajo de 44,37dB por coeficientes.

Se aprecia que a medida que aumenta el nivel de descomposición, aumenta también la cantidad de valores por debajo del umbral, siendo los coeficientes diagonales de tercer nivel el grupo de coeficientes con mayor cantidad de valores por debajo del umbral de PSNR.

Tras analizar a mayor detalle cada conjunto de coeficientes, se aprecia que en los coeficientes horizontales y verticales de segundo y tercer nivel (Figuras 4.9,4.10,4.11,4.12), todos los valores por debajo del umbral corresponden a combinaciones de estas 3 familias Wavelets: bior1.1, bior1.3 y haar.

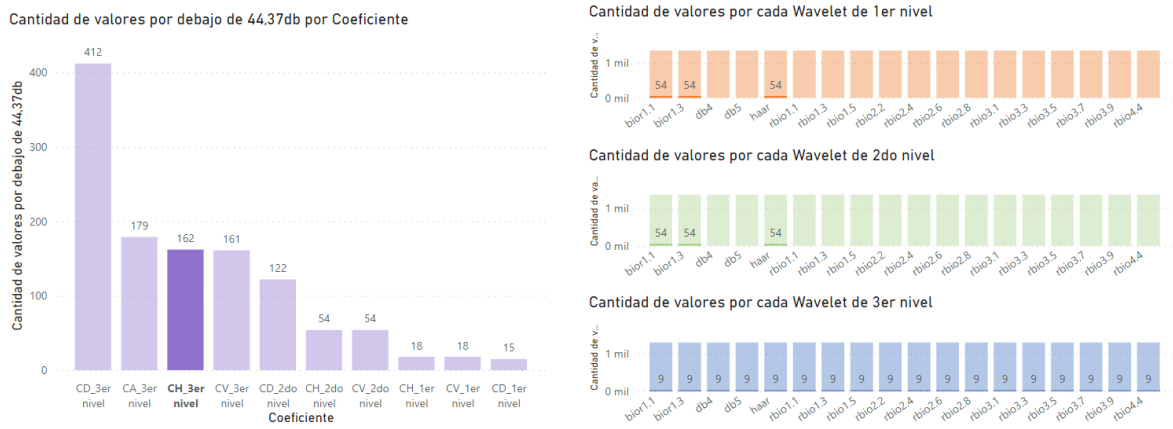


Figura 4.9. Valores por debajo del umbral para coeficientes horizontales de tercer nivel.

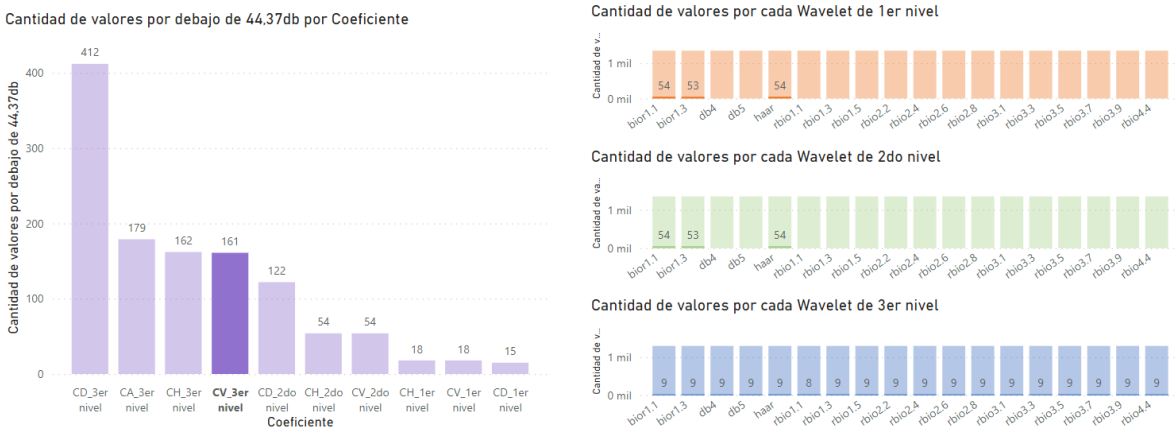


Figura 4.10. Valores por debajo del umbral para coeficientes verticales de primer nivel.

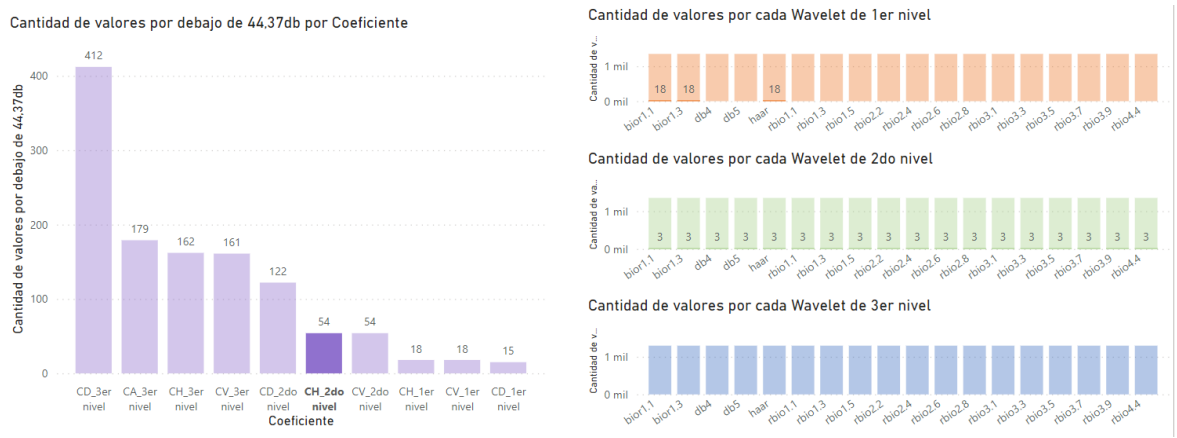


Figura 4.11. Valores por debajo del umbral para coeficientes horizontales de segundo nivel.

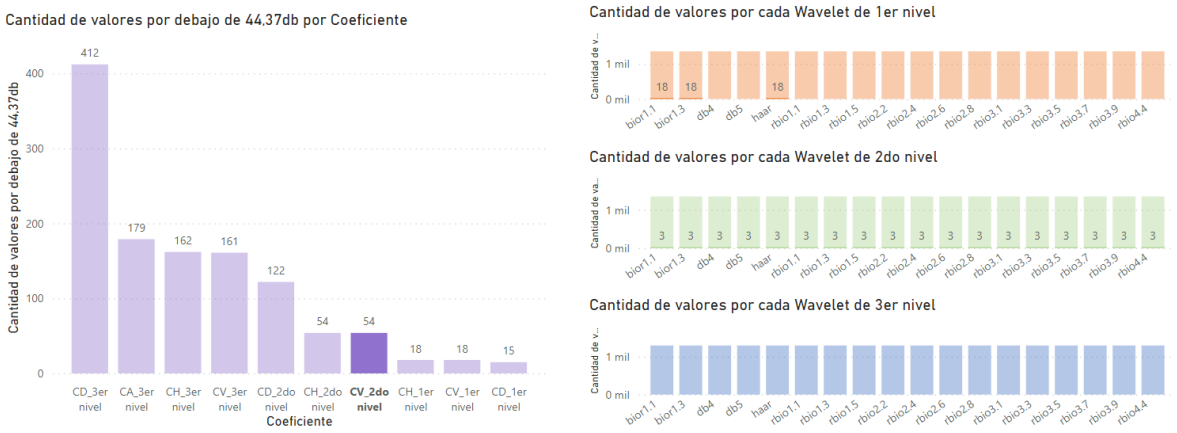


Figura 4.12. Valores por debajo del umbral para coeficientes verticales de segundo nivel.

Para los demás coeficientes (Coeficientes Verticales y Horizontales de primer nivel, Coeficientes diagonales de primer, segundo y tercer nivel y Coeficientes de aproximación de tercer nivel), no se presenta ningún patrón claro sobre las familias Wavelets que se ven afectadas.

Es así que, si se evita el uso de las 3 familias Wavelets mencionadas anteriormente (bior1.1, bior1.3 y haar), es posible utilizar como ROI los coeficientes horizontales y verticales de segundo y tercer nivel para un porcentaje de inserción del 100%, ya que, con la implementación en estos coeficientes, se obtienen valores de porcentaje de igualdad y de PSNR mayores a los umbrales establecidos. Cabe resaltar que no es necesario evitar el uso de las 5 familias que afectan el porcentaje de igualdad (Figura 4.7), ya que estas familias solo afectan los coeficientes de aproximación del tercer nivel, los cuales no son aptos como ROI según lo observado en los resultados de PSNR.

El evitar las familias bior1.1, bior1.3 y haar, no sólo resulta en la posibilidad del uso de las ROI que muestran el patrón de afectación claro con estas familias (CV,CH de segundo y tercer nivel), sino también en la facultad de utilizar los CD de tercer nivel.

Tras analizar gráficamente las combinaciones Wavelets que no superan el umbral en PSNR, omitiendo las 3 familias mencionadas anteriormente, se aprecia que todos los valores de PSNR para esta ROI superan el umbral de 44,37dB. Esto se ve reflejado en la Figura 4.13, la cual muestra la cantidad de valores por debajo del umbral de cada conjunto de coeficientes.

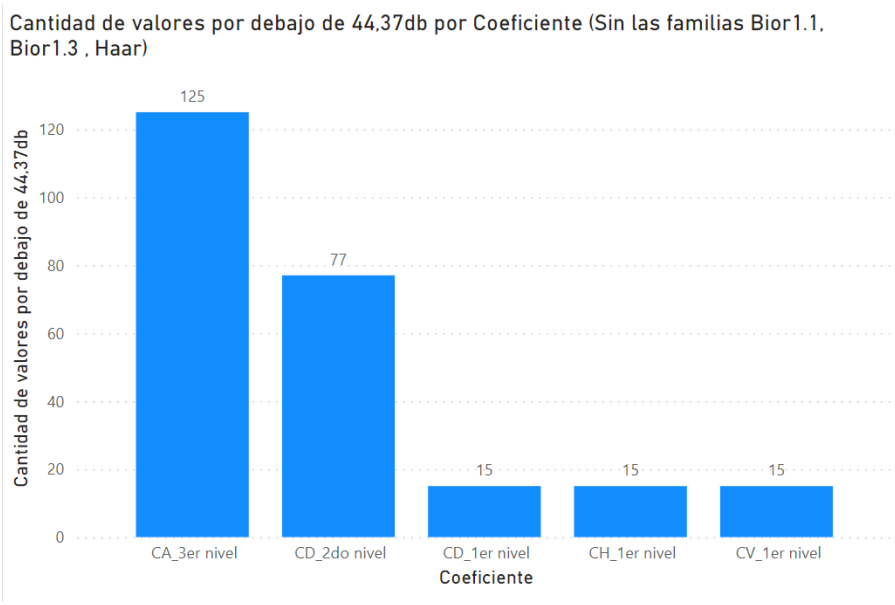


Figura 4.13. Cantidad de valores por debajo de 44,37dB sin las familias Bior1.1, Bior1.3 y Haar.

4.3. Escenario 3

Tras analizar cada una de las combinaciones de familias Wavelets ocultando una imagen correspondiente al 100% del tamaño de cada uno de los 10 conjuntos de coeficientes (Escenario 2), se procede a analizar el comportamiento de cada una de estas ROI al guardar imágenes de distinto tamaño (25%, 50%, 75% y, nuevamente, 100%), para obtener un panorama general del comportamiento del algoritmo de acuerdo con el tamaño de imagen secreta.

Para esta prueba se tomaron 7 combinaciones de familias Wavelets, considerando distintos valores tanto de PSNR como de porcentaje de igualdad en la prueba anterior, las combinaciones se muestran en la Figura 4.14.

WN1	WN2	WN3	Promedio de igualdad %	Promedio de PSNR Imagen Portada
bior1.1	bior1.1	bior1.1	99,43	43,78
haar	rbio3.9	rbio2.4	97,64	50,25
rbio3.1	rbio3.1	rbio3.1	85,92	43,82
rbio3.1	rbio3.3	rbio3.1	90,56	44,10
rbio3.5	rbio3.3	rbio3.5	96,87	44,50
rbio3.7	rbio3.3	rbio3.1	93,42	44,02
rbio3.9	rbio3.1	rbio3.9	94,56	44,09

Figura 4.14. Combinaciones de Wavelets escogidas.

Para estas pruebas, se mantiene el umbral establecido anteriormente, (95,64% para el porcentaje de igualdad y 44.37dB para la PSNR), de esta manera, en las figuras mostradas en este escenario, se utiliza el color azul para los valores por encima del umbral y el color rojo para los valores por debajo del umbral, tanto en porcentaje de igualdad como en PSNR.

La Figura 4.15 muestra el promedio del porcentaje de igualdad con los 4 porcentajes de inserción para todas las 7 combinaciones y se observa que la mayoría de los promedios superan el umbral escogido, a excepción el coeficiente de aproximación del tercer nivel, i.e., se mantiene el mismo comportamiento si se compara con el presentado en la prueba del 100% de inserción, en la cual este coeficiente fue el único con valores por debajo del umbral.

Figura 4.15 Promedios de igualdad generales para pruebas con 4 diferentes porcentajes.

A continuación, se analizan los promedios de PSNR para los 4 porcentajes de inserción, los resultados obtenidos (ver Figura 4.16) muestran que el promedio de PSNR de los coeficientes de aproximación del tercer nivel es un valor muy bajo respecto al valor umbral, esto concuerda con los resultados obtenidos en la sección anterior, siendo la ROI con la segunda mayor cantidad de valores por debajo del umbral, además de esto, los coeficientes diagonales de tercer nivel tampoco superan el umbral de 44,37dB.

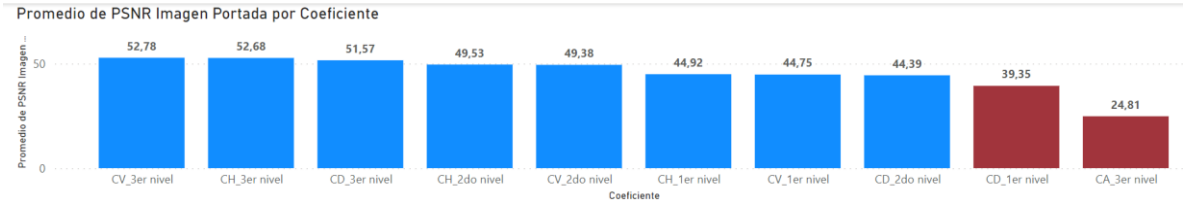


Figura 4.16. Promedios de PSNR para pruebas con diferentes porcentajes.

En la siguiente etapa de este escenario se analiza cada porcentaje de inserción de manera individual, con el fin de determinar de manera más específica las condiciones bajo las cuales se puede utilizar cada una de las ROI.

4.3.1. Análisis del 25% de inserción

Inicialmente se guarda una imagen que ocupa el 25% de cada coeficiente, al ser este el porcentaje de inserción más bajo utilizado en este escenario, se espera que la mayoría de los valores promedio de las ROI superen el umbral establecido. Para determinar lo anterior, se promedian, para cada conjunto de coeficientes, los 7 valores tanto de PSNR como de porcentaje de igualdad.

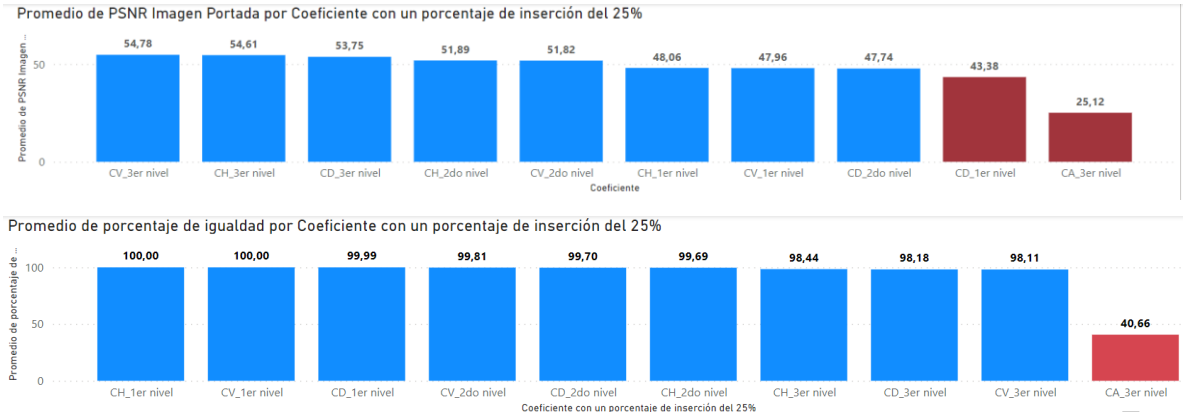


Figura 4.17 Promedio de PSNR y de porcentaje de igualdad para prueba con el 25% de capacidad de cada coeficiente.

La Figura 4.17 presenta un comportamiento similar al promedio de los 4 porcentajes de inserción, ya que son las mismas ROI que no superan los umbrales, tanto en PSNR como en porcentaje de igualdad. Teniendo en cuenta lo anterior, se puede inferir que estos coeficientes (CA de tercer nivel y CD de primer nivel) no son aptos para ser usados como ROI en este algoritmo, debido a que no superan el umbral establecido al insertar una imagen del 25% de la capacidad de la ROI.

4.3.2. Análisis del 50% de inserción

A continuación, se aumenta el porcentaje de inserción hasta un 50% de la capacidad de cada conjunto de coeficientes y se grafica el promedio de PSNR y porcentaje de igualdad para cada conjunto de coeficientes, tal como se muestra en la Figura 4.18.

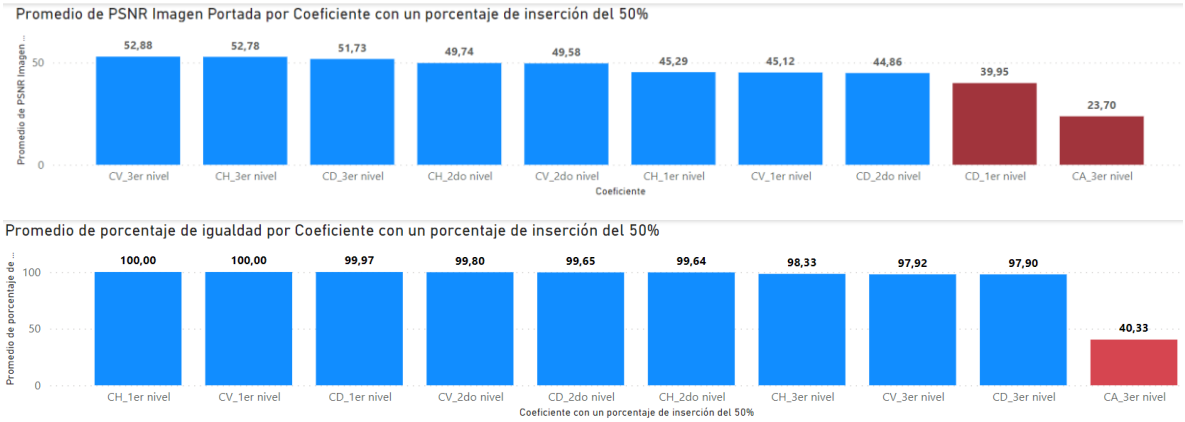


Figura 4.18. Promedio de PSNR y de porcentaje de igualdad para prueba con el 50% de capacidad de cada coeficiente.

Si se comparan los resultados de este porcentaje de inserción (ver Figura 4.18) con los resultados del 25% (ver Figura 4.17) se observa una reducción general del valor de PSNR en más o menos de 2 dB para cada ROI, lo que se entiende debido a que en esta prueba se afecta el 50% de la ROI; no obstante, esta reducción no genera que otros conjuntos de coeficientes (diferentes al CA de tercer nivel y al CD de primer nivel) reduzcan su promedio a un valor por debajo del umbral. Por otra parte, en la integridad de los datos se muestra una leve reducción general del porcentaje de igualdad.

4.3.3. Análisis del 75% de inserción

Posteriormente, se examinan los datos obtenidos tanto para el PSNR como para el porcentaje de igualdad para una inserción del 75%, con el fin de encontrar las ROI que no superen el umbral establecido.

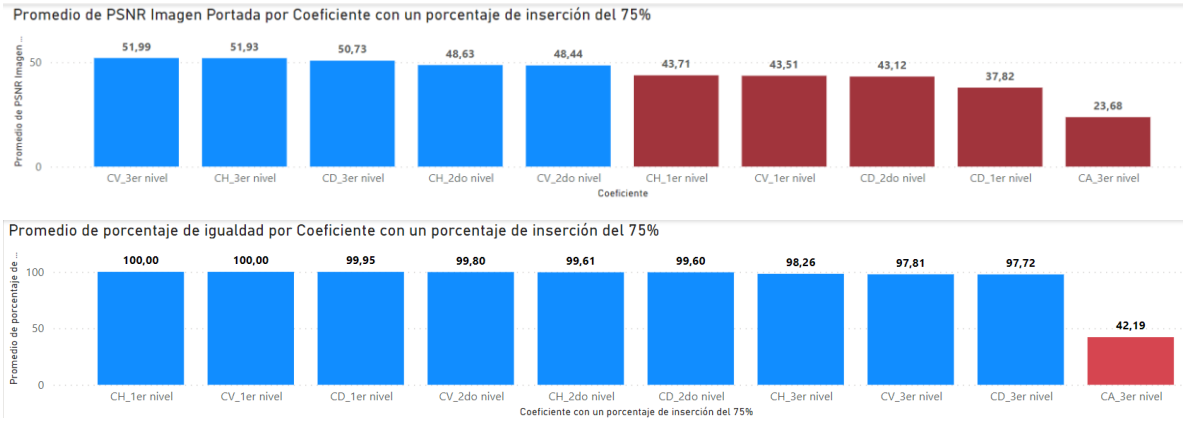


Figura 4.19. . Promedio de PSNR y de porcentaje de igualdad para prueba con el 75% de capacidad de cada coeficiente.

La Figura 4.19 muestra que este porcentaje de inserción del 75% genera que los CH y CV de primer nivel y los CD de segundo nivel (además del CD de 1er nivel y el CA de 3er) no superen el valor de 44.37dB. Lo anterior se produce ya que, al modificar la mayoría de los coeficientes de la ROI, se genera una afectación en estos coeficientes que produce una reducción en la imperceptibilidad de la imagen estego, en otras palabras, y acorde con lo planteado en el triángulo esteganográfico, a mayor capacidad de incrustación menor imperceptibilidad.

4.3.4. Análisis del 100% de inserción

Es importante aclarar que no se puede hacer una comparación directa entre los resultados del escenario 2 y los del escenario 3 debido al número de combinaciones de familias Wavelets consideradas, esta es la razón por la que en este escenario se repite la prueba para un porcentaje de inserción del 100%.

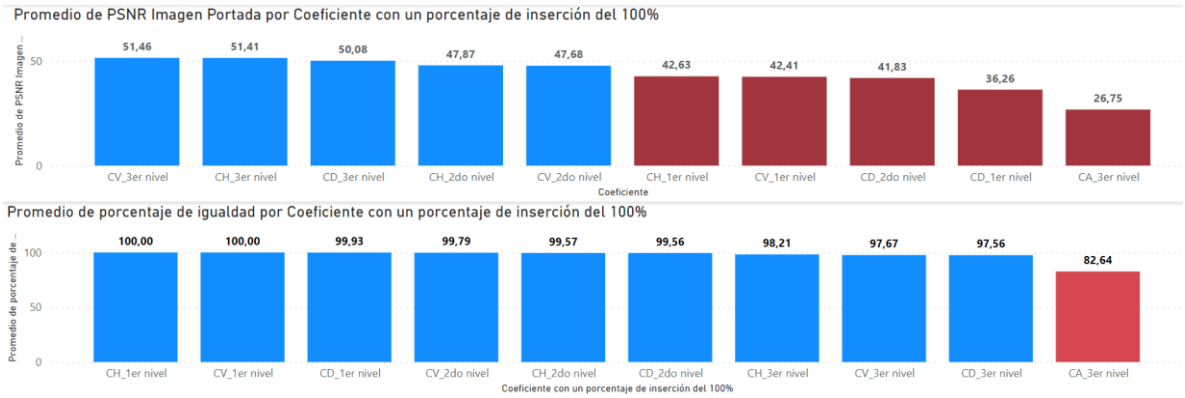


Figura 4.20. Promedio de PSNR y de porcentaje de igualdad para prueba con el 100% de capacidad de cada coeficiente.

Tras observar la Figura 4.20 se determina que los mismos conjuntos de coeficientes que no superan el umbral en la prueba del 75% (ver Figura 4.19), tampoco superan

el umbral para un porcentaje de inserción del 100%. En resumen, se puede concluir que no es posible usar los CA de tercer nivel, ni los CD de primer nivel, ya que tanto para el 25%,50%,75% y 100% su valor de PSNR está por debajo del umbral. Por otro lado, si la afectación es hasta del 50%, es posible usar los CH de primer nivel, los CV de primer nivel y los CD de segundo nivel, debido a que al aumentar el porcentaje de inserción de estos coeficientes a 75%, el valor de PSNR obtenido está por debajo del umbral de 44.37dB. Por último, es posible utilizar bajo cualquier porcentaje de afectación los CH, CV y CD de tercer nivel y los CH y CV de segundo nivel.

4.3.5. Porcentajes de inserción equivalentes

Hasta el momento se han analizado las diferentes ROI según el porcentaje de inserción, es decir, el porcentaje de coeficientes de cada ROI que se modifican. No obstante, como las ROI resultantes de la DWT tienen diferente tamaño, una imagen secreta se puede guardar en diferentes ROI variando el porcentaje de inserción.

La parte izquierda de la Figura 4.21 resume lo encontrado en las pruebas hasta el momento, esto es, las ROI que no es recomendable utilizar y las que se pueden utilizar hasta cierto porcentaje de inserción.

La parte derecha de la Figura 4.21 es una representación gráfica de las equivalencias de cada nivel de descomposición, por ejemplo, tomando el CV de tercer nivel, se aprecia que al tomar los cuatro cuadros de color amarillo que lo representan y colocarlos en el CV de segundo nivel, estos ocupan un 25% de este conjunto de coeficientes. De la misma manera si se observan los 16 cuadros verdes que ocupan el 100% del CH de segundo nivel, al representarlos en el CH de primer nivel, éstos llenan el 25% de este conjunto de coeficientes.

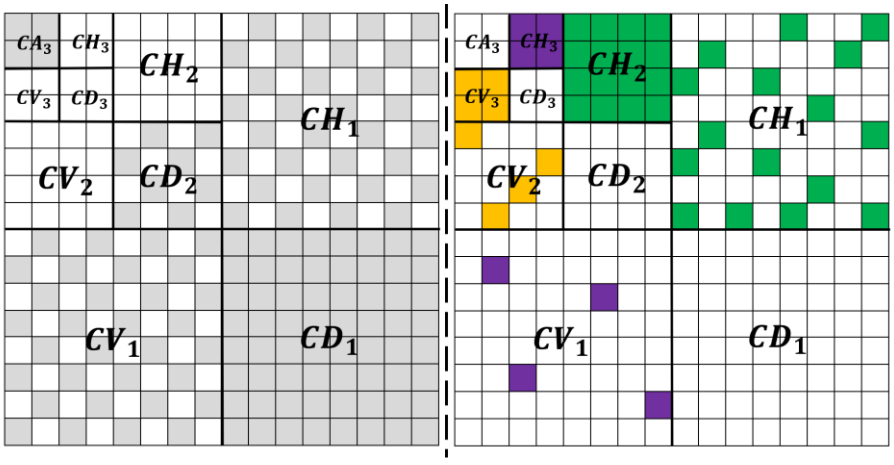


Figura 4.21 Equivalencias entre los coeficientes.

Para comparar las alternativas con las que se puede ocultar una imagen secreta variando la ROI, se evalúa la imperceptibilidad de la imagen estego y la integridad de los datos, i.e., se realiza una comparación del porcentaje de igualdad y la PSNR para porcentajes de inserción equivalentes. Para ello, inicialmente la Figura 4.22 muestra la diferencia del porcentaje de igualdad entre el 25% del primer nivel y el 100% del segundo nivel para los coeficientes horizontal y vertical[27]

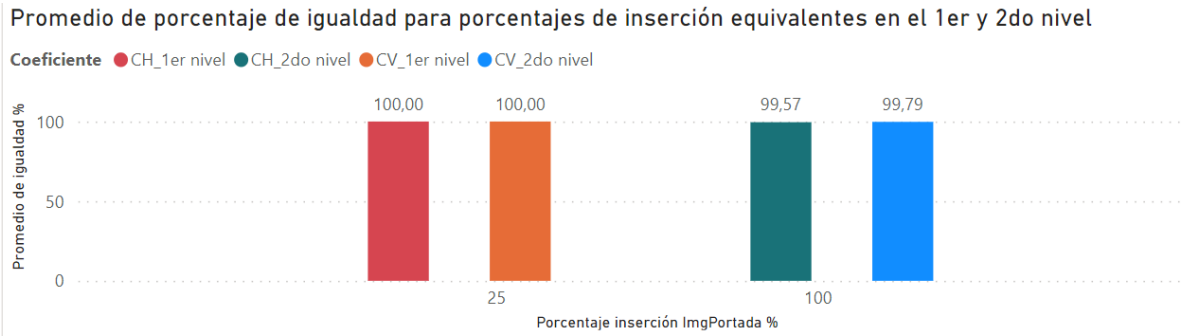


Figura 4.22. Diferencia de porcentajes de igualdad para equivalencias en el primer y segundo nivel.

En la Figura 4.22 se observa que, al usar el coeficiente horizontal o vertical del segundo nivel, resulta en una disminución en el porcentaje de igualdad; sin embargo, esta reducción es mínima y los valores obtenidos siguen siendo menores al 95.64%, lo que indica que se puede usar cualquiera de estos conjuntos de coeficientes sin que se afecte la integridad de la imagen secreta. De igual manera, se comparan estos dos escenarios tomando como referencia el valor de la PSNR.

La Figura 4.23 muestra que, de igual manera que con el porcentaje de igualdad, el uso de los coeficientes de segundo nivel comparados con sus equivalentes en el primer nivel, generan una pequeña reducción del valor de PSNR (menos de 1 dB), lo cual mantiene el nivel de imperceptibilidad por encima del umbral.

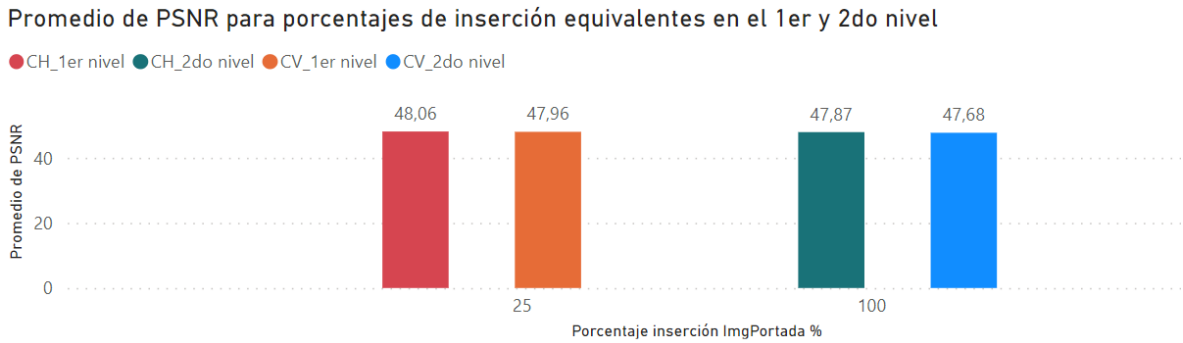


Figura 4.23. Diferencia de PSNR para equivalencias en el primer y segundo nivel.

[27] No se incluyen los coeficientes diagonales, ya que no son aptos para usarlos como ROI por lo demostrado en el Escenario 3.

A continuación, se realiza la misma comparación anterior, esta vez con los coeficientes del segundo y tercer nivel.

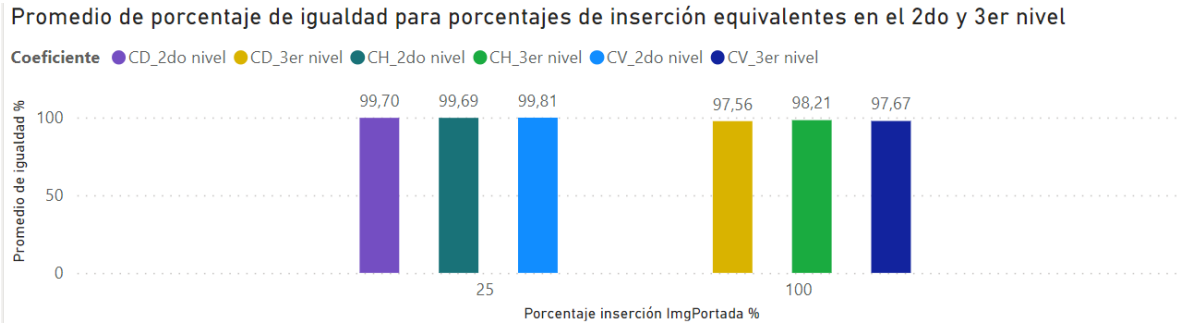


Figura 4.24. Diferencia de porcentajes de igualdad para equivalencias en el segundo y tercer nivel.

Se puede observar en la Figura 4.24 que, si bien el porcentaje de igualdad se reduce en mayor cantidad que entre el primer y segundo nivel (ver Figura 4.22), los niveles de igualdad se mantienen por encima del umbral. Para finalizar, se compara la PSNR para porcentajes equivalentes del segundo y tercer nivel.

La Figura 4.25 muestra que el uso de los CV y CD del tercer nivel, en comparación con sus semejantes del segundo nivel, reduce en menos de 1dB la PSNR. Por otra parte, al usar los CD de tercer nivel, el resultado tiene un mayor nivel de PSNR en comparación con los CD del segundo nivel, lo cual concuerda con los resultados obtenidos anteriormente, dado que solo los CD de tercer nivel no tienen restricciones en su uso como ROI.

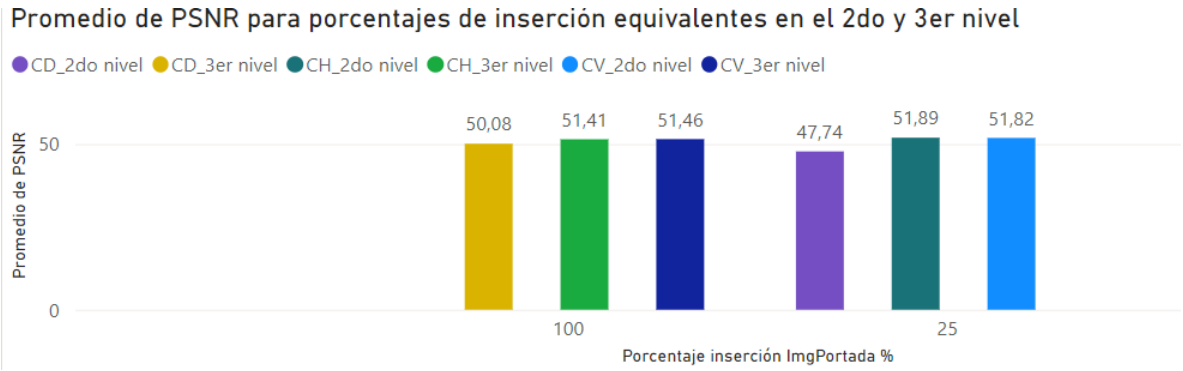


Figura 4.25. Diferencia de PSNR para equivalencias en el segundo y tercer nivel.

Todo lo planteado hasta ahora, indica que es posible usar porcentajes de inserción equivalentes para el algoritmo presentado en este trabajo de grado, debido a que no se encuentran cambios significativos ni en la integridad de la información, ni en la imperceptibilidad de la imagen estego.

4.4. Escenario Ideal Para el Algoritmo

Una vez realizadas las pruebas anteriores, se cuenta con la información necesaria para mostrar el escenario ideal con el cual el algoritmo planteado en este trabajo de grado genera su mayor rendimiento. Estas condiciones son:

- Las imágenes portada deben contener pocos valores cercanos a los tonos blancos o negros, la mayoría de los valores deben corresponder a tonos medios (grises).

- La cantidad de LSB utilizados al incrustar la información secreta debe ser igual a 3.

- Las imágenes secretas deben cumplir con el criterio de tamaño para asegurar la máxima capacidad de incrustación sin que se vea afectada ni la imperceptibilidad, ni la integridad de los datos.

- Las familias Wavelets usadas para realizar la DWT deben ser alguna de las siguientes

  {db4, db5, rbio1.1, rbio1.3, rbio1.5, rbio2.2, rbio2.4, rbio2.6, rbio2.8, rbio3.1, rbio3.3, rbio3.5, rbio3.7, rbio3.9, rbio4.4},

  es posible utilizar cualquier combinación de las anteriores 15 familias Wavelets hasta en 3 niveles de descomposición.

- Las ROI en las que se inserta la información secreta deben ser los CH, CV, CD de tercer nivel o los CH, CV de segundo nivel para cualquier grado de afectación. Por otra parte, si el grado de afectación de la ROI no excede el 50% de su tamaño, es posible usar los CH,CV de primer nivel o el CD de segundo nivel.

  Cabe resaltar que, si el tamaño de la imagen secreta es igual o menor al 25% del tamaño de un coeficiente de primer nivel, es posible usar como ROI tanto los coeficientes de primer nivel[28] como los de segundo nivel, ya que el 25% de un primer nivel de descomposición es igual al 100% de un segundo nivel de descomposición. De la misma manera se cumple si la imagen secreta tiene un tamaño igual o menor al 25% del segundo nivel, puesto que el 25% de un segundo nivel de descomposición es igual al 100% de un tercer nivel de descomposición, esto permite usar como ROI tanto los coeficientes del segundo nivel como los de tercer nivel[29].

[28] Excepto los CD de primer nivel.
[29] Excepto los CA de tercer nivel.

CONCLUSIONES

1. La transformada Wavelet es una herramienta útil para realizar esteganografía, ya que ésta permite la representación biunívoca de la información en un dominio transformado, con lo cual se pueden realizar aplicaciones más complejas para ocultar información y así mejorar la imperceptibilidad y robustez ante ataques. Esto le brinda al algoritmo planteado una buena ubicación en el *triángulo mágico de la esteganografía*. Además, se obtiene una robustez alta ante ataques de detección de error de nivel y sólo considerando las variaciones por las familias Wavelet se tienen 3.615 posibles combinaciones que tendría que considerar un atacante para poder acceder a la información secreta, no obstante, este algoritmo también genera aleatoriedad por la ubicación de la información y la selección de la ROI. Por otro lado, se definen aquellos factores que se deben configurar para que el algoritmo funcione correctamente, como lo son los niveles de grises de la imagen portada, la cantidad de LSB, la proporción P, el formato en el que se guarda la imagen estego, las familias Wavelets y las combinaciones de éstas. Un punto clave para el algoritmo planteado es la utilización de LWT, puesto que éste, junto con la transformada entera wavelet, facilitaron la inserción de la información secreta, definiendo una base para el uso de la WT en esteganografía.

2. Durante el proceso de detección de las ROI, se determina que su uso influye en las 3 aristas del *Triángulo Mágico de la Esteganografía,* debido a que las ROI están ligadas a la descomposición Wavelet. Esto significa que a medida que se aumentan los niveles de descomposición, la capacidad de incrustación se reduce, pero se aumenta la robustez ya que se cuenta con un mayor número de posibles combinaciones de familias Wavelets. Por otra parte, la imperceptibilidad se ve influenciada a razón de que se encuentran diferentes valores de PSNR para diferentes ROI; no obstante, es factible utilizar 8 de las 10 ROI inicialmente planteadas, las cuales repercuten en la imperceptibilidad según sea el grado de afectación aplicado al coeficiente. Esta afectación resulta en valores de PSNR menores al umbral establecido para algunas ROI, pero se concluye que, si se disminuye el porcentaje de inserción, se alcanzan los valores de PSNR establecidos por el umbral. Por otra parte, debido a las equivalencias del porcentaje de inserción, es posible utilizar una ROI de un nivel superior o inferior sin afectar el rendimiento del algoritmo.

3. Con base al análisis descrito, se establece que existen dos puntos clave que definieron el desarrollo del algoritmo propuesto. Primero está la transformada Wavelet y su variante con el algoritmo Lifting, que permitió la posibilidad de utilizar 15 familias Wavelets a diferentes niveles de descomposición y por el otro lado, la detección de ROI para concluir que es posible utilizar el 80% de los coeficientes Wavelets como ROI.

4. Cabe resaltar que se analizó cada bloque del diagrama del proceso esteganográfico de manera independiente para conseguir el máximo desempeño del algoritmo. Esto permitió encontrar la proporción de capacidad de incrustación adecuado para éste, también alcanzar niveles de imperceptibilidad que permiten que herramientas externas no detecten las alteraciones en la imagen estego y procurar el mayor porcentaje de integridad de los datos (robustez). Además, se evidencia que es un algoritmo con un alto grado de aleatoriedad y adaptabilidad, ya que, si se necesita para una aplicación que requiera una mayor robustez y no una gran capacidad de incrustación (o viceversa), es posible utilizar una u otra ROI debido a las equivalencias en el porcentaje de inserción. Por otra parte, se determina que no es práctico reducir el número de familias Wavelets para obtener resultados perfectos, ya que se prioriza la aleatoriedad del algoritmo y es por ello que se decide dejar un número elevado de posibilidades para tener más opciones de implementación.

TRABAJOS FUTUROS

- Determinar el grado de afectación de la imagen secreta si la imagen estego se corrompe.

- Analizar la influencia de la arquitectura del algoritmo LWT en el número de familias Wavelets y ROI que se pueden utilizar en el algoritmo de esteganografía propuesto.

- Generar una distribución de pixeles a múltiples ROI para aumentar la capacidad de inserción del algoritmo.

- Si a futuro el manejo de imágenes de escalas más grandes llega a ser comercial, implementar un cuarto nivel de descomposición y encontrar las familias Wavelets posibles a utilizar y sus ROI.

- Crear un algoritmo diseñado para atacar el esquema planteado en este trabajo de grado e intentar acceder a la información secreta.

- Exponer la imagen estego a una inteligencia artificial con el fin de verificar si logra extraer la imagen secreta.

REFERENCIAS

[1] M. Ghebleh and A. Kanso, “A robust chaotic algorithm for digital image steganography,” *Commun Nonlinear Sci Numer Simul*, vol. 19, no. 6, pp. 1898–1907, Jun. 2014, doi: 10.1016/J.CNSNS.2013.10.014.

[2] S. Sun, “A novel edge based image steganography with 2k correction and Huffman encoding,” *Inf Process Lett*, vol. 116, no. 2, pp. 93–99, Feb. 2016, doi: 10.1016/J.IPL.2015.09.016.

[3] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, “Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research,” *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/J.NEUCOM.2018.06.075.

[4] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, “A Novel DWT Based Image Securing Method Using Steganography,” *Procedia Comput Sci*, vol. 46, pp. 612–618, Jan. 2015, doi: 10.1016/J.PROCS.2015.02.105.

[5] N. F. Johnson, Z. Duric, and S. Jajodia, “Information Hiding: Steganography and Watermarking-Attacks and Countermeasures,” vol. 1, 2001, doi: 10.1007/978-1-4615-4375-6.

[6] P. Thiyagarajan and G. Aghila, “Reversible dynamic secure steganography for medical image using graph coloring,” *Health Policy Technol*, vol. 2, no. 3, pp. 151–161, Sep. 2013, doi: 10.1016/J.HLPT.2013.05.005.

[7] R. Jarusek, E. Volna, and M. Kotyrba, “Photomontage detection using steganography technique based on a neural network,” *Neural Netw*, vol. 116, pp. 150–165, Aug. 2019, doi: 10.1016/J.NEUNET.2019.03.015.

[8] J. Vico, “Esteganografía y estegoanálisis: Ocultación de datos en streams de audio Vorbis,” 2011.

[9] M. I. S. Reddy and A. P. S. Kumar, “Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm,” *Procedia Comput Sci*, vol. 85, pp. 62–69, Jan. 2016, doi: 10.1016/J.PROCS.2016.05.177.

[10] R. Roy, A. Sarkar, and S. Changder, “Chaos based Edge Adaptive Image Steganography,” *Procedia Technology*, vol. 10, pp. 138–146, Jan. 2013, doi: 10.1016/J.PROTCY.2013.12.346.

[11] M. S. Subhedar and V. H. Mankar, “Image steganography using redundant discrete wavelet transform and QR factorization,” *Computers & Electrical Engineering*, vol. 54, pp. 406–422, Aug. 2016, doi: 10.1016/J.COMPELECENG.2016.04.017.

[12] M. J. Tovée, “An introduction to the visual system,” *An Introduction to the Visual System*, pp. 1–228, Jan. 2008, doi: 10.1017/CBO9780511801556.

[13] H. Sajedi and M. Jamzad, “BSS: Boosted steganography scheme with cover image preprocessing,” *Expert Syst Appl*, vol. 37, no. 12, pp. 7703–7710, Dec. 2010, doi: 10.1016/J.ESWA.2010.04.071.

[14] X. Wu and C. N. Yang, “Invertible secret image sharing with steganography and authentication for AMBTC compressed images,” *Signal Process Image*

Commun, vol. 78, pp. 437–447, Oct. 2019, doi: 10.1016/J.IMAGE.2019.08.007.

[15] S. Chakraborty, A. S. Jalal, and C. Bhatnagar, “Secret image sharing using grayscale payload decomposition and irreversible image steganography,” *Journal of Information Security and Applications*, vol. 18, no. 4, pp. 180–192, Dec. 2013, doi: 10.1016/J.ISTR.2013.02.006.

[16] A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, “A multiple-format steganography algorithm for color images,” *IEEE Access*, vol. 8, pp. 83926–83939, 2020, doi: 10.1109/ACCESS.2020.2991130.

[17] S. Sidhik, S. K. Sudheer, and V. P. Mahadhevan Pillai, “Performance and analysis of high capacity Steganography of color images involving Wavelet Transform,” *Optik (Stuttg)*, vol. 126, no. 23, pp. 3755–3760, Dec. 2015, doi: 10.1016/J.IJLEO.2015.08.208.

[18] “Implementación de la Transformada Wavelet Discreta 2-D con filtros no separables* - PDF Descargar libre.” https://docplayer.es/85679895-Implementacion-de-la-transformada-wavelet-discreta-2-d-con-filtros-no-separables.html (accessed Mar. 13, 2023).

[19] R. Atta and M. Ghanbari, “A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set,” *J Vis Commun Image Represent*, vol. 53, pp. 42–54, May 2018, doi: 10.1016/J.JVCIR.2018.03.009.

[20] R. Karakiş, I. Güler, I. Çapraz, and E. Bilir, “A novel fuzzy logic-based image steganography method to ensure medical data security,” *Comput Biol Med*, vol. 67, pp. 172–183, Dec. 2015, doi: 10.1016/J.COMPBIOMED.2015.10.011.

[21] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3, pp. 727–752, Mar. 2010, doi: 10.1016/J.SIGPRO.2009.08.010.

[22] C. M. Vasco Estupiñan and F. R. Acosta Buenaño, “Una nueva técnica de transmisión segura de imágenes aplicando transformaciones de color reversibles en zonas ruidosas de la imagen / A new secure image transmission technique applying reversible color transformations in noisy regions of the image,” *RECI Revista Iberoamericana de las Ciencias Computacionales e Informática*, vol. 7, no. 13, pp. 80–105, Apr. 2018, doi: 10.23913/RECI.V7I13.80.

[23] N. A. Flayh and S. I. Ahson, “Wavelet Based image Encryption,” *International Conference on Signal Processing Proceedings, ICSP*, pp. 797–800, 2008, doi: 10.1109/ICOSP.2008.4697770.

[24] “(PDF) An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms.” https://www.researchgate.net/publication/275338264_An_experimental_study_on_Performance_Evaluation_of_Asymmetric_Encryption_Algorithms (accessed Mar. 13, 2023).

[25] E. Kawaguchi, “BPCS-steganography - Principle and applications,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3684 LNAI, pp. 289–299, 2005, doi: 10.1007/11554028_41/COVER.

[26] H. Noda, T. Furuta, M. Niimi, and E. Kawaguchi, “Application of BPCS steganography to wavelet compressed video,” *Proceedings - International*

Conference on Image Processing, ICIP, vol. 4, pp. 2147–2150, 2004, doi: 10.1109/ICIP.2004.1421520.

[27] R. X. Gao and R. Yan, “Wavelets: Theory and applications for manufacturing,” *Wavelets: Theory and Applications for Manufacturing*, pp. 1–224, 2011, doi: 10.1007/978-1-4419-1545-0/COVER.

[28] A. Djebbari and F. B. Reguig, “Short-time fourier transform analysis of the phonocardiogram signal,” *Proceedings of the IEEE International Conference on Electronics, Circuits, and Systems*, vol. 2, pp. 844–847, 2000, doi: 10.1109/ICECS.2000.913008.

[29] D. Espinosa Pérez and J. Delgado, “Wavelets y Superresolución,” 2012.

[30] I. Daubechies, “Where do wavelets come from? - a personal point of view,” *Proceedings of the IEEE*, vol. 84, no. 4, pp. 510–513, Apr. 1996, doi: 10.1109/5.488696.

[31] Y. Wang, Z. Li, C. Wang, L. Feng, and Z. Zhang, “Implementation of discrete wavelet transform,” *Proceedings - 2014 IEEE 12th International Conference on Solid-State and Integrated Circuit Technology, ICSICT 2014*, Jan. 2014, doi: 10.1109/ICSICT.2014.7021561.

[32] “Introducción a la Transformada Wavelet DESCOMPOSICIÓN DE SEÑALES”.

[33] R. A. Gopinath, J. E. Odegard, and C. S. Burrus, “Optimal Wavelet Representation of Signals and the Wavelet Sampling Theorem,” *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 41, no. 4, pp. 262–277, 1994, doi: 10.1109/82.285705.

[34] D. F. Walnut, “An Introduction to Wavelet Analysis,” p. 452.

[35] A. Cohen and A. J. Kovačević, “Wavelets: The mathematical background,” *Proceedings of the IEEE*, vol. 84, no. 4, pp. 514–522, 1996, doi: 10.1109/5.488697.

[36] “Implementación de la Transformada Wavelet Discreta 2-D con filtros no separables* - PDF Descargar libre.” https://docplayer.es/85679895-Implementacion-de-la-transformada-wavelet-discreta-2-d-con-filtros-no-separables.html (accessed Mar. 13, 2023).

[37] G. P. Nason and B. W. Silverman, “The Discrete Wavelet Transform in S,” *Journal of Computational and Graphical Statistics*, vol. 3, no. 2, p. 163, Jun. 1994, doi: 10.2307/1390667.

[38] M. Puttaraju and Dr. A. R. A. -, “FPGA Implementation of 5/3 Integer DWT for Image Compression,” *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 10, 2012, doi: 10.14569/IJACSA.2012.031030.

[39] H. Liao, M. K. Mandal, and B. F. Cockburn, “Efficient architectures for 1-D and 2-D lifting-based wavelet transforms,” *IEEE Transactions on Signal Processing*, vol. 52, no. 5, pp. 1315–1326, May 2004, doi: 10.1109/TSP.2004.826175.

[40] S. G. Mallat, “A Theory for Multiresolution Signal Decomposition: The Wavelet Representation,” *IEEE Trans Pattern Anal Mach Intell*, vol. 11, no. 7, pp. 674–693, 1989, doi: 10.1109/34.192463.

[41] W. Sweldens, “The Lifting Scheme: A Custom-Design Construction of Biorthogonal Wavelets,” *Appl Comput Harmon Anal*, vol. 3, no. 2, pp. 186–200, Apr. 1996, doi: 10.1006/ACHA.1996.0015.

[42] G. Puetamán, G. Hernán, and S. Escobar, “Compresión de imágenes usando wavelets,” 2007.
[43] Y. Chibani and A. A. Houacine, “Redundant versus orthogonal wavelet decomposition for multisensor image fusion,” *Pattern Recognit*, vol. 36, no. 4, pp. 879–887, Apr. 2003, doi: 10.1016/S0031-3203(02)00103-6.
[44] L. Vázquez and E. R. Cerezo, “Wavelets Proyecto Sistemas Informáticos”.
[45] B. Lei, I. Yann Soon, F. Zhou, Z. Li, and H. Lei, “A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition,” *Signal Processing*, vol. 92, no. 9, pp. 1985–2001, Sep. 2012, doi: 10.1016/J.SIGPRO.2011.12.021.
[46] “(PDF) A Three Cycle View of Design Science Research.” https://www.researchgate.net/publication/254804390_A_Three_Cycle_View_of_Design_Science_Research (accessed Mar. 13, 2023).
[47] “Forensically, free online photo forensics tools - 29a.ch.” https://29a.ch/photo-forensics/#error-level-analysis (accessed Mar. 19, 2023).
[48] “FotoForensics - Analysis.” https://fotoforensics.com/analysis.php?id=00c1c6e04963c3ce3cf351e9d313520e04c94da5.9895983 (accessed Mar. 19, 2023).
[49] “Google Lens: Busca lo que ves.” https://lens.google/intl/es-419/#cta-section (accessed Mar. 19, 2023).
[50] “TinEye Reverse Image Search.” https://tineye.com/ (accessed Mar. 19, 2023).

APÉNDICE A: PROPIEDADES DE LA IMAGEN PORTADA

Para obtener un análisis objetivo sobre cómo la integridad de la información se ve afectada por características de imágenes portada como: la saturación, el contraste o la exposición; se realizan diferentes pruebas con la misma imagen portada y la misma imagen secreta, pero antes de cada prueba, a la imagen portada se le varían los niveles de cada propiedad en específico[30]. Posteriormente se aplica el algoritmo de esteganografía para comparar la imagen secreta original con la imagen resultante tras la extracción de la información al finalizar el proceso; las imágenes escogidas se muestran en la Figura A.1, donde en la parte superior se encuentran las imágenes originales, que son modificadas en cada prueba, y en la parte inferior su equivalente en escala de grises[31], las cuales se utilizan en el algoritmo de esteganografía.

Figura A.1. Imágenes base para pruebas de propiedades de la imagen.

La Figura A.1 muestra la imagen portada a la izquierda (Elmo), esta imagen tiene un tamaño de 1024×1024 pixeles, mientras que la imagen de la derecha (Rana René) es tomada como imagen secreta y su tamaño es de 225×225 pixeles. Para

[30] Estos cambios en la imagen se logran mediante el uso de la herramienta de edición de fotografía *Snapseed* desarrollada por *Google.inc*.
[31] Resultado de promediar sus valores en cada una de las 3 matrices RGB.

obtener un umbral de comparación, se incrusta la imagen secreta en imagen portada sin ninguna modificación previa.

En la Figura A.2 es mostrada la imagen resultante tras incrustar la imagen secreta en la imagen portada original; la pérdida de información es notoria y tras hacer la comparación bit a bit entre la imagen secreta original y la imagen secreta resultante, se encuentra un porcentaje de igualdad de 44.37%. Este porcentaje es tomado como valor base para determinar si las pruebas realizadas en las secciones posteriores aumentan o disminuyen la integridad de la información en el algoritmo.

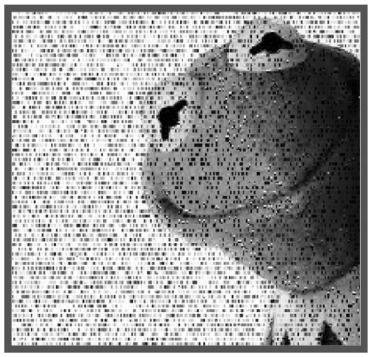


Figura A.2. Imagen secreta reconstruida tras incrustarla en Elmo sin modificar.

A.1. Saturación

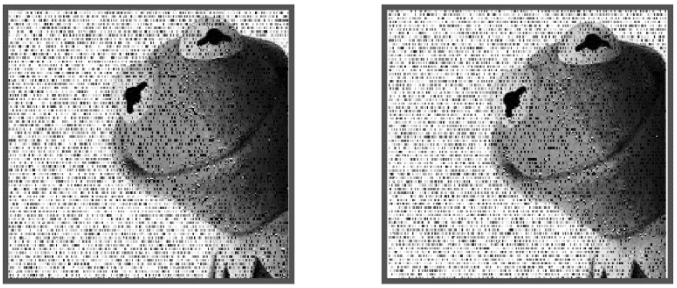
Teniendo en cuenta que la saturación es la intensidad del color en cada pixel de la imagen, en una imagen con altos niveles de saturación, los colores se ven más vívidos, mientras que, en una imagen con saturación baja, los colores pierden intensidad hasta obtener una imagen en escala de grises. De este modo, se realiza la edición correspondiente a la imagen secreta.

Alta saturación Baja saturación

Figura A.3. Imagen portada con alta y baja saturación.

En la Figura A.3, se muestra por una parte la imagen portada (Elmo) en escala de grises tras su modificación en saturación. Estas son las nuevas dos imágenes portada y en ambas se incrusta la información de la imagen secreta (Rana René).

Al finalizar los dos procesos esteganográficos, se extrae la información oculta de ambas imágenes estego, se reconstruyen las dos imágenes secretas y se mide el porcentaje de igualdad de cada una de ellas con respecto a la imagen de la Rana René original.



Alta saturación Baja saturación

Figura A.4. Imágenes de la Rana René resultantes tras incrustación en imágenes portada con alta y baja saturación.

Tras un análisis visual de la Figura A.4, no se puede determinar si el uso de imágenes portada modificadas en saturación, generan una mejora o reducción de la integridad en la imagen secreta, es por ello que se realiza la comparación bit a bit entre las dos imágenes resultante y la imagen secreta original.

Tabla A.1. Porcentaje de igualdad tras prueba de saturación.

	Imagen portada sin cambios	Cambiando Saturación	
		Alta	Baja
% Igualdad Imagen secreta (Comparación Bit a bit)	44.37%	44.55%	44.64%

Con ayuda de la Tabla A.1 se logra comparar el porcentaje de igualdad entre la imagen secreta recuperada a partir de la imagen portada original y las imágenes secretas resultantes de incrustar la información en imágenes portada con variaciones en sus niveles de saturación. A partir de estos resultados, se infiere que modificar la saturación en la imagen portada no tiene, en este caso, un efecto notable en el porcentaje de igualdad. Por lo anterior, se considera que la saturación no representa una propiedad fundamental para aumentar la integridad de la información en el sistema, es por ello por lo que no se toma en cuenta como factor discriminador al momento de elegir la imagen portada para el algoritmo planteado.

A.2. Exposición

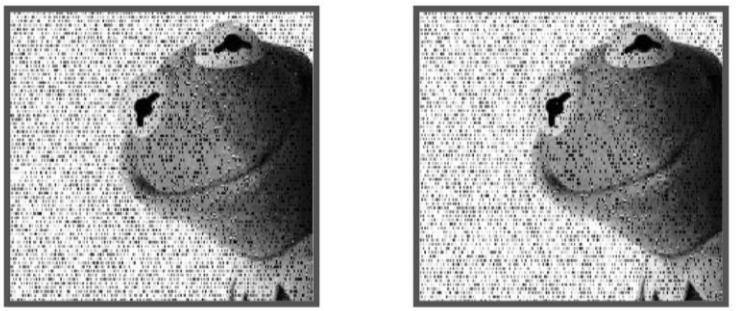
La exposición refleja la cantidad de luz presente en los colores de una imagen, así, mientras mayor sea su exposición, más cerca estarán sus colores a los blancos puros, hasta ser una imagen totalmente blanca; mientras que, a menor exposición, menor es la cantidad de luz en los colores, por lo que la imagen tiende a ser más oscura, hasta llegar a ser totalmente negra. La aplicación *Snapseed* no modifica la

imagen hasta los extremos de exposición; sin embargo, la diferencia luminosa alcanzada en las imágenes de la Figura A.5 es suficiente para que el efecto sea notorio.

Alta exposición Baja exposición

Figura A.5. Imagen portada con alta y baja exposición.

Contando con las nuevas dos imágenes portada, se procede a realizar el ocultamiento la imagen secreta en cada una de ellas. Posteriormente, se obtiene el porcentaje de igualdad tras extraer las dos imágenes secretas resultantes y compararlas con la imagen secreta original.



Alta exposición Baja exposición

Figura A.6. Resultados del algoritmo usando imagen portada con alta y baja exposición.

De igual manera que con la prueba de saturación, la Figura A.6 no permite notar visualmente un cambio significativo en ninguna de las dos imágenes resultantes, por ello, se analiza de manera cuantitativa, cuyos resultados se condensan en la Tabla A.2.

Tabla A.2. Porcentaje de igualdad tras prueba de exposición.

	Imagen portada sin cambios	Cambiando Exposición	
		Alta	Baja
% Igualdad Imagen secreta (Comparación Bit a bit)	44.3733%	43.6168%	47.4963%

En la Tabla A.2 se muestra una diferencia de casi un 4% en el porcentaje de igualdad entre las imágenes resultantes tras la prueba con alta y baja exposición. Además de ello, al comparar estos resultados con los de la imagen resultante generada a partir de la imagen portada sin cambios, se aprecia un decrecimiento del porcentaje de igualdad para la prueba de alta exposición y un ligero aumento al usar la imagen con baja exposición, sin embargo, este margen de mejora es únicamente de 3.1%, el cual no se considera un valor suficiente para determinar que una baja exposición represente un aumento significativo en la integridad de la información resultante al aplicar el algoritmo de esteganografía.

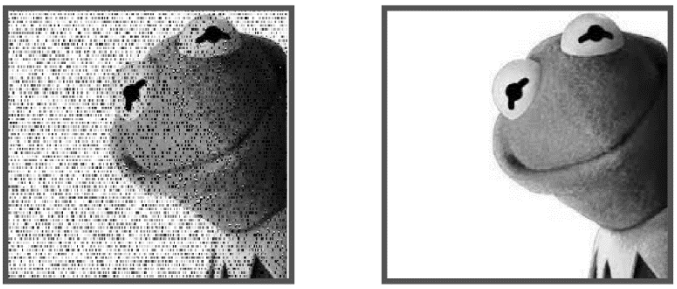
A.3 Contraste

A diferencia de la exposición, en la que se modifican todos los colores de la imagen para llevarlos hacia los blancos o los negros puros, al aumentar el contraste, los tonos claros se llevan hacia los blancos y los tonos oscuros se llevan hacia los negros; mientras que, al reducir el contraste, se llevan tanto los tonos claros, como los oscuros hacia los tonos medios (grises), esto hace que la imagen se vea de manera homogénea y sin colores que resalten respecto a otros. Lo anterior se puede apreciar en la Figura A.7, donde a la izquierda está la imagen portada con alto contraste y a la derecha la imagen con bajo contraste.

Alto contraste Bajo contraste

Figura A.7. Imagen portada con alto y bajo contraste.

Posteriormente, se incrusta la imagen secreta en cada una de esas imágenes portada y los resultados obtenidos tras el proceso esteganográfico se muestran en la Figura A.8.



Alto contraste Bajo contraste

Figura A.8. Resultados del algoritmo usando imagen portada con alto y bajo contraste.

Visualmente, la Figura A.8 muestra que la prueba de bajo contraste tiene una mejora sustancial al compararla con la prueba de alto contraste y además se aprecia una gran similitud a la imagen de la rana René original. Para comprobar lo anterior, se realiza la comparación bit a bit entre las imágenes extraídas y la imagen secreta original.

Tabla A.3. Porcentaje de igualdad tras prueba de contraste.

	Imagen portada sin cambios	Contraste	
		Alta	Baja
% Igualdad Imagen secreta (Comparación Bit a bit)	44.3733%	44.47%	100%

La Tabla A.3 muestra que el margen de mejora es mínimo para la imagen de alto contraste, por el contrario, con la prueba de bajo contraste se logra un 100% de igualdad al comparar bit a bit con la imagen original. Por esta razón, en la sección A.4 se procede a realizar un análisis detallado de los cambios ocurridos en una imagen tras modificar su contraste, con el fin de clarificar la razón por la que en esta prueba se obtuvo un alto nivel de integridad en los datos para el algoritmo planteado.

A.4. Análisis de blancos, negros, sombras y brillos

Con el fin de comprender los cambios generados a una imagen tras modificar su contraste se hace uso de un histograma, dado que éste permite visualizar la forma en la que están distribuidos los valores de los pixeles de una imagen de acuerdo con los distintos tonos en los que se encuentran. La Figura A.9 muestra que los tonos en una imagen pueden ser blancos, luces, medios (o grises), sombras y negros.

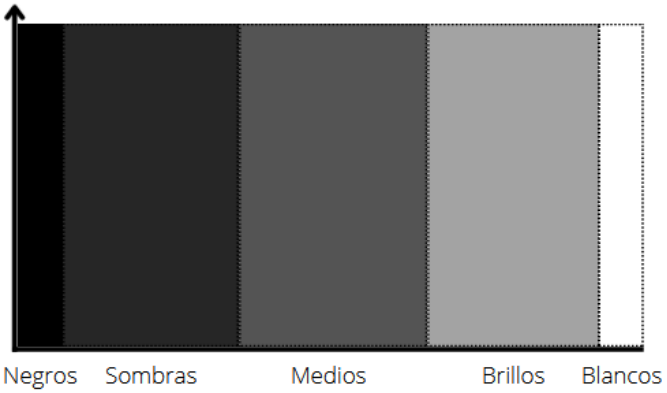


Figura A.9. Distribución de tonos en una imagen en escala de grises.

En este orden de ideas, una imagen totalmente blanca, que tiene todos sus pixeles en los tonos blancos (255), tiene asociado un histograma con un comportamiento impulsivo en 255, tal como se evidencia en la Figura A.10.

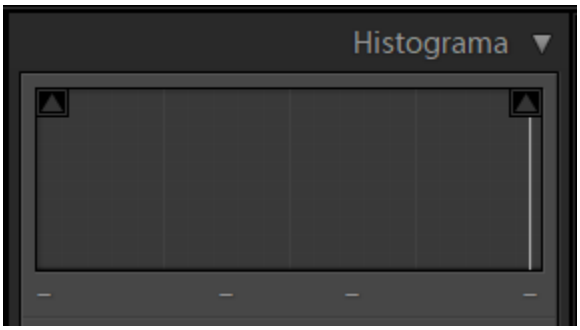


Figura A.10. Histograma de una imagen totalmente blanca.

A continuación, se realiza el histograma sobre la imagen portada original, en escala de grises, utilizada en las pruebas de la sección anterior. La Figura A.11 muestra el histograma de la imagen portada, en el cual se aprecia la distribución de los valores de los pixeles de la imagen. El histograma muestra que se tienen picos muy altos en los tonos blancos, negros y en las sombras. Por otro lado, el histograma de la imagen portada de Elmo con bajo contraste (ver Figura A.12) muestra que los valores de los pixeles se mueven hacia los tonos medios, es decir, todos los pixeles que se encontraban en los tonos blancos y negros se encuentran ahora en los tonos de brillos y de sombras, por lo cual la imagen portada carece de pixeles de valor 0 y de valor 255.

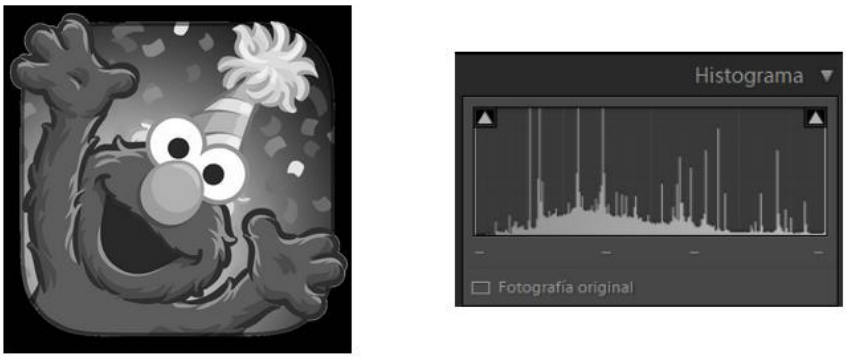


Figura A.11. Histograma de imagen portada Elmo.

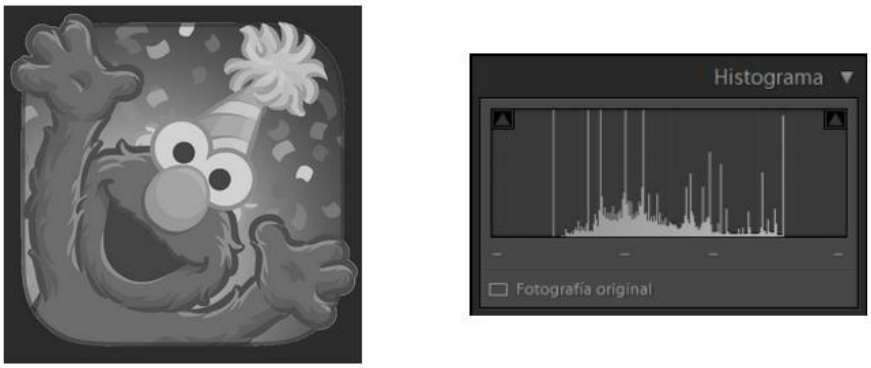


Figura A.12. Histograma de imagen portada con bajo contraste.

Para el algoritmo planteado en el presente trabajo de grado, al guardar información en los pixeles blancos y negros, se presentan pérdidas en gran porcentaje de la información secreta, es por ello que, para lograr la integridad de la información secreta, se deben evitar imágenes portada que contengan valores en los tonos blancos y negros. Para lograr esto, se implementa una función que clasifica los pixeles con el fin encontrar la cantidad de blancos y negros presentes en las imágenes y determinar si son aptas como imágenes portada. Cabe aclarar que estas condiciones se cumplen para el algoritmo planteado en el presente trabajo de grado, ya que las características de las imagen portada pueden cambiar de acuerdo con el proceso esteganográfico que se lleve a cabo, Por ejemplo, en [132] se menciona que para ese algoritmo planteado lo que se busca son imágenes con alto contraste y menor homogeneidad.

APÉNDICE B: TABLAS DE RESULTADOS

Los datos relacionados con las pruebas presentadas en la sección 3.3 y la sección 4.1 se encuentran disponible en el directorio siguiente:

https://drive.google.com/drive/folders/1xiOS4Ha59c8vEET6amSZANbvK987Pe-C?usp=sharing

En esta carpeta se encuentran 3 archivos correspondientes a las pruebas realizadas a 1,2 y 3 niveles de descomposición respectivamente.

- El archivo *1 nivel de descomposición* contiene una tabla con los resultados encontrados en porcentaje de igualdad de la imagen secreta y PSNR de la imagen portada al guardar una imagen secreta en una imagen portada, con 39 Wavelets distintas a un nivel de descomposición. Estos resultados han sido utilizados para las pruebas de la sección 4.1.

- El archivo *2 niveles de descomposición* contiene una tabla con los resultados de porcentaje de igualdad de la imagen secreta, encontrados al insertar cada una de las 6 imágenes secretas en 6 imágenes portada utilizando 39 Wavelets de primer nivel y 39 Wavelets de segundo nivel. Los datos de este archivo han sido útiles para las pruebas realizadas en la sección 3.3 y la sección 4.1.

- El archivo *3 niveles de descomposición* contiene una tabla que muestra los resultados de porcentaje de igualdad y PSNR, para la prueba realizada al guardar una imagen secreta en una imagen portada, usando 22 familias Wavelets de primer nivel, 35 familias de segundo nivel y 39 familias de tercer nivel. Estos datos han sido utilizados para las pruebas realizadas en la sección 4.1.