

**MARCAS DE AGUA ROBUSTAS A ATAQUES  
GEOMÉTRICOS**

**TESIS**

Que para obtener el grado de  
**MAESTRÍA EN CIENCIAS EN INGENIERÍA ELÉCTRICA**

presenta

**Sergio Bravo Solorio**

**Félix Calderón Solorio**

**Director de Tesis**

Universidad Michoacana de San Nicolás de Hidalgo

**septiembre 2007**



*A María Elena  
y todos los frutos  
que florezcan de  
nuestro amor*



## Agradecimientos

En primer lugar, quiero agradecer a mi esposa, María Elena Lemus, por todo su cariño, confianza, paciencia y buen humor, que siempre me ayudaron a continuar con mi trabajo hasta terminar.

Tengo la fortuna de haber recibido una sólida formación por parte de mis padres, Lucila Solorio y Sigifredo Bravo. Les agradezco por transmitirme esa avidez por seguir avanzando profesionalmente, sin menospreciar, en ningún momento, la importancia que tienen las relaciones familiares, que tan profundamente nos han inculcado a mi hermana, Cinthia Bravo, y a mí. Me faltaría vida para retribuirles, a mis padres y a mi hermana, todo lo que han hecho por mí. Sólo quiero que sepan que siempre les estaré infinitamente agradecido.

Gracias a mis abuelos, tíos, primos y sobrinos por todo ese afecto que me han demostrado y por todas sus enseñanzas que, de una u otra forma, han contribuido para ir alcanzando mis metas.

Agradezco el apoyo que siempre me han proporcionado mis amigos Antonio Pola, Guadalupe Bedolla, Alfredo Rodríguez, J. Manuel Torres, Ricardo Magaña, Yetzi Hurtado, Erika Barbosa, Gerardo Zavala, Carlos A. Orozco, Rubén Sánchez y Edgar J. Juárez. Gracias también a mis compañeros y amigos que me acompañaron, ayudaron y regañaron durante estos dos años: Mario Graff, Eric S. Téllez y Luis E. Gamboa.

Quiero agradecer especialmente a Félix Calderón, Leonardo Muñoz, Antonio Camarena, Julio C. Herrera, Marlene Flores y todos aquellos profesores que, con su conocimiento y paciencia, han sembrado en mí el gusto por seguir aprendiendo.



## Resumen

Los avances tecnológicos ofrecen formas más económicas y rápidas para copiar y distribuir datos multimedia con gran calidad. Consecuentemente, se han propuesto técnicas de marcas de agua para evitar y detectar violaciones a los derechos de autor, falsificaciones, etc. Sin embargo, como cualquier otra señal digital, las imágenes pueden sufrir un enorme conjunto de distorsiones que pueden dañar seriamente, e incluso eliminar, las marcas de agua insertadas. Las distorsiones geométricas usualmente causan detecciones erróneas en la mayoría de los esquemas, debido a la pérdida de sincronización entre las marcas de agua y los detectores. Se han propuesto algunas estrategias para enfrentar los efectos de las distorsiones geométricas en los esquemas de marcas de agua, ya sea insertando patrones de sincronización junto con las marcas de agua, o utilizando dominios invariantes o semi-invariantes. No obstante, las debilidades identificadas en dichas estrategias hacen de éste, un problema abierto para nuevas contribuciones. En esta tesis se propone una nueva estrategia que utiliza un detector basado en un Algoritmo Genético que maximiza la correlación entre la marca de agua insertada originalmente y la imagen de entrada. Se propone además una implementación de esta estrategia y se reportan algunos resultados obtenidos al aplicar distorsiones con una herramienta estándar, los cuales muestran que el esquema es robusto a rotación, escalamiento, traslación, filtrado, compresión con pérdida (JPEG), entre otras distorsiones. También, se reportan comparaciones entre un esquema de marcas de agua previo, basado en mapas log-polar, y la presente contribución. Los resultados muestran que el esquema propuesto es más robusto y causa una menor degradación en las imágenes, a pesar de utilizar un proceso de inserción simple.



# Abstract

Technological advances afford cheaper and faster forms of copying and distributing multimedia data with high quality. Consequently, watermarking techniques have been proposed to prevent and detect copyright infringements, tampering, and so on. However, like any digital signal, images might experience a huge set of distortions that can severely damage, and even destroy, the embedded watermarks. Geometrical distortions usually lead to erroneous detections in most watermarking schemes, due to synchronisation loss between watermarks and detectors. Some strategies have been proposed to counterattack the effects of geometrical distortions in watermarking schemes, by either embedding synchronisation-patterns along with the watermarks or by using invariant or semi-invariant domains. Nevertheless, the pitfalls detected in such strategies leave the problem open for further contributions. In this thesis a new strategy is proposed, which is based on a Genetic Algorithm that attempts to maximise the correlation between the originally inserted watermark and the input image. An implementation of this strategy is proposed and reported results, obtained after applying distortions with a standard benchmark, show the proposed scheme is resilient to rotation, scaling, translation, filtering, lossy-compression (JPEG), among other distortions. Furthermore, comparisons between a previous watermarking method, based on log-polar maps, and the present approach are reported. Results show the proposed scheme provides more robustness and lower image degradation, even when a simple insertion process is used.



# Contenido

|  |      |
|--|------|
| Agradecimientos . . . . .  | V    |
| Resumen . . . . .  | VII  |
| Abstract . . . . .   | IX   |
| Contenido . . . . .  | XI   |
| Lista de Figuras . . . . .   | XIII |
| Lista de Tablas . . . . .  | XV   |
| Lista de Algoritmos . . . . .  | XVII |
| Lista de Símbolos . . . . .  | XIX  |
| Lista de Publicaciones . . . . .   | XXI  |
| <br>   |      |
| 1. Introducción . . . . .  | 1    |
| 1.1. Antecedentes . . . . .  | 1    |
| 1.2. Planteamiento del Problema . . . . .  | 3    |
| 1.3. Objetivos de la Tesis . . . . .   | 3    |
| 1.4. Descripción de Capítulos . . . . .  | 4    |
| <br>   |      |
| 2. Marcas de Agua en Imágenes Digitales . . . . .                                | 7    |
| 2.1. Principios Básicos . . . . .  | 8    |
| 2.2. Requerimientos y Aplicaciones . . . . .                                     | 9    |
| 2.3. Evaluación de los Sistemas de Marcas de Agua . . . . .                      | 12   |
| 2.4. Efectos de los Ataques Geométricos en Marcas de Agua . . . . .              | 14   |
| 2.4.1. Distorsiones geométricas comunes en imágenes digitales . . . . .          | 15   |
| 2.5. Estrategias Propuestas para Contrarrestar los Ataques geométricos . . . . . | 16   |
| 2.5.1. Búsqueda exhaustiva . . . . .   | 16   |
| 2.5.2. Patrones de sincronización . . . . .                                      | 17   |
| 2.5.3. Auto-sincronización . . . . .   | 18   |
| 2.5.4. Dominios invariantes . . . . .  | 19   |
| 2.5.5. Extracción de características . . . . .                                   | 20   |
| <br>   |      |
| 3. Revisión de Esquemas . . . . .  | 23   |
| 3.1. Mapas Log-Polar y Transformada de Fourier-Mellin . . . . .                  | 23   |
| 3.1.1. Propiedades de la DFT . . . . .   | 23   |
| 3.1.2. Mapa log-polar . . . . .  | 24   |
| 3.1.3. Transformada Fourier-Mellin . . . . .                                     | 27   |

|        |   |    |
|--------|---|----|
| 3.1.4. | Discusión sobre los mapas log-polar . . . . .               | 28 |
| 3.2.   | Esquema Basado en Fourier-Mellin . . . . .                  | 29 |
| 3.2.1. | Proceso de inserción . . . . .                              | 29 |
| 3.2.2. | Proceso de detección . . . . .                              | 29 |
| 3.2.3. | Discusión del esquema . . . . .                             | 31 |
| 3.3.   | Esquema de Lin Basado en LPM . . . . .                      | 33 |
| 3.3.1. | Descripción general del esquema . . . . .                   | 33 |
| 3.3.2. | Proceso de inserción . . . . .                              | 34 |
| 3.3.3. | Proceso de detección . . . . .                              | 37 |
| 3.3.4. | Experimento . . . . .                                       | 38 |
| 3.3.5. | Discusión del esquema . . . . .                             | 40 |
| 3.4.   | Conclusiones del Capítulo . . . . .                         | 41 |
| 4.     | Contribuciones . . . . .                                    | 45 |
| 4.1.   | Justificación del Método de Optimización . . . . .          | 45 |
| 4.2.   | Descripción General de la Estrategia . . . . .              | 48 |
| 4.3.   | Proceso de Inserción . . . . .                              | 49 |
| 4.4.   | Proceso de Detección . . . . .                              | 50 |
| 4.4.1. | Especificaciones del AG . . . . .                           | 51 |
| 4.4.2. | Filtro para mejorar la correlación . . . . .                | 54 |
| 4.5.   | Pasos del Proceso de Detección Propuesto . . . . .          | 56 |
| 5.     | Resultados . . . . .  | 59 |
| 5.1.   | Filtro para Mejorar la Detección . . . . .                  | 59 |
| 5.2.   | Definición del Umbral de Detección . . . . .                | 60 |
| 5.3.   | Pruebas Estándares . . . . .                                | 62 |
| 5.3.1. | Correlación usando diferentes valores de $\alpha$ . . . . . | 62 |
| 5.3.2. | Compresión con pérdida . . . . .                            | 64 |
| 5.3.3. | Adición de ruido . . . . .                                  | 64 |
| 5.3.4. | Eliminación de líneas . . . . .                             | 65 |
| 5.3.5. | Convolución con diferentes filtros . . . . .                | 65 |
| 5.3.6. | Rotación y escalamiento . . . . .                           | 69 |
| 5.4.   | Comparación de Resultados . . . . .                         | 72 |
| 5.4.1. | Distorsión de las imágenes marcadas . . . . .               | 72 |
| 5.4.2. | Casos de estudio . . . . .                                  | 72 |
| 5.4.3. | Comparación de tiempos . . . . .                            | 74 |
| 6.     | Conclusiones . . . . .                                      | 77 |
| 6.1.   | Conclusiones Generales . . . . .                            | 77 |
| 6.2.   | Trabajo Futuro . . . . .                                    | 78 |
|        | Referencias . . . . .                                       | 79 |
|        | Glosario . . . . .  | 87 |
|        | Índice . . . . .  | 93 |

# Lista de Figuras

|   |    |
|---|----|
| 2.1. Esquema de marcas de agua general. . . . .   | 9  |
| 2.2. Presentación de resultados de dos sistemas diferentes. . . . .   | 14 |
| 3.1. Imágenes en coordenadas cartesianas y log-polar. . . . .   | 26 |
| 3.2. Distorsiones causadas por los procesos de LPM e ILPM. . . . .  | 30 |
| 3.3. Esquema de O'Ruanaidh basado en Fourier-Mellin. . . . .  | 32 |
| 3.4. Espectro de Fourier de una imagen real. . . . .  | 36 |
| 3.5. Imagen marcada y la correlación obtenida al probar con 500 marcas de agua<br>diferentes. . . . .   | 41 |
| 3.6. Pruebas de ataques geométricos simples. . . . .  | 42 |
| 3.7. Pruebas de ataques geométricos compuestos. . . . .   | 43 |
| 4.1. Medidas de correlación detectadas entre la imagen distorsionada y la marca<br>de agua modificada por diferentes parámetros de rotación y escalamiento. . . | 47 |
| 4.2. Descripción general de la estrategia propuesta. . . . .  | 49 |
| 4.3. Esquemas de inserción y extracción propuestos. . . . .   | 52 |
| 4.4. Distribución de la población inicial. . . . .  | 54 |
| 4.5. Funcionamiento del filtro para mejorar la correlación. . . . .   | 55 |
| 5.1. Correlación detectada utilizando cuatro diferentes filtros. . . . .  | 60 |
| 5.2. Probabilidad de falsos positivos dependiendo del umbral. . . . .   | 61 |
| 5.3. Imágenes estándares utilizadas. . . . .  | 62 |
| 5.4. Imágenes creadas con diferentes valores de $\alpha$ . . . . .  | 63 |
| 5.5. Resultados de pruebas de $\alpha$ y compresión JPEG. . . . .   | 63 |
| 5.6. Imágenes comprimidas con JPEG. . . . .   | 65 |
| 5.7. Resultados de pruebas de ruido y eliminación de líneas. . . . .  | 66 |
| 5.8. Imágenes marcadas a las que se les agregó ruido. . . . .   | 66 |
| 5.9. Eliminación de renglones y columnas de las imágenes marcadas. . . . .  | 67 |
| 5.10. Imágenes distorsionadas con diferentes filtros. . . . .   | 68 |
| 5.11. Ataques geométricos. . . . .  | 71 |
| 5.12. Comparación de la distorsión causada por los procesos de inserción. . . . .   | 73 |
| 5.13. Imágenes marcadas con el esquema propuesto en esta tesis y el basado en<br>LPM. . . . .   | 75 |



# Lista de Tablas

|   |    |
|---|----|
| 5.1. Pruebas de convolución con diferentes filtros. . . . . | 68 |
| 5.2. Pruebas de rotación y escalamiento. . . . .            | 70 |
| 5.3. Casos de estudio. . . . .                              | 73 |



# Lista de Algoritmos

|    |  |    |
|----|--|----|
| 1. | Proceso de inserción de Ruanaidh . . . . . | 31 |
| 2. | Proceso de detección de Ruanaidh . . . . . | 32 |
| 3. | Proceso de inserción de Lin . . . . .      | 37 |
| 4. | Proceso de detección de Lin . . . . .      | 39 |
| 5. | Proceso de inserción propuesto . . . . .   | 51 |
| 6. | Proceso de detección propuesto . . . . .   | 57 |



# Lista de Símbolos

| Símbolos                                 | Descripción   |
|--|---|
| $\overset{\mathcal{F}}{\leftrightarrow}$ | Cambio del dominio del tiempo al de la frecuencia y viceversa.  |
| $\circ$                                  | Composición de transformaciones.  |
| $*$                                      | Convolución de funciones.   |
| $\alpha$                                 | Parámetro para controlar la energía de un esquema de marcas de agua.  |
| $\eta = [-1, 1]$                         | Filtro Bidimensional de Diferencias Separable (SBD-WF).   |
| $\theta$                                 | Parámetro de rotación de un punto en una representación log-polar.  |
| $\theta'$                                | Índice de la suma de ángulos ortogonales.   |
| $\lambda$                                | Peso de un coeficiente en un mapa log-polar, utilizando interpolación bilineal.                                       |
| $\mu$                                    | Parámetro que representa el logaritmo natural de la distancia de un punto al origen, en una representación log-polar. |
| $\mu_{max}$                              | Distancia máxima de un píxel respecto del origen de una imagen.   |
| $\sigma$                                 | Parámetro de escalamiento.  |
| $\tau$                                   | Umbral de detección.  |
| $\phi$                                   | Parámetro de rotación de un ataque.   |
| $\Omega_i$                               | Cromosoma del $i$ -ésimo individuo de un AG.  |
| $C_i$                                    | Costo del $i$ -ésimo individuo de un AG.  |
| $C_n$                                    | Correlación normalizada.  |
| $f(x, y)$                                | Imagen en el dominio espacial.  |
| $f(\mu, \theta)$                         | Imagen en el dominio espacial en coordenadas log-polar.   |
| $\hat{f}(x, y)$                          | Imagen en el dominio espacial rotada, escalada y trasladada.  |
| $\bar{f}(x, y)$                          | Imagen de entrada en un detector.   |
| $f_w(x, y)$                              | Imagen, en el dominio espacial, que ha sido marcada.  |
| $F(k, l)$                                | Imagen en el dominio de la frecuencia.  |
| $\hat{F}(k, l)$                          | Imagen, en el dominio de la frecuencia, rotada, escalada y trasladada.  |
| $\bar{F}(k, l)$                          | Imagen en el dominio de la frecuencia de entrada en un detector.  |
| $F_w(k, l)$                              | Imagen, en el dominio de la frecuencia, que ha sido marcada.  |
| $F(\mu, \theta)$                         | Imagen en el dominio de la frecuencia representada con coordenadas log-polar.   |
| $F_M(k, l)$                              | Imagen en el dominio de Fourier-Mellin.   |
| $ F(k, l) $                              | Magnitud de Fourier de una imagen.  |
| $ \hat{F}(k, l) $                        | Magnitud de Fourier de una imagen rotada, escalada y trasladada.  |

---

**Símbolos**    **Descripción**


---

|                       |   |
|-----------------------|---|
| $ \bar{F}(k, l) $     | Magnitud de Fourier de una imagen de entrada en un detector.  |
| $ F_w(k, l) $         | Magnitud de una imagen marcada.   |
| $\Phi F(k, l)$        | Fase de Fourier de una imagen.  |
| $\ln  F(k, l) $       | Logaritmo natural de la magnitud de Fourier de una imagen.  |
| $\ln  \bar{F}(k, l) $ | Logaritmo natural de la magnitud de Fourier de una imagen de entrada en un detector.                                      |
| $\ln  F_w(k, l) $     | Logaritmo natural de la magnitud de una imagen marcada.   |
| $g$                   | Vector de proyección de la magnitud de Fourier a 1-D.   |
| $k$ y $l$             | Índices de imágenes en el dominio de la frecuencia.   |
| $M_C$                 | Total de columnas de un mapa log-polar.   |
| $M_R$                 | Total de renglones de un mapa log-polar.  |
| $mix(g_1, w)$         | Función de mezclado que encuentra un vector lo suficientemente parecido a $g_1$ , pero lo suficientemente cercano a $w$ . |
| $N_w$                 | Longitud de marca de agua en 1-D.   |
| $N_C$                 | Total de columnas de una imagen.  |
| $N_R$                 | Total de renglones de una imagen.   |
| $p_w(x, y)$           | Patrón pseudoaleatorio con distribución Gaussiana, con media cero y varianza uno.   |
| $\mathcal{R}$         | Transformación de rotación.   |
| $\mathcal{S}$         | Transformación de escalamiento.   |
| $w$                   | Marca de agua original.   |
| $w_m$                 | Marca de agua mejorada por una función <i>mix</i> .   |
| $\bar{w}$             | Marca de agua extraída.   |
| $\hat{w}$             | Marca de agua rotada, escalada y trasladada.  |
| $(x_0, y_0)$          | Parámetros de traslación en $x$ y $y$ .   |

# Lista de Publicaciones

- S. Bravo y F. Calderón. Maximum Correlation Search Based Watermarking Scheme Resilient to RST. En *10th Iberoamerican Congress on Pattern Recognition, CIARP'05. Lecture Notes in Computer Science*, Habana Cuba, Noviembre 15-18, 2005.
- S. Bravo. Panorama de las Marcas de Agua en Imágenes Digitales. En *Ciclo de Exposiciones y Conferencias en ESIME Culhuacán (CECEC'04)*, México D.F., Marzo, 2004.



# Capítulo 1

## Introducción

### 1.1. Antecedentes

Gracias a los nuevos avances tecnológicos es posible compartir datos digitales con mayor calidad, utilizando menos recursos de almacenamiento y distribución. No es difícil imaginar que existan personas dispuestas a utilizar estas tecnologías para vulnerar algunas leyes; sobre todo aquellas relacionadas con la propiedad intelectual o derechos de autor. Como consecuencia, se han propuesto técnicas para insertar información imperceptible en los datos digitales con el fin de detectar reproducciones ilegales. A estas técnicas se les conoce en la literatura como esquemas de marcas de agua digitales.

Las distorsiones que pueden sufrir las señales digitales pueden dañar severamente las marcas de agua que contienen. Si hablamos de imágenes digitales, por ejemplo, la mayoría de los esquemas reportan errores cuando se intenta detectar una marca de agua en alguna imagen que han sufrido distorsiones geométricas (e.g. rotación, escalamiento, traslación, etc.). A este problema se le conoce en la literatura como *pérdida de sincronización* [Licks03], pues las distorsiones geométricas no destruyen las marcas de agua, pero cambian su posición a localidades desconocidas para los detectores.

Cuando la imagen original (sin marcar) está disponible para el detector, la sincronización se puede restaurar utilizando técnicas convencionales de registro de imágenes [Brown92]. Sin embargo, los esquemas de marcas de agua difícilmente son provistos de

las imágenes originales en aplicaciones reales. Por esta razón, se han desarrollado diferentes estrategias para solucionar la pérdida de sincronización causada por las distorsiones geométricas en los esquemas de marcas de agua.

Algunas estrategias proponen insertar un patrón junto con la marca de agua, o bien, sugieren insertar una marca de agua periódica que genere un patrón determinado al calcular la autocorrelación de la imagen marcada [Fleet97, Pereira99a, Pereira99b, Pereira00, Kutter98, Delannay02, Deguillaume02]. Dichos patrones son detectados y utilizados para invertir cualquier tipo de transformación afín. Se ha demostrado que estas estrategias proporcionan robustez ante distorsiones geométricas, pero son incapaces de restaurar la sincronización una vez que los patrones son removidos utilizando ataques de colusión [Craver00, Ergün99] o filtros especializados [Herrigel01, Licks03].

Otra estrategia consiste en insertar las marcas de agua en dominios invariantes a algunas distorsiones geométricas, o bien, en dominios semi-invariantes, en donde ciertas distorsiones se convierten en otras más sencillas de resolver. En [O' Ruanaidh97] se propuso por primera vez utilizar el dominio de Fourier-Mellin, el cual es invariante a Rotación, Escalamiento y Traslación (RST, por sus siglas en inglés). El esquema es teóricamente robusto a RST en señales continuas, pero su implementación en señales discretas requiere de procesos de discretización que pueden degradar significativamente las marcas de agua. Lin *et al.* [Lin01] proponen un esquema robusto a RST que inserta las marcas de agua modificando los coeficientes de Fourier de la imagen, dependiendo de su contribución con un mapa log-polar. Este esquema mejora el desempeño del algoritmo propuesto por O'Ruanaidh, pero conserva algunos problemas numéricos inherentes a la discretización utilizada en los mapas log-polar. Otros esquemas robustos a RST proponen insertar/detectar las marcas de agua en versiones normalizadas de las imágenes [Alghoniemy00, Dong02]. Sin embargo, la sincronización no se puede restaurar si los parámetros de normalización cambian debido a recortes en las imágenes marcadas. En general, algunas distorsiones geométricas severas ocasionan detecciones erróneas debido a la degradación que sufren las marcas de agua a causa de la discretización e interpolación necesarias en los dominios invariantes o semi-invariantes en los que se basan este tipo de esquemas.

En contribuciones más recientes se propone enfrentar el problema insertando las marcas de agua en regiones cercanas a ciertas características extraídas de las imágenes (e.g. esquinas, bordes, etc.) [Bas02, Feng02, Tang03]. Desafortunadamente, la robustez de este tipo de esquemas dependen, en gran parte, de la precisión de los algoritmos de extracción de características utilizados.

## 1.2. Planteamiento del Problema

La mayoría de los esquemas de marcas de agua reportan detecciones erróneas cuando se aplican distorsiones geométricas en las imágenes marcadas. Las debilidades identificadas en las estrategias propuestas para resolver la sincronización de los esquemas de marcas de agua, hacen de éste un campo abierto para nuevas contribuciones.

Concretamente, se requiere una estrategia que no inserte patrones para resolver la sincronización de los esquemas de marcas de agua, los cuales pueden ser fácilmente removidos por ataques de colusión y filtros especializados [Craver00, Ergün99, Herrigel01, Licks03]. Además, es necesario que la estrategia propuesta no utilice dominios invariantes o semi-invariantes que requieran de procesos de discretización, los cuales pueden degradar las marcas de agua disminuyendo su robustez ante ataques geométricos severos.

## 1.3. Objetivos de la Tesis

El objetivo general de la tesis es proponer una nueva estrategia que logre restablecer la sincronización, la cual se pierde debido a ataques de RST en los esquemas de marcas de agua.

Los objetivos específicos que se persiguen son los siguientes:

- Insertar/detectar las marcas de agua en el dominio de Fourier, el cual reúne las siguientes propiedades importantes:
  - La pérdida de información que se genera al calcular esta transformada no es significativa para los propósitos de los esquemas de marcas de agua.
  - La magnitud de Fourier es invariante a traslación.

- Se conocen perfectamente los efectos que se tienen en este dominio cuando se aplica rotación y escalamiento en el dominio espacial.
  - En general, se ha demostrado que los esquemas que utilizan este dominio para insertar/detectar las marcas de agua son robustos a una gran variedad de distorsiones como compresión con pérdida y diversos filtros.
- Resolver la sincronización sin utilizar dominios que requieran de métodos de discretización e interpolación.
  - No utilizar patrones para resolver la sincronización, los cuales pueden ser fácilmente removidos por ataques de colusión y filtros especializados.
  - Medir el desempeño del esquema propuesto utilizando herramientas de distorsión estándares.
  - Comparar la estrategia propuesta con un esquema robusto a RST.

## 1.4. Descripción de Capítulos

En esta tesis se presentan los temas importantes para la comprensión de las contribuciones y resultados alcanzados por el presente proyecto de investigación, organizados de la siguiente manera. El Capítulo 2 contiene los conceptos básicos de las marcas de agua, algunas de sus aplicaciones y requerimientos. También se definen las distorsiones geométricas y se discuten las estrategias propuestas hasta ahora para restablecer la sincronización en los esquemas de marcas de agua digitales. En el Capítulo 3 se describen el dominio de Fourier-Mellin y los mapas log-polar, los cuales son utilizados en algunos esquemas de marcas de agua para evitar la pérdida de sincronización debido a distorsiones geométricas. Se discuten además, dos esquemas robustos a RST propuestos en la literatura. En el Capítulo 4 se propone una nueva estrategia basada en un detector con un mecanismo de optimización que encuentra los parámetros de RST con los cuales se atacó una imagen marcada. Asimismo, se describen los procesos de inserción y extracción de un esquema que implementa la estrategia propuesta. En el Capítulo 5 se discuten los resultados obtenidos con el esquema

propuesto al aplicar distorsiones con una herramienta estándar, y algunas comparaciones con un esquema basado en mapas log-polar. Finalmente, algunas conclusiones y futuras extensiones de este trabajo se presentan en el Capítulo 6.



## Capítulo 2

# Marcas de Agua en Imágenes Digitales

Los esquemas de marca de agua describen técnicas que se utilizan para transmitir información que es insertada en datos digitales de forma imperceptible para los sentidos humanos [Kutter00]. La facilidad con que se puede copiar y transmitir información digital ha impulsado el desarrollo de esquemas de marcas de agua como estrategia para evitar o detectar algunas infracciones, como la distribución ilegal de datos digitales (especialmente imágenes, audio y video). La presente tesis se enfoca específicamente en marcas de agua aplicadas sobre imágenes digitales, por lo tanto, los esquemas aplicados sobre otro tipo de datos quedan fuera del alcance de este documento. Para más información sobre marcas de agua en general, se recomienda consultar [Kutter00, Cox02].

En este capítulo se presenta el material introductorio más importante sobre las marcas de agua digitales organizado de la siguiente manera. En la Sección 2.1 se revisan los conceptos más importantes de los esquemas de marcas de agua. Los principales requerimientos y aplicaciones de las marcas de agua se discuten en la Sección 2.2. Los efectos de las distorsiones geométricas en las marcas de agua y las estrategias que se han propuesto para solucionarlos se discuten en las Secciones 2.4 y 2.5, respectivamente. Finalmente, en la Sección 2.3 se describen las herramientas y procedimientos, considerados estándares, que se utilizan para evaluar el desempeño de los esquemas de marcas de agua.

## 2.1. Principios Básicos

Todos los algoritmos de marcas de agua comparten el mismo esquema general, el cual se divide en un *proceso de inserción* y un *proceso de detección o extracción*.

En la Figura 2.1(a) se muestra el proceso general de inserción de un esquema de marcas de agua. La marca de agua, utilizada como entrada del proceso, puede ser numérica o representar otro tipo de información visual o de texto. En general, los procesos de inserción se pueden clasificar en dos grandes grupos:

- *inserción ciega* - en donde las imágenes originales se ven como un simple canal de transmisión que no es analizado para diseñar las marcas de agua. Ejemplos de esquemas que utilizan este tipo de inserción son los propuestos en [vanSchyndel94, Cox97, Cox02].
- *inserción informada o no ciega*- en donde se analizan las características de las imágenes para establecer los parámetros más adecuados (e.g. localización, energía, etc.) de las marcas de agua. Algunos esquemas que utilizan este tipo de inserción son los propuestos en [Cox02, Feng02, Tang03].

El proceso general de detección se muestra en la Figura 2.1(b). Kutter y Hartung [Kutter00] proponen una clasificación que divide los procesos de detección en tres grandes grupos, que son:

- *detección privada o no ciega* - en donde se requiere, al menos, de la imagen original para poder extraer la marca de agua. Ejemplos de esquemas en donde se utiliza este tipo de detección son los propuestos en [Cox97, O' Ruanaidh97].
- *detección semi-privada o semi-ciega* - en donde no se requiere de la imagen original, pero sí de la marca de agua insertada originalmente. Comúnmente, este tipo de detectores sólo indican la existencia o ausencia de una marca de agua. Este tipo de detectores se utilizan en los esquemas propuestos en [Kundur97, Lin01, Cox02].
- *detección pública o ciega* - que representan el mayor reto, ya que no se requiere ni de la imagen original, ni de la marca de agua insertada originalmente. Un ejemplo de este tipo de esquemas es el propuesto en [Bloom99].

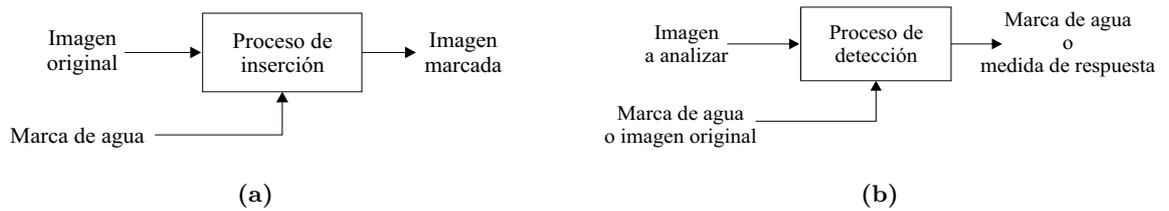


Figura 2.1: Esquema de marcas de agua general. (a) Proceso de inserción. (b) Proceso de detección.

## 2.2. Requerimientos y Aplicaciones

Algunos autores afirman que la marca de agua ideal debería ser capaz de resistir cualquier tipo de distorsión, antes de que la calidad de la *imagen protegida*<sup>1</sup> se degrade hasta perder su utilidad [Kutter00, Cox02]. Por la complejidad que requiere el diseño de tal esquema, usualmente se diseñan marcas de agua robustas a distorsiones relacionadas con aplicaciones específicas. Por ejemplo, si se desea diseñar marcas de agua en datos que se van a transmitir por televisión analógica, sería necesario que dichas marcas fueran robustas a las distorsiones causadas por ruido aditivo y multiplicativo, corrección de color y contraste, conversiones A/D y D/A, etc.

En la literatura, las distorsiones que se aplican a una imagen protegida sin la intención de alterar la marca de agua, se conocen como *ataques accidentales*. Dependiendo de la aplicación, los ataques accidentales incluyen la compresión con pérdida, cambio de formato, corrección de la imagen, etc. En contraste, las distorsiones que requieren análisis más sofisticados se consideran *ataques incidentales*, puesto que se aplican en una imagen protegida con el propósito de eliminar o modificar la marca de agua. Por ejemplo, un atacante podría tener acceso a un conjunto de imágenes iguales protegidas con diferentes marcas de agua y promediarlas para obtener una imagen con poca distorsión y con baja probabilidad de detección (ataque de *colusión* [Craver00, Ergün99]). Otro ataque consiste en dividir las imágenes protegidas en fragmentos pequeños que no contienen suficiente información para detectar las marcas de agua, los cuales son publicados con la ayuda de un navegador de Internet simulando una sola imagen (ataque de *mosaico* [Craver00]).

<sup>1</sup>En el resto de la tesis, una imagen marcada será referida también como una *imagen protegida*.

Kutter y Hartung [Kutter00] consideran que las distorsiones que se aplican con mayor frecuencia a las imágenes protegidas son:

- mejoramiento de la imagen (corrección de nitidez, color, contraste y gamma),
- ruido aditivo y multiplicativo (Gaussiano, uniforme, mosquito),
- filtrado lineal (filtros pasa-bajas, pasa-altas, pasa-banda),
- filtrado no lineal (filtro de mediana y morfológico),
- compresión con pérdida (como JPEG),
- transformaciones afines globales y locales (traslación, rotación, escalamiento, cizallamiento),
- reducción de la imagen (recorte, modificación del histograma),
- composición de la imagen (inserción de logo, composición de la escena),
- cambio de formato (GIF - JPEG),
- conversión D/A y A/D (imprimir y digitalizar, transmisión por televisión analógica),
- inserción de varias marcas de agua,
- ataques de colusión y
- ataques de mosaico.

Las estrategias utilizadas para el diseño de marcas de agua son diversas, pero algunos esquemas han demostrado una mayor robustez contra diferentes ataques, incidentales y accidentales, insertando y/o detectando la marca de agua en dominios discretos como los que se obtienen con la Transformada de Fourier Discreta (DFT, por sus siglas en inglés), Transformada de Cosenos Discreta (DCT, por sus siglas en inglés) o la Transformada Wavelets Discreta (DWT, por sus siglas en inglés) [Cox97, Minzer97, Kundur97, Loo99].

Además de la robustez, existen otros requerimientos dependientes de la aplicación como son la invisibilidad de la marca de agua, la rapidez de inserción/detección, entre otras.

A continuación se describen algunas de las aplicaciones<sup>2</sup>, propuestas en [Kutter00, Cox02], y algunos de sus requerimientos.

### **Protección de derechos de autor**

Consiste en insertar marcas de agua que contengan información sobre el autor o propietario dentro de imágenes digitales. De esta manera se podrían resolver litigios legales relacionados con infracciones a los derechos de autor. Para esta aplicación se requiere una excelente robustez contra una gran cantidad de ataques, accidentales e incidentales. Además, es necesario que los esquemas de este tipo utilicen medidas de seguridad para detectar inserciones no autorizadas en imágenes protegidas, etc.

### **Rastreo de copias**

Suponga que se inserta una marca de agua diferente en cada una de las copias de una determinada imagen, antes de distribuirlas entre un reducido círculo de personas. Si alguna persona redistribuye la imagen sin autorización, es posible rastrear al responsable de la infracción detectando la marca de agua de alguna de las copias ilegales. Puesto que la persona que va a compartir la imagen podría saber de la existencia de la marca de agua en su imagen, este tipo de sistemas deben evitar inserciones no autorizadas, ataques de colusión, etc.

### **Protección de copias**

Algunos sistemas multimedia necesitan algún mecanismo de seguridad para evitar la reproducción de copias no autorizadas. Es viable utilizar marcas de agua para ofrecer esta característica dentro de los mismos dispositivos electrónicos, sobre todo en sistemas cerrados o propietarios. Las marcas de agua, insertadas dentro de los datos multimedia, indican a los reproductores el número de copias que están autorizadas de un determinado volumen. Por ejemplo, las marcas de agua utilizadas en los Discos Versátiles Digitales (DVD), indican

---

<sup>2</sup>Para obtener información sobre aplicaciones enfocadas a resolver problemas en áreas específicas como la medicina y el monitoreo de transmisiones, se recomienda consultar [Anand98, Miaou00, Coatrieux01, Cox02, Bravo03].

a los dispositivos electrónicos si se permite o no la copia de ese volumen [Bloom99]. Generalmente se requiere que este tipo de esquemas sean robustos contra cambios geométricos y de formato, adición de ruido, etc.

### Autenticación de imágenes

El objetivo de esta aplicación es detectar modificaciones en los datos. Consiste en diseñar marcas de agua que se destruyan o modifiquen cuando las imágenes protegidas sufren cualquier tipo de distorsión. Los esquemas diseñados con esta aplicación son conocidos como de *marcas de agua frágiles*.

Algunos autores afirman que algunas aplicaciones requieren marcas de agua que se destruyan con distorsiones que afecten severamente la imagen protegida, pero que sobrevivan a ciertos ataques accidentales como compresión con pérdida, cambio de formato, etc. Los esquemas que se han diseñado con estas características se conocen como de *marcas de agua semi-frágiles*.

## 2.3. Evaluación de los Sistemas de Marcas de Agua

Para evaluar apropiadamente los sistemas de marcas de agua se sugiere que todos los esquemas de marcas de agua se evalúen bajo condiciones equiparables [Petitcolas99].

Para evaluar la degradación causada en las imágenes, debido a la inserción de una marca de agua, se pueden utilizar medidas de distorsión cuantitativas como la Relación Mayor de Señal-a-Ruido (PSNR, por sus siglas en inglés), definida como,

$$\text{PSNR}(f, f_w) = \frac{1}{N_C N_R} 10 \log_{10} \left( \frac{255^2}{\sum_{x,y} (f(x,y) - f_w(x,y))^2} \right), \quad (2.1)$$

donde  $f$  y  $f_w$  son la imagen original y marcada (con 256 niveles de gris), respectivamente, y  $N_C$  y  $N_R$  es el número de renglones y columnas de las imágenes (se asume que ambas tienen el mismo número de columnas y renglones).

El PSNR es una medida en decibelios (dB) que indica la cantidad de distorsión que sufre una señal al agregar ruido, y ha sido utilizada durante mucho tiempo para comparar la distorsión causada por diferentes métodos de compresión de imágenes con pérdida. A

pesar de que el PSNR no es una medida de comparación basada en algún modelo del sistema visual humano, es una medida que ha sido ampliamente aceptada para comparar la distorsión provocada por diferentes esquemas de marcas de agua.

Como respuesta a la necesidad de establecer puntos de comparación para evaluar la robustez de los esquemas de marcas agua, se han propuesto herramientas estándares que aplican diversas distorsiones en las imágenes marcadas. Las herramientas más utilizadas con este propósito son Stirmark [Petitcolas98, Petitcolas00] y Checkmark [Pereira01b], las cuales aplican ataques como: recortes, rotación, escalamiento, filtros de mediana, Gaussianos y de FMLR, distorsiones geométricas aleatorias, eliminación de líneas, compresión con pérdida JPEG y JPEG2000, entre otros.

Los resultados se presentan comúnmente utilizando tablas o gráficas que permitan comparar las respuestas del proceso de detección ante diferentes cantidades de distorsión [Kutter00]. En la Figura 2.2 se puede observar un ejemplo de una gráfica comparativa en donde se muestran resultados hipotéticos de dos sistemas de marcas de agua diferentes. En este ejemplo se asume que la respuesta de los detectores de ambos esquemas es cercana a 1.0 cuando se encuentra la marca de agua. Se puede observar que el sistema 2 es el que presenta mayor robustez a compresión JPEG, pues la respuesta del detector es superior al del sistema 1 en la mayor parte de la gráfica. Así como se realizó esta prueba, se generan gráficas o tablas comparativas para el resto de los ataques que se desean aplicar (adición de ruido, de brillo, etc.) para finalmente evaluar el desempeño global de los sistemas.

Al proponer un esquema de marcas de agua nuevo es importante mencionar la probabilidad de *falsos positivos*, que es cuando se detecta alguna marca de agua en imágenes que no han sido marcadas. Asimismo, es necesario reportar la probabilidad de *falsos negativos*, que ocurren cuando no se detecta la marca de agua en una imagen protegida. Dependiendo de los esquemas de inserción/detección propuestos, en ocasiones no es posible modelar matemáticamente la probabilidad de falsos positivos y falsos negativos. En estos casos, es posible estimar empíricamente una probabilidad realizando una cantidad suficientemente grande de pruebas utilizando imágenes diferentes.

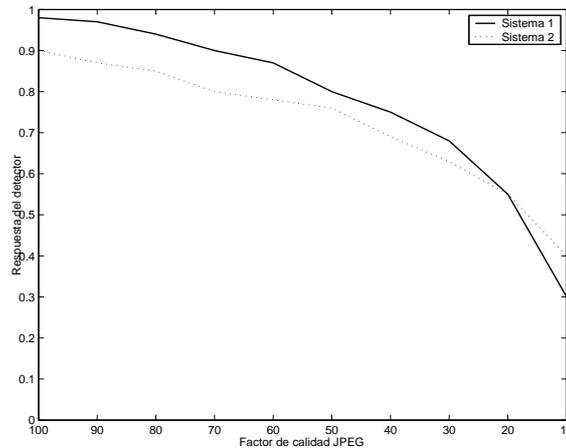


Figura 2.2: Presentación de resultados de dos sistemas diferentes.

## 2.4. Efectos de los Ataques Geométricos en Marcas de Agua

Se han propuesto un gran número de esquemas de marcas de agua que han mostrado robustez ante diversos ataques como compresión con pérdida, adición de ruido, y la aplicación de diferentes filtros [Kundur97, Cox97, Cox02, Anastassopoulos02]. Sin embargo, la mayoría de estos esquemas comúnmente reportan detecciones erróneas cuando se aplican distorsiones geométricas a las imágenes protegidas, especialmente cuando los detectores no tienen acceso a las imágenes originales. En estos casos, las marcas de agua siguen existiendo, pero en localidades que resultan desconocidas para los detectores. A este fenómeno se le conoce en la literatura como *pérdida de sincronización* [Licks03].

A continuación se definen algunas de las distorsiones geométricas más comunes que se utilizan en imágenes digitales. Sin embargo, para conocer el efecto de las distorsiones geométricas en un esquema en particular, se deben analizar los efectos que tienen dichas distorsiones en el dominio de extracción. Por ejemplo, si la detección se realiza en el dominio de Fourier, es necesario estudiar de qué manera se afectan los coeficientes de Fourier de la imagen cuando se aplican distorsiones geométricas en el dominio espacial (ver Sección 3.1).

### 2.4.1. Distorsiones geométricas comunes en imágenes digitales

Algunas distorsiones geométricas como la reflexión, traslación, rotación, escalamiento y cizallamiento, son aplicaciones o transformaciones lineales [deBurgós97] utilizadas comúnmente en imágenes digitales. Suponga una imagen cualquiera  $f(x, y)$ , donde  $0 < x \leq N_C$  y  $0 < y \leq N_R$  representan sus coordenadas y  $N_C$  y  $N_R$  denotan el total de columnas y renglones de la imagen, respectivamente.

$$\text{(Reflexión)} \quad f_f(x, y) = f(N_C - x + 1, N_R - y + 1), \quad (2.2)$$

$$\text{(Traslación)} \quad f_t(x, y) = f(x + x_0, y + y_0) \text{ donde } x_0, y_0 \in \mathcal{R}, \quad (2.3)$$

$$\text{(Rotación)} \quad f_r(x, y) = f(x \cos \theta + y \sin \theta, -x \sin \theta + y \cos \theta) \text{ donde } 0 \leq \theta < 2\pi, \quad (2.4)$$

$$\text{(Escalamiento)} \quad f_e(x, y) = f(x \sigma_1, y \sigma_2) \text{ donde } \sigma_1, \sigma_2 > 0, \quad (2.5)$$

$$\text{(Cizallamiento)} \quad f_c(x, y) = f(x + y \gamma_1, y + x \gamma_2) \text{ donde } \gamma_1, \gamma_2 \in \mathcal{R}. \quad (2.6)$$

A las transformaciones definidas por las ecuaciones (2.2)-(2.6), y a sus posibles composiciones, se les conoce como *transformaciones afines*, y se caracterizan por conservar el paralelismo y el centro de masa de las imágenes<sup>3</sup>. Las *transformaciones de semejanza*, que conservan los ángulos y la proporción de las distancias en las imágenes, son conformadas por el conjunto de transformaciones definidas por las ecuaciones (2.2)-(2.5) (para  $\sigma_1 = \sigma_2$ ), y sus diversas composiciones. Finalmente, a la reflexión, la traslación y la rotación, así como todas sus posibles composiciones, se les conoce como *transformaciones Euclidianas*, y se caracterizan por conservar las distancias dentro de las imágenes.

Existen además las *transformaciones proyectivas*, que se pueden entender como la proyección de una imagen en otro plano, en donde no necesariamente se conserva el paralelismo de las imágenes transformadas.

Otro tipo de distorsiones geométricas importantes para los esquemas de marcas de agua, discutidos en [Delannay01], son las *distorsiones radiales*, que modelan la distorsión de los lentes en la adquisición de imágenes, y las *distorsiones bilineales*, que modifican la forma de una imagen desplazando sus esquinas en cantidades y direcciones aleatorias.

<sup>3</sup>La demostración de las características de las siguientes transformaciones están fuera del alcance de la presente tesis, sin embargo, para mayor información se sugiere consultar [Faugeras01].

En la literatura se utilizan dos conceptos diferentes: los *ataques geométricos globales* y los *ataques geométricos locales* [Licks03]. Un ataque geométrico global implica la utilización del mismo conjunto de parámetros de distorsión en todos los píxeles de una imagen, a diferencia de un ataque geométrico local, en donde se pueden utilizar diferentes parámetros de distorsión en diferentes regiones de una misma imagen. Como es de suponer, el espacio de todos los ataques locales posibles puede ser mucho mayor que el espacio de todos los ataques globales posibles. Por esta razón, frecuentemente se diseñan nuevos ataques geométricos locales para intentar lograr la pérdida de sincronización de los esquemas de marcas de agua [Licks03].

## 2.5. Estrategias Propuestas para Contrarrestar los Ataques geométricos

Los ataques geométricos se han convertido en los “ataques a vencer” por los esquemas de marcas de agua por su enorme diversidad y, en algunos casos, por la poca distorsión que causan a las imágenes protegidas. A continuación se discuten algunos de las estrategias propuestas en la literatura para evitar o restaurar la sincronización en los esquemas de marcas de agua, cuando ésta se pierde debido a ataques geométricos.

Cuando al detector se le proporciona la imagen original, es posible utilizar alguna técnica de registro de imágenes [Brown92] para restaurar la sincronización entre la marca de agua y el detector. Sin embargo, ésta es una estrategia que ha recibido poca atención debido a la limitada aplicación que tienen los esquemas de marcas de agua con detectores no ciegos.

### 2.5.1. Búsqueda exhaustiva

Una estrategia impopular es la utilización de un algoritmo de búsqueda que encuentre de forma exhaustiva los parámetros involucrados en una determinada distorsión. Para lograr una detección aceptable es necesario utilizar incrementos muy pequeños en la búsqueda, lo cual implica un aumento considerable del costo computacional. Para evitar que el cómputo de esta estrategia resulte tan costoso se propone delimitar los intervalos

de búsqueda a rangos muy pequeños, suponiendo que una imagen protegida sólo recibiría ataques geométricos suficientemente pequeños que no afecten demasiado su calidad [Cox02].

### 2.5.2. Patrones de sincronización

La inserción de patrones para sincronizar los esquemas de marcas de agua es una estrategia que ha sido explorada por varios autores [Fleet97, Pereira99a, Pereira99b, Pereira00].

Fleet y Heger [Fleet97] insertan, en el dominio espacial, una señal sinusoidal junto con la marca de agua, lo que produce picos en el dominio de la frecuencia que son utilizados para sincronizar el detector con la marca de agua.

Pereira y Pun [Pereira99a, Pereira99b] proponen insertar, junto con la marca de agua, un patrón de picos en un anillo circular correspondiente a los coeficientes de frecuencias medias de Fourier. El esquema se basa en encontrar los parámetros de cualquier ataque geométrico previo para hacer coincidir los picos del patrón original con el de la imagen protegida. Estos esquemas han demostrado excelente robustez contra transformaciones afines.

En [Pereira00] se inserta un patrón cambiando el espectro de Fourier a coordenadas log-polar y log-log, lo cual permite simplificar la estimación de la rotación, el escalamiento y cambios de dimensión no proporcionales, ya que éstas se vuelven simples traslaciones utilizando ambos dominios. La principal desventaja de este esquema es la degradación que sufren las imágenes debido a la discretización e interpolación necesarias en los dominios log-polar y log-log.

Desafortunadamente, esquemas de este tipo son incapaces de restablecer la sincronización con una imagen marcada cuyo patrón de sincronización ha sido eliminado mediante ataques de colusión [Craver00, Ergün99]. Para contrarrestar este problema, en [Delannay02] se propuso insertar el patrón dependiendo de una llave dependiente de la imagen. No obstante, los patrones conservan su vulnerabilidad a filtros óptimos, como los propuestos en [Herrigel01, Licks03].

Se sabe que la cantidad de energía de una señal que se va a insertar en una imagen está restringida por el requerimiento de invisibilidad de los esquemas de marcas de agua. En

este tipo de esquemas, la energía de inserción se debe compartir entre la marca de agua y el patrón de sincronización, reduciendo así la capacidad de las marcas de agua. El aumento de capacidad de las marcas de agua tendría una repercusión directa en la calidad de las imágenes marcadas, y la disminución de la energía de los patrones de sincronización reduciría la efectividad de los esquemas para detectar marcas de agua en imágenes distorsionadas geoméricamente.

### 2.5.3. Auto-sincronización

Otra estrategia explorada por algunos autores consiste en diseñar marcas de agua cuya auto-correlación genere un patrón de picos, el cual es utilizado por los detectores para invertir distorsiones geométricas.

Kutter [Kutter98] propone un esquema que inserta varias veces la misma marca de agua con ciertos desplazamientos en renglones y columnas. La múltiple inserción de la marca de agua genera cierto patrón de picos al calcular la auto-correlación de la imagen analizada por el detector. Al comparar los picos extraídos con la configuración esperada es posible determinar cualquier transformación afín sufrida por la imagen protegida.

Deguillaume y Voloshynovskiy [Deguillaume02] propusieron utilizar, como marca de agua, una señal periódica que genere una malla uniforme de picos al calcular la magnitud de Fourier o la auto-correlación de la imagen marcada. La malla tiene la forma de dos ejes principales y puntos distribuidos uniformemente a través de toda la malla. El detector utiliza la transformada Hough/Radon para extraer los dos ejes principales y los utiliza para invertir cualquier rotación y cizallamiento sufrido por la imagen. Posteriormente se calculan la distancia entre los puntos de la malla para poder determinar cualquier cambio en la escala y/o en la proporción de la imagen, logrando robustez contra transformaciones afines.

El problema en estos esquemas, al igual que en aquellos basados en patrones de sincronización, es que los patrones obtenidos por la auto-correlación pueden ser removidos por filtros y ataques de colusión, como los propuestos en [Herrigel01, Craver00, Ergün99].

#### 2.5.4. Dominios invariantes

Una de las estrategias más populares en la literatura consiste en insertar las marcas de agua en dominios que son invariantes o semi-invariantes a ciertas distorsiones geométricas.

Algunos esquemas utilizan la bien conocida invariancia a traslación de la magnitud de Fourier [Zelniker93] en los esquemas de marcas de agua [O' Ruanaidh97, Lin01], así como algunas propiedades invariantes a transformaciones geométricas de la Transformada Wavelets Compleja (CWT, por sus siglas en inglés) [Loo00].

En [O' Ruanaidh97] se propuso por primera vez la utilización de la transformada Fourier-Mellin, invariante a RST, en esquemas de marcas de agua. Los autores crean una marca de agua en el dominio de Fourier-Mellin, que después es llevada al dominio espacial para sumarla finalmente a la imagen original. El detector calcula la diferencia entre la imagen original y la marcada, y a la señal resultante se le aplica la transformada de Fourier-Mellin para calcular su correlación con la marca de agua insertada originalmente. El artículo es una referencia obligada por la teoría presentada sobre esta transformada, pero la robustez del esquema contra ataques geométricos no es satisfactoria. La gran desventaja de este esquema es la distorsión ocasionada en las marcas de agua debido a la interpolación y discretización utilizadas en la transformada Fourier-Mellin y su inversa en los procesos de inserción y extracción. La transformada Fourier-Mellin y este esquema en particular se discuten con más detalle en las Secciones 3.1 y 3.2, respectivamente.

Otros esquemas insertan/detectan las marcas de agua en versiones normalizadas de las imágenes [Alghoniemy00, Dong02]. El problema con estos esquemas es que los parámetros de normalización pueden cambiar si la imagen protegida sufre algún recorte [Pei95], aumentando así la probabilidad de detecciones falsas. Para solucionar este problema, Kim *et al.* [Kim02] proponen marcar una región alrededor del centroide invariante de la imagen, utilizando técnicas convencionales de normalización. Los autores argumentan que dicha región difícilmente sufriría recortes. Sin embargo, nada asegura que la región alrededor del centroide de la imagen contenga información de interés para el atacante. Además, el centroide también puede ser calculado por un intruso para aplicar distorsiones que afecten los parámetros de normalización de la región de marcado.

En otra contribución, presentada en [Lin01], se inserta una marca de agua en la magnitud de Fourier, modificando cada coeficiente dependiendo de su contribución con un mapa log-polar. El detector calcula la magnitud de Fourier de la imagen de entrada y crea un mapa log-polar que se proyecta en un vector que resulta invariante a escalamiento, y en donde la rotación se vuelve una simple traslación circular que puede ser encontrada con una simple búsqueda exhaustiva. El esquema demuestra robustez ante algunos ataques de RST. Sin embargo, se pueden tener detecciones erróneas cuando se aplican ataques severos en las imágenes protegidas, pues es inevitable perder información de la marca de agua en los procesos de inserción/extracción, debido a la interpolación y discretización necesarias al calcular el mapa log-polar. Para aumentar la robustez del esquema es necesario incrementar la energía de la marca de agua, lo cual puede afectar significativamente la calidad de las imágenes marcadas. Los mapas log-polar y este esquema se discuten detalladamente en las Secciones 3.1 y 3.3, respectivamente.

### 2.5.5. Extracción de características

Kutter *et al.* [Kutter99] proponen establecer regiones de marcado alrededor de ciertas esquinas de las imágenes, detectadas mediante los cruces por cero de la imagen filtrada por una señal Sombrero Mexicano. A pesar de que sólo se reportan resultados preliminares contra compresión JPEG y no contra ataques geométricos, los autores proponen el término de “esquemas de marcas de agua de segunda generación” para aquellos que extraigan las características específicas de las imágenes para los procesos de inserción y extracción. A partir de entonces se han propuesto varios esquemas de marcas de agua de segunda generación, en donde se sugieren diversas técnicas para la selección de características de las imágenes [Bas02, Feng02, Tang03].

Bas *et al.* [Bas02] insertan la marca de agua en los triángulos creados por un teselado de Delaunay, basado en características invariantes extraídas de las imágenes. Los autores muestran comparaciones en donde el detector de bordes y esquinas Harris [Harris88] muestra un mejor desempeño que el detector Achard-Rouquet [Devars99] y el SUSAN [Smith95]. El esquema muestra robustez ante compresión y algunos ataques geométricos, globales y locales, aplicados con Stirmark 3.1 (ver Sección 2.3).

Feng e Izquierdo [Feng02] proponen insertar la marca de agua utilizando mapas log-polar en regiones seleccionadas alrededor de esquinas robustas. Se propone utilizar mapas log-polar con ángulos uniformes y distancias no uniformes para disminuir la pérdida de información por discretización e interpolación, y un detector de Curvatura de Escala-Espacio (CSS, por sus siglas en inglés) para extraer esquinas robustas. El esquema muestra robustez ante diferentes ataques aplicados con Stirmark 3.1 (ver Sección 2.3).

Tang y Hang [Tang03] extraen esquinas robustas de las imágenes utilizando la interacción de diferentes escalas de la wavelet Sombrero Mexicano (invariante a rotación). Alrededor de cada esquina seleccionada se establece una región circular que contiene dos regiones cuadradas de tamaño  $32 \times 32$ . En cada región circular se inserta la misma marca de agua de 32 bits, distribuida entre sus dos regiones cuadradas. Se calcula la magnitud de Fourier en cada región cuadrada y se normaliza antes de insertar los correspondientes 16 bits de marca de agua. Los resultados muestran que el esquema es robusto a diferentes ataques aplicados con Stirmark 3.1 (ver Sección 2.3).

Los esquemas de marcas de agua basados en extracción de características parecen ser la alternativa más indicada para alcanzar robustez ante ataques geométricos locales. Sin embargo, todos ellos dependen de la precisión del algoritmo de extracción utilizado, pues, si las características seleccionadas por el proceso de detección no son las mismas que fueron marcadas, el resultado es impredecible.



## Capítulo 3

# Revisión de Esquemas

En este capítulo se discuten dos esquemas que insertan y/o extraen las marcas de agua en dominios invariantes o semi-invariantes a RST. En la Sección 3.1 se describen algunas propiedades importantes de la DFT, de los mapas log-polar y del dominio de Fourier-Mellin, que han sido utilizadas para resolver la pérdida de sincronización en los esquemas de marcas de agua [O' Ruanaidh97, Lin01, Feng02, Zheng03]. El algoritmo de la Sección 3.2 fue el primero en utilizar la transformada de Fourier-Mellin en los esquemas de marcas de agua. El esquema descrito en la Sección 3.3 está basado en mapas log-polar y es uno de los que han mostrado mayor robustez a ataques de RST.

### 3.1. Mapas Log-Polar y Transformada de Fourier-Mellin

Comenzaremos esta sección por revisar algunas propiedades importantes de la DFT, que son de importancia para resolver los problemas de sincronización en los esquemas de marcas de agua.

#### 3.1.1. Propiedades de la DFT

Suponga la DFT de una imagen cualquiera,  $f$ , a la cual se le han aplicado cambios geométricos. La manera en que se afectan los coeficientes de Fourier de la imagen con dichas distorsiones se describe a continuación.

### Propiedades traslación

Un desplazamiento en el dominio espacial causa un desplazamiento lineal en el componente de fase [Zelniker93],

$$f(x + x_0, y + y_0) \xleftrightarrow{\mathcal{F}} F(k, l) e^{-j(x_0 k, y_0 l)} . \quad (3.1)$$

Sin embargo, la magnitud de Fourier es invariante a traslación, debido a que  $|e^{-j(x_0 k, y_0 l)}| = 1$ . Puesto que la DFT presupone que  $F$  y  $f$  son periódicas, la traslación que se asume es circular. Por lo tanto, una traslación ordinaria puede representarse como una traslación circular con pérdida de información.

### Propiedades de escalamiento

El escalamiento en el dominio espacial causa un escalamiento inverso en el dominio de la frecuencia.

$$f(\sigma x, \sigma y) \xleftrightarrow{\mathcal{F}} \frac{1}{\sigma} F\left(\frac{k}{\sigma}, \frac{l}{\sigma}\right) . \quad (3.2)$$

### Propiedades de rotación

La rotación de una imagen en el dominio espacial corresponde a una rotación, con el mismo ángulo, en el dominio de la frecuencia.

$$f(x \cos \phi - y \sin \phi, x \sin \phi + y \cos \phi) \xleftrightarrow{\mathcal{F}} F(k \cos \phi - l \sin \phi, k \sin \phi + l \cos \phi) . \quad (3.3)$$

Con las tres propiedades anteriores sabemos entonces, que la magnitud de Fourier es invariante a traslación, que el escalamiento en el tiempo produce un escalamiento inverso en la frecuencia, y que la rotación en el tiempo provoca una rotación, con el mismo ángulo, en el dominio de la frecuencia.

#### 3.1.2. Mapa log-polar

A continuación revisaremos el dominio log-polar que tiene propiedades importantes para resolver los problemas de sincronización en los esquemas de marcas de agua.

Un mapa log-polar está conformado por dos ejes: uno que representan el ángulo, y que denotaremos como  $\theta$ , y otro que representa el logaritmo natural de la distancia de cada píxel respecto del centro de la imagen (origen), y que denotaremos como  $\mu$ . En las dos imágenes superiores de la Figura 3.1 se puede apreciar la imagen de Lena representada en coordenadas cartesianas (izquierda) y en coordenadas log-polar (derecha). Al cambio de coordenadas cartesianas a log-polar se le conoce como Proyección Log-Polar (LPM, por sus siglas en inglés).

En la Figura 3.1 se muestran dos de las propiedades más importantes de los mapas log-polar. Por un lado, la rotación en coordenadas cartesianas causa una rotación circular en el mapa log-polar (observe la traslación circular vertical entre los dos primeros mapas). Por otro lado, el escalamiento en coordenadas cartesianas causa una traslación en el mapa log-polar (observe las diferencias en el margen derecho entre el primero y el último mapa).

Para explicar el proceso de LPM consideremos la representación log-polar de un punto  $(x, y)$  de una imagen,

$$x = e^\mu \cos \theta + \frac{N_C}{2} \quad \text{y} \quad y = e^\mu \sin \theta + \frac{N_R}{2}, \quad (3.4)$$

donde  $N_C$  y  $N_R$  es el total de columnas y renglones de la imagen, respectivamente. Note que en la ecuación (3.4) se considera el centro de la imagen como origen, tal como se mostró en la Figura 3.1.

Para obtener un mapa log-polar, con un total de  $M_R$  renglones y  $M_C$  columnas, es necesario discretizar los parámetros mediante,

$$\theta = \frac{2\pi i}{M_R} \quad \text{y} \quad \mu = \frac{j \ln \mu_{\text{máx}}}{M_C}, \quad (3.5)$$

donde  $0 < i \leq M_R$  y  $0 < j \leq M_C$  son índices enteros del mapa log-polar y  $\mu_{\text{máx}} = \frac{1}{2} \sqrt{N_R^2 + N_C^2}$  es la distancia máxima a la que puede estar un píxel respecto del origen en su representación cartesiana. Los parámetros del mapa,  $(\theta, \mu)$ , se sustituyen en (3.4) para obtener las coordenadas cartesianas de la imagen y calcular la intensidad del píxel que le corresponde, utilizando algún método de interpolación.

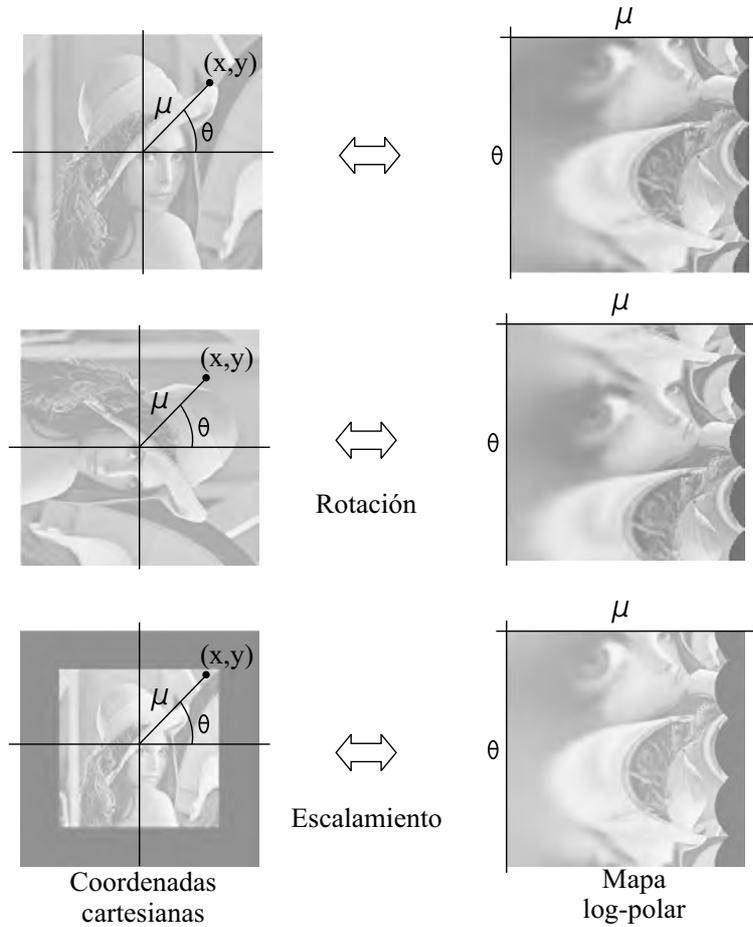


Figura 3.1: Imágenes en coordenadas cartesianas y log-polar.

En este sistema de coordenadas log-polar, el escalamiento de una imagen,  $f(\sigma x, \sigma y)$  se convierte en una traslación dada por,

$$f(\mu + \ln \sigma, \theta) . \quad (3.6)$$

Asimismo, la rotación de una imagen,  $f(x \cos \phi - y \sin \phi, x \sin \phi + y \cos \phi)$ , se convierte en una traslación dada por,

$$f(\mu, \theta + \phi) . \quad (3.7)$$

Note que las propiedades que se describen en las ecuaciones (3.6) y (3.7) son las mismas que se aprecian en la Figura 3.1.

Finalmente, describiremos el procedimiento para cambiar la representación log-polar de la imagen a una representación en coordenadas cartesianas. Para ello, es necesario calcular la intensidad de cada pixel de la imagen inversa, interpolando los píxeles vecinos a las coordenadas del mapa, las cuales se obtienen al sustituir cada punto  $(x, y)$  en,

$$\theta = \left( \frac{\text{atan2}(x, y)}{\pi} + 1 \right) \frac{N_R}{2} \quad \text{y} \quad \mu = \frac{\ln \sqrt{x^2 + y^2}}{\ln \mu_{\text{máx}}} N_C, \quad (3.8)$$

donde  $-\frac{N_C}{2} \leq x < \frac{N_C}{2}$  y  $-\frac{N_R}{2} \leq y < \frac{N_R}{2}$  son los índices de las coordenadas cartesianas. A este proceso se le conoce como Proyección Inversa Log-Polar (ILPM, por sus siglas en inglés).

### 3.1.3. Transformada Fourier-Mellin

En las dos secciones anteriores se discutió el dominio de Fourier, cuya magnitud es invariante a traslación, y el dominio log-polar, en donde el escalamiento y la rotación se transforman en simples traslaciones. Utilizando estos dos dominios es posible llevar a la imagen a un dominio invariante a RST, siguiendo el procedimiento que se describe a continuación:

1. Se calcula la magnitud de Fourier de la imagen,
2. Se calcula el mapa log-polar de la magnitud de Fourier,
3. Se calcula la magnitud de Fourier del mapa log-polar.

Con el primer paso se llega a un dominio invariante a traslación. En este nivel, cualquier escalamiento en el dominio espacial produce un escalamiento inverso en magnitud de Fourier, y cualquier rotación en el dominio espacial produce una rotación, con el mismo ángulo, en la magnitud de Fourier. Con el segundo paso, cualquier escalamiento y rotación de la magnitud de Fourier se transforman en simples traslaciones, que se resuelven en el tercer paso, al calcular nuevamente la magnitud de Fourier del mapa log-polar. Este proceso es equivalente a aplicar la transformada de Fourier-Mellin [O' Ruanaidh97] definida como,

$$F_M(k, l) = \int_{-\infty}^{\infty} \int_0^{2\pi} f(e^\mu \cos \theta, e^\mu \sin \theta) e^{i(k\mu + l\theta)} d\mu d\theta. \quad (3.9)$$

La transformada de Fourier-Mellin inversa se realiza calculando la Transformada Discreta de Fourier Inversa (IDFT, por sus siglas en inglés), seguida del ILPM y la IDFT.

### 3.1.4. Discusión sobre los mapas log-polar

Los procesos de discretización e interpolación que se requieren en los procesos de LPM e ILPM causan pérdidas significativas de la información. Para mostrar este efecto se utilizó la imagen de Lena de tamaño  $256 \times 256$ , que se muestra Figura 3.2(a), con la cual se formaron tres mapas log-polar de diferentes dimensiones ( $128 \times 128$ ,  $256 \times 256$  y  $512 \times 512$ ). Posteriormente se aplicó el proceso de ILPM a los tres mapas para obtener tres imágenes inversas con las mismas dimensiones que la imagen original ( $256 \times 256$ ).

En la Figura 3.2(b) se muestra la imagen que se obtuvo al aplicar el proceso de ILPM en el mapa log-polar de  $128 \times 128$ . En esta imagen se percibe una degradación en su calidad, que se acentúa en las regiones más alejadas del centro de la imagen. Esta degradación también se puede apreciar en la Figura 3.2(e), en donde se ilustran las diferencias entre las imágenes de las Figuras 3.2(a) y 3.2(b). En la Figura 3.2(c) se muestra la imagen inversa del mapa log-polar de  $256 \times 256$ . Al igual que en el caso anterior, se observa pérdida de calidad en las regiones lejanas al centro de la imagen. Este mismo fenómeno se aprecia también en la imagen de diferencias de la Figura 3.2(f). En la imagen inversa del mapa log-polar de  $512 \times 512$ , de la Figura 3.2(d), se perciben menos distorsiones, pero la pérdida de información se sigue observando en la imagen de diferencias de la Figura 3.2(g).

En estos resultados es evidente que mientras más grande es el mapa log-polar, es mejor la calidad en la imagen resultado del proceso de ILPM, pues la discretización necesaria durante el proceso de LPM es más fina. Además, observe que las diferencias más grandes se concentran en los bordes de las imágenes. Este efecto es resultado de la interpolación necesaria durante los procesos de LPM e ILPM, que actúa en la imagen, de manera similar al de un *filtro pasa-bajas*, afectando las altas frecuencias (los bordes) de las imágenes.

Este experimento nos permite concluir que las marcas de agua insertadas en dominios dependientes de los procesos de LPM e ILPM sufren distorsiones que pueden afectar su detección. Por esta razón, en esta tesis se propone una estrategia que no se basa en este tipo de dominios para restaurar la sincronización de los esquemas de marcas de agua.

## 3.2. Esquema Basado en Fourier-Mellin

En el esquema que se describe a continuación, propuesto por O’Ruanaidh y Pun [O’ Ruanaidh97], se propuso por primera vez la utilización de la transformada de Fourier-Mellin como estrategia para soportar ataques de RST.

### 3.2.1. Proceso de inserción

El proceso de inserción se describe en el Algoritmo 1 y se ilustra en la Figura 3.3(a). Primero se crea una marca de agua pseudo-aleatoria de la que se obtiene primero la IDFT. En este primer paso se sugiere utilizar un componente de fase aleatorio para lograr una distribución de la magnitud de Fourier razonablemente plana, y mejorar el desempeño del proceso de ILPM, que se aplica a continuación. Posteriormente se obtiene la IDFT de la señal resultante, utilizando la fase de la imagen que se va a marcar. Finalmente, se suma la señal a la imagen original para obtener la imagen marcada.

Observe que en este esquema de inserción se utiliza el proceso de ILPM en la imagen, con lo cual se pretende mantener la calidad de la imagen marcada.

### 3.2.2. Proceso de detección

El proceso de detección mostrado en el Algoritmo 2 e ilustrado en la Figura 3.3(b) requiere sustraer la imagen original (sin marcar) de la imagen marcada, calcular la DFT de la imagen resultante, obtener su magnitud de Fourier y calcular con ella un mapa log-polar. Posteriormente, se vuelve a calcular la magnitud de Fourier de la señal, y en este dominio, idealmente invariante a RST, se calcula la correlación entre la marca de agua insertada originalmente y la extraída.

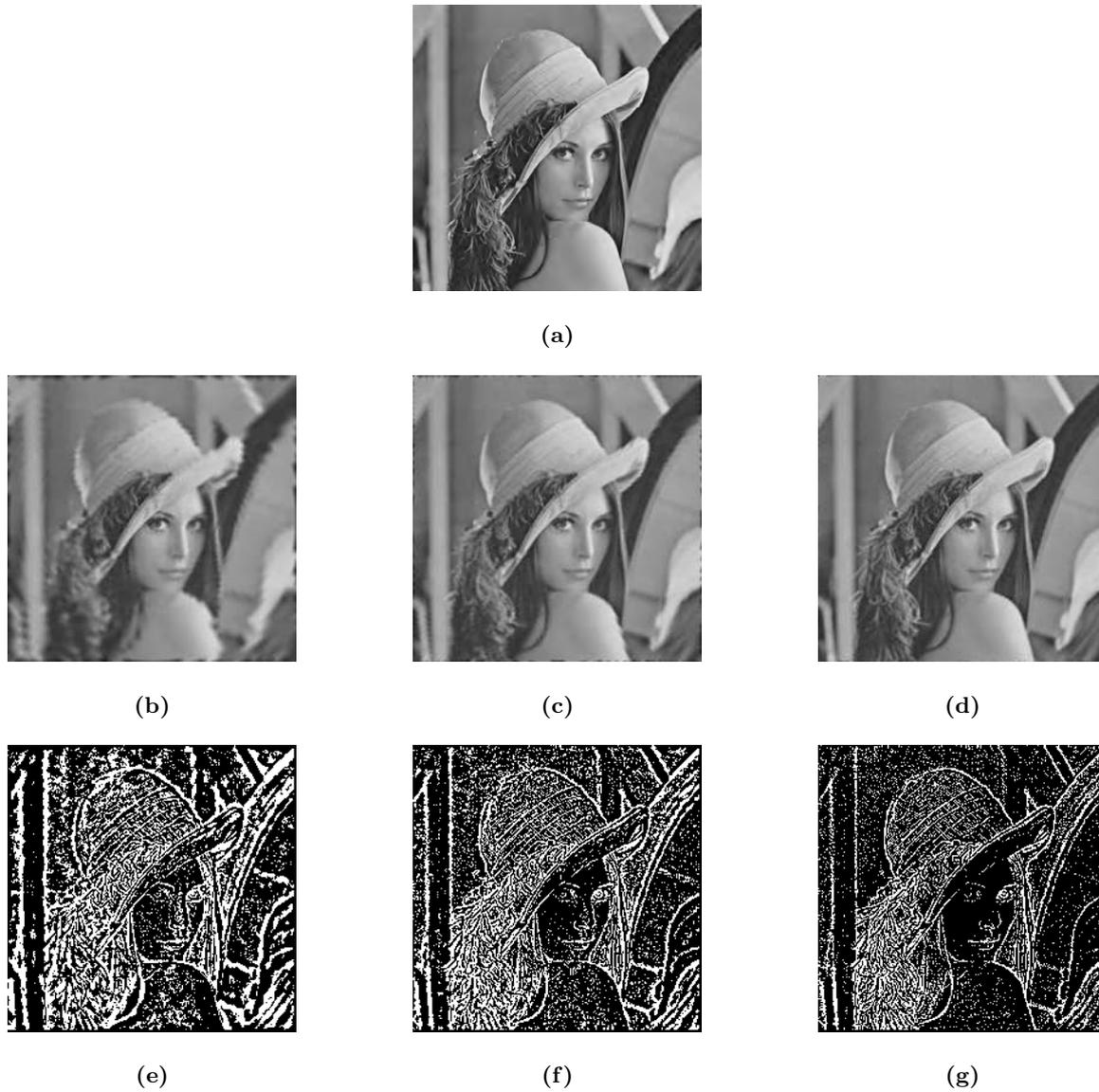


Figura 3.2: Distorsiones causadas por los procesos de LPM e ILPM. (a) Imagen original de tamaño  $256 \times 256$ . (b) y (e) Inversa del mapa log-polar de  $128 \times 128$ , y sus diferencias respecto a la imagen original. (c) y (f) Inversa del mapa log-polar de  $256 \times 256$ , y sus diferencias respecto a la imagen original. (d) y (g) Inversa del mapa log-polar de  $512 \times 512$ , y sus diferencias respecto a la imagen original.

### 3.2.3. Discusión del esquema

Se sabe que la interpolación y discretización que requieren los procesos de LPM e ILPM implican cierta pérdida de información (ver Sección 3.1.4). El esquema descrito en esta sección utiliza el proceso de ILPM en la inserción y el proceso de LPM en la detección. El deterioro causado en las marcas de agua puede provocar detecciones erróneas, aún sin haber recibido ningún ataque. El esquema tiene un fundamento interesante, basado en la utilización de la transformada Fourier-Mellin que es invariante a RST en señales continuas, pero que sufre de serias complicaciones numéricas al ser utilizada en señales discretas.

---

#### Algoritmo 1 Proceso de inserción de Ruanaidh

---

```

ALGINSRUANAIDH(rImg, mMarcaFM)
1  fMarcaFM ← GENERADORDENUMALEATORIOS()
2  [rMarcaFM, iMarcaFM] ← CALCULAREALIMAG(mMarcaFM, fMarcaFM)
3  [rMarcaLPM, iMarcaLPM] ← FFTINVERSA(rMarcaFM, iMarcaFM)
4  [mMarcaLPM, fMarcaLPM] ← CALCULAMAGFASE(rMarcaLPM, iMarcaLPM)
5  mMarcaFFT ← LPMINVERSA(mMarcaLPM)
6  iImg ← LLENACEROS()
7  [rImgFFT, iImgFFT] ← FFT(rImg, iImg)
8  [mImgFFT, fImgFFT] ← CALCULAMAGFASE(rImgFFT, iImgFFT)
9  [rMarcaFFT, iMarcaFFT] ← CALCULAREALIMAG(mMarcaFFT, fImgFFT)
10 [rMarca, iMarca] ← FFTINVERSA(rMarcaFFT, iMarcaFFT)
11 rMarcada = SUMAIMAGENES(rImg, rMarca)
12 regresar rMarcada

```

---

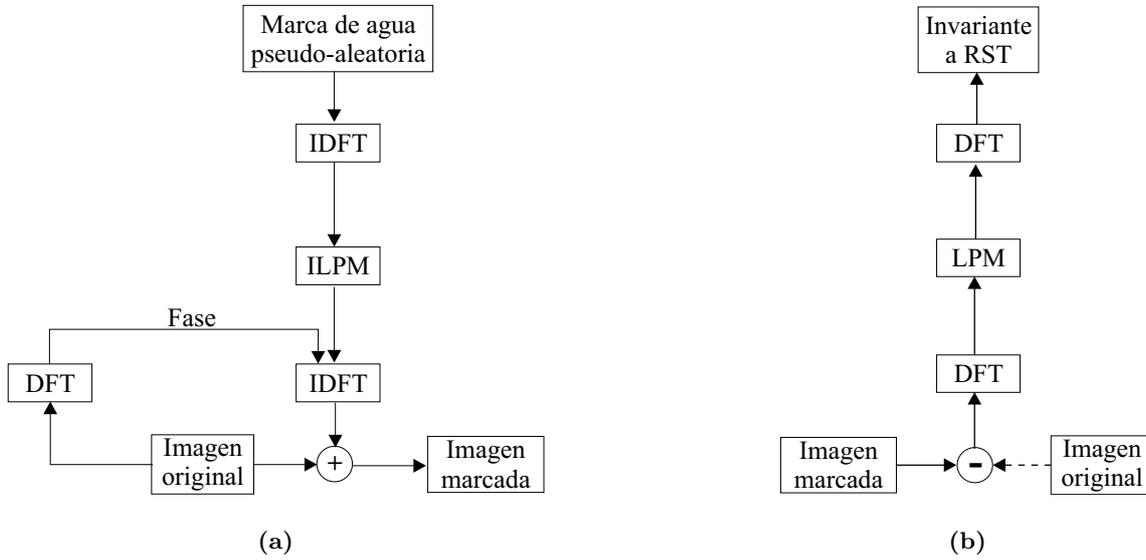


Figura 3.3: Esquema de O'Ruanaidh basado en Fourier-Mellin. (a) Esquema de inserción. (b) Esquema de detección.

---

**Algoritmo 2** Proceso de detección de Ruanaidh

---

```

ALGDETRUANAIHD(rImg, rMarcada, marcaBuscada)
1  rMarca ← CALCULADIFERENCIA(rImg, rMarcada)
2  iMarca ← LLENACEROS()
3  [rMarcaFFT, iMarcaFFT] ← FFT(rMarca, iMarca)
4  rMarcaLPM ← LPM(rMarcaFFT)
5  iMarcaLPM ← LPM(iMarcaFFT)
6  [rMarcaFM, iMarcaFM] ← FFT(rMarcaLPM, iMarcaLPM)
7  [mMarcaFM, fMarcaFM] ← CALCULAMAGFASE(rMarcaFM, iMarcaFM)
8  corr ← CALCULACORRELACION(mMarcaFM, marcaBuscada)
9  regresar corr

```

---

### 3.3. Esquema de Lin Basado en LPM

El esquema que se describe a continuación fue propuesto por Lin *et al.* [Lin01] como alternativa para superar los problemas encontrados en el esquema de O'Ruanaidh. Es robusto a RST y otros ataques más como compresión con pérdida y algunos filtros.

#### 3.3.1. Descripción general del esquema

Considere la magnitud de Fourier de una imagen  $f(x, y)$ ,

$$f(x, y) \xleftrightarrow{\mathcal{F}} |F(k, l)| . \quad (3.10)$$

Si cambiamos la magnitud de Fourier a un sistema de coordenadas log-polar,  $|F(\mu, \theta)|$ , y aplicamos rotación, escalamiento y traslación a la imagen  $f(x, y)$ , se tiene,

$$f(\sigma(x \cos \phi + y \sin \phi) - x_0, \sigma(-x \sin \phi + y \cos \phi) - y_0) \xleftrightarrow{\mathcal{F}} |\sigma|^{-2} |F(\mu - \ln \sigma, \theta - \phi)| , \quad (3.11)$$

donde los parámetros de rotación, escalamiento y traslación son  $\phi$ ,  $\sigma$  y  $(x_0, y_0)$ , respectivamente. Note que la magnitud de Fourier no depende de los parámetros de traslación.

Puesto que el algoritmo de detección utiliza la correlación normalizada, que es invariante a escalamiento, no es importante el escalamiento, por  $|\sigma|^{-2}$ , que sufre la amplitud del espectro log-polar en la ecuación (3.11).

Se denota  $g(\theta)$  como una proyección de  $|F(\mu, \theta)|$  a 1-D, tal que,

$$g(\theta) = \sum_j \ln |F(\mu_j, \theta)| , \quad (3.12)$$

donde, solamente se calcula  $g(\theta)$  para  $\theta \in [0^\circ \dots 180^\circ]$ , debido a la simetría del espectro de las imágenes reales.

Sumando las dos mitades de  $g(\theta)$ , se obtiene el vector,

$$g_1(\theta') = g(\theta') + g(\theta' + 90^\circ) , \quad (3.13)$$

con  $\theta' \in [0^\circ \dots 90^\circ)$ , que es invariante a traslación y escalamiento. Las rotaciones de la imagen  $f$  causan un desplazamiento circular de los valores de  $g_1(\theta')$ . Si  $\theta'$  se calcula redondeando los valores al grado entero más cercano sólo se tendrán 90 traslaciones discretas, y es posible realizar búsquedas exhaustivas que no resultarían costosas.

### 3.3.2. Proceso de inserción

La marca de agua a insertar,  $w$ , es un vector pseudoaleatorio de longitud  $N_w$ . La longitud de la marca de agua sugerida por los autores es de 90, puesto que se replica la marca de agua cada  $90^\circ$  en el mapa log-polar como se explica a continuación.

Teniendo como entrada una imagen original  $f(x, y)$ , se inicia el proceso calculando el logaritmo natural de la magnitud de Fourier,  $\ln |F(k, l)|$ , que sabemos es simétrica, y se traslada su origen al centro de la imagen.

Se calcula a continuación el mapa log-polar  $F(\mu, \theta)$  de  $\ln |F(k, l)|$ , el cual resulta en una matriz de  $M_R$  renglones por  $M_C$  columnas, en donde cada renglón representa un valor diferente de  $\theta$ , y cada columna representa un valor diferente de  $\mu$ . Se extrae el vector  $g_1(\theta')$  como se indica en la ecuación (3.13), para  $N_w$  valores de  $\theta$ , distribuidos entre  $0^\circ$  y  $90^\circ$ .

Al calcular el mapa log-polar, la mayoría de los coeficientes no caen en coordenadas enteras y se requiere algún método de interpolación para calcularlos. Utilizando *interpolación bilineal* se conocen los coeficientes ponderados  $\lambda_1 \ln |F(k_1, l_1)|$ ,  $\lambda_2 \ln |F(k_2, l_2)|$ ,  $\lambda_3 \ln |F(k_3, l_3)|$  y  $\lambda_4 \ln |F(k_4, l_4)|$  (donde  $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 1$ ) que contribuyeron a cada coeficiente del mapa log-polar  $F(\mu_i, \theta_j)$ . Manteniendo esta relación, se puede distribuir el elemento de la marca  $w(\theta_j)$  entre los coeficientes contribuyentes, ayudados de sus respectivos pesos  $\lambda_1 \dots \lambda_4$ , de manera que al calcular de nuevo el mapa log polar (en el proceso de detección), se pueda extraer una buena aproximación  $\bar{w} \approx w$ . Considerando lo anterior, se contemplaron los siguientes casos para la inserción de la marca de agua<sup>1</sup>:

- Si el coeficiente  $\ln |F(k, l)|$  no hizo contribuciones al mapa log-polar, no es necesario marcarlo, se calcula entonces,

<sup>1</sup>El algoritmo original sólo contempla el tercer caso.

$$\ln |F_w(k, l)| = \ln |F_w(m_k + (m_k - k), m_l + (m_l - l))| = \ln |F(k, l)| . \quad (3.14)$$

- Si el coeficiente  $\ln |F(k, l)|$  contribuyó para un solo coeficiente del mapa log-polar, supongamos que a  $F(\mu_i, \theta_j)$  (para  $0^\circ \leq \theta_j < 90^\circ$ ), ponderado con  $\lambda$ , entonces,

$$\ln |F_w(k, l)| = \ln |F_w(m_k + (m_k - k), m_l + (m_l - l))| = \ln |F(k, l)| + \lambda w(\theta_j) . \quad (3.15)$$

- Si un determinado coeficiente  $\ln |F(k, l)|$  contribuyó para más de un coeficiente del mapa log polar, supongamos que  $F(\mu_1, \theta_1)$ ,  $F(\mu_2, \theta_2)$ ,  $F(\mu_3, \theta_3)$  (para  $0^\circ \leq \theta_1, \theta_2, \theta_3 < 90^\circ$ ), ponderados con  $\lambda_1, \lambda_2$  y  $\lambda_3$  respectivamente, entonces

$$\ln |F_w(k, l)| = \ln |F(k, l)| + \frac{\lambda_1 w(\theta_1) + \lambda_2 w(\theta_2) + \lambda_3 w(\theta_3)}{\lambda_1 + \lambda_2 + \lambda_3} , \quad (3.16)$$

y

$$\ln |F_w(m_k + (m_k - k), m_l + (m_l - l))| = \ln |F_w(k, l)| ,$$

donde  $\ln |F_w(k, l)|$  es el logaritmo de la magnitud de la imagen marcada y  $(m_k, m_l)$  denotan las coordenadas del centro del arreglo. Observe que las tres ecuaciones anteriores contemplan la preservación de la simetría del espectro de Fourier. Los ángulos ortogonales se deben marcar con la misma información de la marca de agua, es decir, tanto los coeficientes que contribuyen para el coeficiente  $F(\mu_i, \theta_j)$  como los coeficientes que contribuyeron para el coeficiente  $F(\mu_i, \theta_j + 90^\circ)$  (para  $0^\circ \leq \theta_j < 90^\circ$ ) del mapa log-polar, se van a marcar con  $w(\theta_j)$ . De esta manera se logra una mejor robustez, puesto que se replica la información en diferentes partes del espectro. Otra razón que se menciona en [Lin01], es que la magnitud de Fourier de algunas imágenes contienen mayor energía en ciertas direcciones ortogonales.

Una vez obtenido el logaritmo del espectro marcado,  $\ln |F_w(k, l)|$ , se obtiene la magnitud calculando  $e^{\ln |F_w(k, l)|} = |F_w(k, l)|$  para cada coeficiente, y se traslada el origen del espectro al origen de la imagen. Finalmente, se obtiene la imagen marcada  $f_w(x, y)$

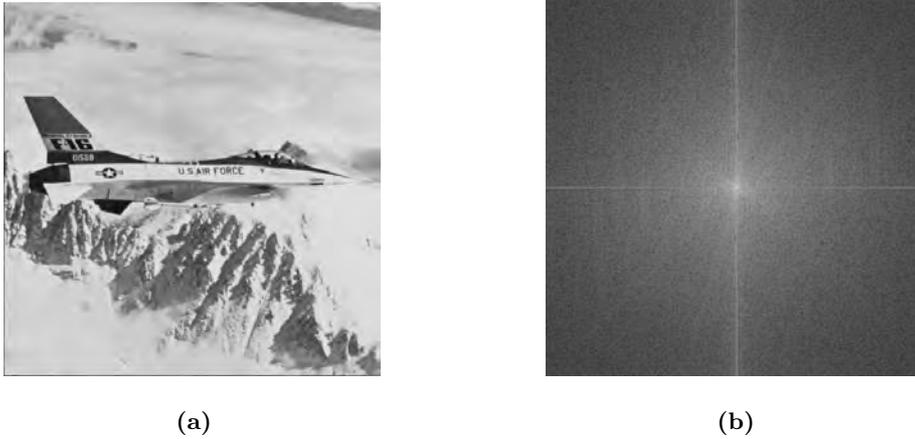


Figura 3.4: Espectro de Fourier de una imagen real. (a) Imagen original. (b) Logaritmo del espectro de Fourier.

calculando la parte real de la IDFT utilizando la fase de la imagen sin marcar; la parte imaginaria se desecha.

Las siguientes son algunas consideraciones se deben tener en cuenta en el algoritmo de inserción:

- La respuesta del detector se mejora modificando el proceso de inserción, como se propone en los esquemas de *inserción informada* propuestos en [Cox02], en los cuales se define una función de mezclado  $mix(g_1, w)$  que encuentra un vector  $g'_1(\theta)$  lo suficientemente parecido a  $g_1(\theta)$  para mantener una menor distorsión, pero suficientemente cerca de  $w(\theta)$  para lograr un coeficiente de correlación mayor que un determinado umbral  $\tau$ . En este caso, se inserta el vector  $w_m(\theta) = g'_1(\theta) - g(\theta)$  en lugar de  $w(\theta)$ .
- Al calcular la DFT se supone que la imagen está repitiéndose infinitamente, lo cual causa generalmente cambios grandes en las orillas de las imágenes, provocando coeficientes con valores grandes en forma de cruz en el centro de la magnitud de Fourier, como se aprecia en la Figura 3.4(b). En [Lin01] se menciona que el artefacto en forma de cruz se comporta de manera diferente al aplicar rotación con y sin pérdida. Por esta razón, los autores proponen no marcar las magnitudes mayores del espectro ni sus coeficientes vecinos, elegidos mediante un umbral.

En el Algoritmo 3 se describen los pasos a seguir durante el proceso de inserción. Observe que la función  $LPM()$  genera el mapa log-polar y una lista de *contribuciones* de cada uno de los coeficientes con el mapa, la cual es utilizada en la función  $esparceMarca()$  para modificar la magnitud de Fourier de la imagen.

---

**Algoritmo 3** Proceso de inserción de Lin
 

---

ALGINSLIN( $rImg, marca1D$ )

- 1  $iImg \leftarrow LLENACEROS()$
  - 2  $[rImgFFT, iImgFFT] \leftarrow FFT(rImg, iImg)$
  - 3  $[mImgFFT, fImgFFT] \leftarrow CALCULAMAGFASE(rImgFFT, iImgFFT)$
  - 4  $[contribuciones, mImgLPM] \leftarrow LPM(mImgFFT)$
  - 5  $g \leftarrow SUMAESCALAS(mImgLPM)$
  - 6  $g1 \leftarrow CALCULAG1(g)$
  - 7  $marca1D_m \leftarrow MIX(marca1D, g1)$
  - 8  $mMarcadaFFT \leftarrow ESPARCEMARCA(mImgLPM, marca1D_m)$
  - 9  $[rMarcadaFFT, iMarcadaFFT] \leftarrow CALCULARREALIMAG(mMarcadaFFT, fImgFFT)$
  - 10  $[rMarcada, iMarcada] \leftarrow FFTINVERSA(rMarcadaFFT, iMarcadaFFT)$
  - 11 **regresar**  $rMarcada$
- 

### 3.3.3. Proceso de detección

Para determinar si la marca de agua está presente, se calcula el mapa log-polar del logaritmo natural de la magnitud de Fourier de la imagen de entrada y se extrae el vector  $g_1(\theta)$ , para  $N_w$  valores de  $\theta$  distribuidos entre  $0^\circ$  y  $90^\circ$ .

Se calcula la correlación normalizada,  $C_n$ , entre el vector  $g_1$  y el vector de la marca de agua insertada  $w$ , como,

$$C_n = \frac{w^T g_1}{\sqrt{(w^T w)(g_1^T g_1)}}. \quad (3.17)$$

El detector reporta la presencia de la marca de agua buscada, sólo si  $C_n$  es mayor que un determinado umbral  $\tau$ .

En [Depovere98] se muestra que se pueden lograr resultados óptimos usando correlación como método de detección en canales de Ruido Blanco Aditivo Gaussiano (AWGN, por sus siglas en inglés). Sin embargo, el vector extraído,  $g_1$ , difícilmente se comportará como ruido Gaussiano, puesto que existe cierta correlación entre los elementos del mapa log-polar. En este caso, los autores proponen utilizar un filtro, conocido por su nombre en inglés como *whitening filter*, en el proceso de detección para eliminar la correlación existente entre los coeficientes de  $g_1$ . Este filtro se aplica tanto en el descriptor  $g_1$  como en la marca de agua buscada  $w$  antes de calcular la correlación entre ambas señales.

El Algoritmo 4 muestra los pasos necesarios para el proceso de detección. Los primeros seis pasos son los mismos que el proceso de inserción, y el resto del algoritmo consiste en la aplicación del filtro para mejorar la detección y el cálculo de la correlación.

### 3.3.4. Experimento

En este experimento se insertó una marca de agua de longitud 90 en la imagen de la Figura 3.5(a). La marca de agua utilizada se generó de forma pseudoaleatoria con una distribución Gaussiana con media cero y varianza unitaria. Para generar la marca de agua se utilizó una semilla  $s = 100$  como valor de arranque del generador de números pseudoaleatorios. Se evitó marcar los coeficientes dentro de una ventana de longitud 5 alrededor de los coeficientes mayores, y se utilizó un filtro de diferencias para mejorar la respuesta del proceso de detección. La prueba consiste en graficar la correlación que se obtiene al detectar 500 marcas de agua diferentes, generadas con semillas  $s = 0, 1, \dots, 499$ , en la imagen marcada distorsionada y sin distorsionar. Se espera que el valor de la correlación obtenida con la marca de agua generada con la semilla  $s = 100$  sea suficientemente mayor que con el resto de las marcas.

**Algoritmo 4** Proceso de detección de Lin

---

```

ALGDETLIN(rImg, marca1DBuscada)
1  iImg ← LLENACEROS()
2  [rImgFFT, iImgFFT] ← FFT(rImg, iImg)
3  [mImgFFT, fImgFFT] ← CALCULAMAGFASE(rImgFFT, iImgFFT)
4  [mImgLPM] ← LPM(mImgFFT)
5  g ← SUMAESCALAS(mImgLPM)
6  g1 ← CALCULAG1(g)
7  g1w ← whiteningFilter(g1)
8  marca1DBuscadaw ← whiteningFilter(marca1DBuscada)
9  corr ← calculaCorrelacion(g1w, marca1DBuscadaw)
10 regresar corr

```

---

La imagen marcada y sin distorsión, se muestra en la Figura 3.5(b) y una gráfica que ilustra la correlación obtenida con las 500 marcas de agua diferentes se puede observar en la Figura 3.5(c). En esta última se puede apreciar un impulso cercano a 0.9 en la correlación detectada con la marca de agua generada con  $s = 100$ , que es suficientemente mayor al que se obtiene con las otras marcas.

Para las siguientes pruebas se aplicó una transformación simple a la imagen marcada, antes de medir la correlación obtenida con las 500 marcas de agua diferentes. La imagen rotada  $45^\circ$  se muestra en la Figura 3.6(a), la imagen escalada con un factor de 1.5 se muestra en la Figura 3.6(c) y la imagen trasladada 50 píxeles dirección horizontal y vertical se muestra en la Figura 3.6(e). En las gráficas de las tres pruebas (Figuras 3.6(b), 3.6(d) y 3.6(f), respectivamente) se puede apreciar un impulso mayor en la correlación detectada con la marca de agua original, generada con la semilla  $s = 100$ .

Finalmente se aplicaron *ataques geométricos compuestos*, que consisten en la aplicación de dos o más transformaciones geométricas, a la imagen marcada, antes de graficar la

correlación detectada con las 500 marcas de agua diferentes. En la Figura 3.7(a) se muestra la imagen rotada  $20^\circ$  y trasladada 50 píxeles en dirección horizontal. En la gráfica de la Figura 3.7(b) se puede observar que la correlación detectada en la marca de agua generada con  $s = 100$  es suficientemente mayor que el resto de las marcas. En la Figura 3.7(c) se muestra la imagen rotada  $25.5^\circ$ , escalada con factor 1.2 y trasladada 50 píxeles en dirección horizontal y vertical. En la gráfica de la Figura 3.7(d), se observa un impulso de 0.4 en la marca de agua generada con  $s = 100$  que es ligeramente mayor al que se obtiene con el resto de las marcas. En la Figura 3.7(e) se muestra la imagen rotada  $10.5^\circ$ , escalada con un factor de 0.7 y trasladada 100 píxeles en dirección horizontal y vertical. En contraste con el resto de las pruebas, en la gráfica de la Figura 3.7(f) se puede observar que la correlación detectada con la marca de agua generada con  $s = 100$  es menor que la detectada en otras marcas de agua.

### 3.3.5. Discusión del esquema

Las primeras cuatro pruebas muestran que el esquema es robusto a ataques geométricos simples y algunos ataques geométricos compuestos. Sin embargo, en los resultados de las últimas dos pruebas se detectó vulnerabilidad del esquema a distorsiones severas causadas por ciertos ataques geométricos compuestos.

Analizando el esquema sabemos que parte de las marcas de agua se pierde al ser esparcidas sobre los coeficientes de la magnitud de Fourier durante el proceso de inserción, y otra parte se pierde en el proceso de LPM en la detección, puesto que éste actúa como filtro pasa-bajas (ver Sección 3.1). Esta pérdida de información provoca que las marcas de agua sean vulnerables a ciertos ataques geométricos que agregan aún más distorsión a las imágenes, como sucedió en las últimas dos pruebas.

La robustez del esquema se puede mejorar utilizando marcas de agua con mayor peso, pero esta medida afectaría significativamente la calidad de las imágenes marcadas.

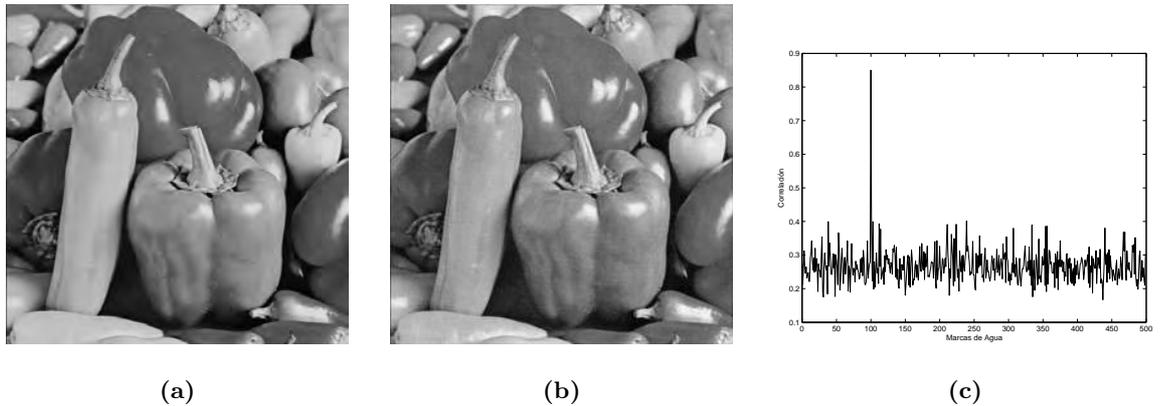


Figura 3.5: Imagen marcada y la correlación obtenida al probar con 500 marcas de agua diferentes. (a) Imagen original de tamaño  $512 \times 512$ . (b) Imagen marcada. (c) Respuesta del detector.

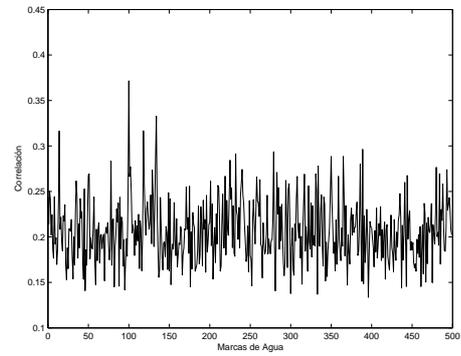
### 3.4. Conclusiones del Capítulo

De lo analizado en este capítulo se puede concluir lo siguiente:

- Los procesos de LPM e ILPM afectan a las señales actuando como filtros pasa-bajas, debido a la discretización y los métodos de interpolación que requieren.
- La transformada de Fourier-Mellin es una transformada invariante a RST en señales continuas, pero en señales discretas se tienen problemas numéricos causados por los procesos de LPM e ILPM.
- Los esquemas basados en LPM pueden causar errores en la detección de las marcas de agua debido a la distorsión ocasionada en los procesos de inserción y detección.



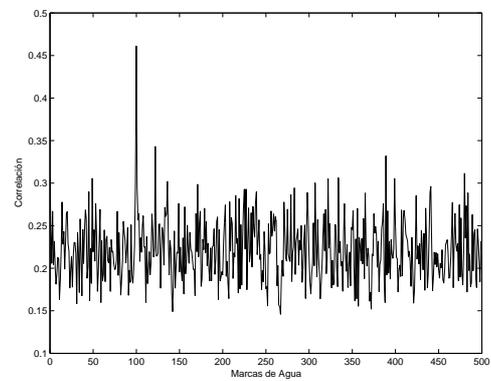
(a)



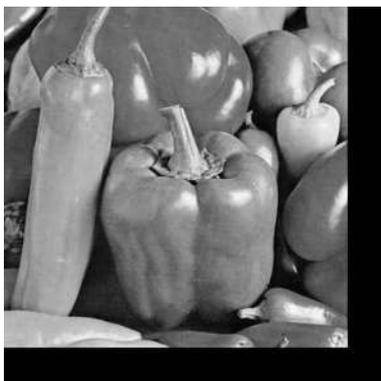
(b)



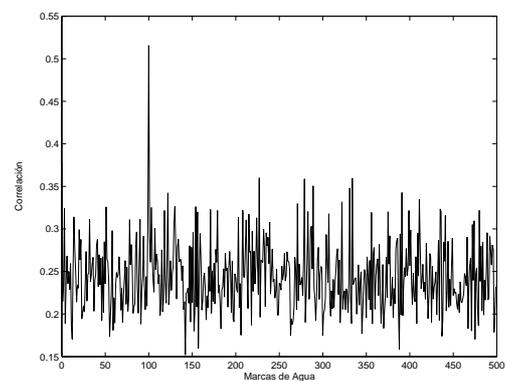
(c)



(d)



(e)

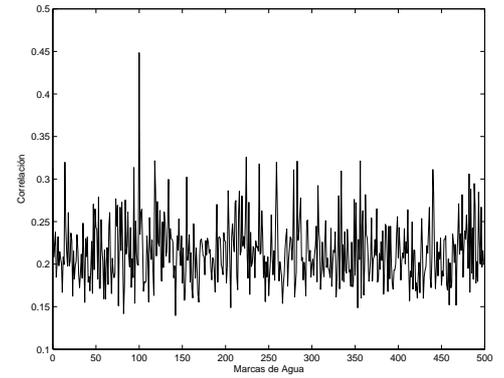


(f)

Figura 3.6: Pruebas de ataques geométricos simples. (a) Imagen rotada  $45^\circ$ ; (b) Correlaciones detectadas. (c) Imagen escalada con factor 1.5; (d) Correlaciones detectadas. (e) Imagen trasladada 50 píxeles en dirección vertical y horizontal; (f) Correlaciones detectadas.



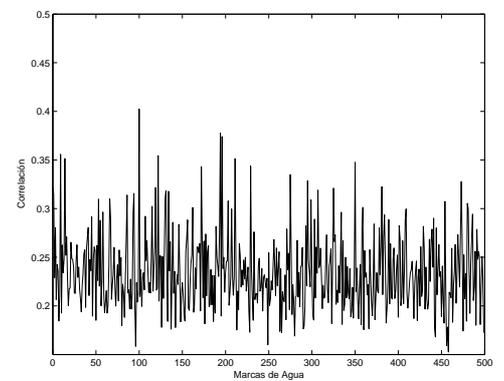
(a)



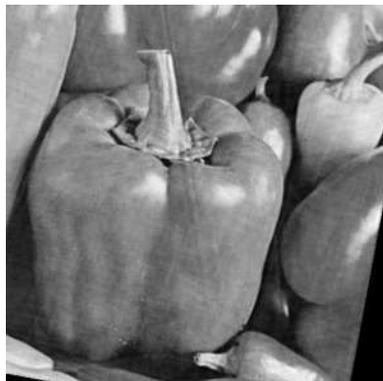
(b)



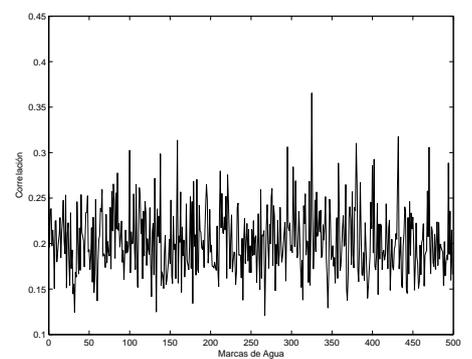
(c)



(d)



(e)



(f)

Figura 3.7: Pruebas de ataques geométricos compuestos. (a) Imagen rotada  $20^\circ$  y trasladada 50 píxeles en dirección horizontal; (b) Correlaciones detectadas. (c) Imagen rotada  $25.5^\circ$ , escalada a 1.2 y trasladada 50 píxeles en dirección vertical y horizontal; (d) Correlaciones detectadas. (e) Imagen rotada  $10.5^\circ$ , escalada con factor 0.7 y trasladada 100 píxeles en dirección vertical y horizontal; (f) Correlaciones detectadas.



## Capítulo 4

# Contribuciones

Los problemas que causan las distorsiones geométricas en los esquemas de marca de agua no han sido resueltos satisfactoriamente por ninguna de las estrategias propuesta hasta ahora (ver Sección 2.5) y, por ello, es necesario explorar nuevas alternativas para su solución.

Este capítulo está organizado de la siguiente manera. En la Sección 4.1 se presentan las justificaciones para el desarrollo de la estrategia propuesta en la tesis, la cual se describe de manera general en la Sección 4.2. En las Secciones 4.3 y 4.4 se muestran el proceso de inserción y detección, respectivamente, de un esquema de marcas de agua en donde se implementa la estrategia propuesta.

### 4.1. Justificación del Método de Optimización

Las diversas estrategias, que han sido propuestas para resolver la sincronización en los esquemas de marcas de agua, tienen las siguientes debilidades:

- *Búsqueda exhaustiva* - Por su alto costo computacional, se debe reducir el intervalo de búsqueda de cada uno de los parámetros necesarios para invertir la distorsión geométrica, asumiendo que los ataques que se aplican a una imagen protegida deben ser ligeros para no afectar su calidad, lo cual, no es necesariamente cierto.
- *Esquemas basados en auto-sincronización y en patrones de sincronización* - Los esque-

mas basados en cualquiera de estas dos estrategias son blancos potenciales de ataques de colusión y filtros especializados. Una vez eliminados los patrones, es imposible restablecer la sincronización del esquema en la detección.

- *Dominios invariantes o semi-invariantes* - Este tipo de esquemas es vulnerable a ataques geométricos severos debido a la pérdida de información en las marcas de agua, causada por los métodos de discretización e interpolación necesarios en algunos de estos dominios.
- *Extracción de características* - La robustez de estos esquemas depende en gran parte de la habilidad del algoritmo utilizado para extraer las características invariantes de las imágenes.

Debido a estas limitaciones, creemos necesario proponer una nueva estrategia para resolver el problema de sincronización en marcas de agua, causados por RST.

Para estudiar el problema de sincronización se realizó el siguiente experimento. Primero se insertó una marca de agua en la magnitud de Fourier de una imagen, utilizando un esquema basado en Espectro Esparcido (SS, por sus siglas en inglés), similar al propuesto en [Cox97]. Posteriormente, se aplicó una distorsión en la imagen marcada que consistió en una rotación de  $90^\circ$  y un escalamiento con factor de 0.9. Finalmente se obtuvo la correlación entre la imagen distorsionada y la marca de agua rotada y escalada con diferentes parámetros, y se generó la gráfica de la Figura 4.1, en donde se puede observar un pico cuando la marca de agua se rota  $90^\circ$  y se escala con un factor de  $1/0.9 = 1.1$ . Este resultado es el esperado si recordamos, de lo visto en la Sección 3.1.1, que la rotación en el dominio espacial causa una rotación en la magnitud de Fourier con el mismo ángulo, y que el escalamiento en el dominio espacial causa un escalamiento inverso en la magnitud de Fourier.

Con este resultado nació la idea de implementar un mecanismo para encontrar los parámetros con los que fue distorsionada la imagen marcada, de forma semejante a un algoritmo de registro de imágenes [Brown92], maximizando la correlación<sup>1</sup> entre la marca

<sup>1</sup>La utilización de métodos de optimización en esquemas de marcas de agua ha sido explorada anteriormente por Pereira *et al.* [Pereira01a], en donde la inserción se aborda como un problema de programación lineal que maximiza la robustez de la marca de agua, con ciertas restricciones relacionadas con el impacto en la percepción visual.

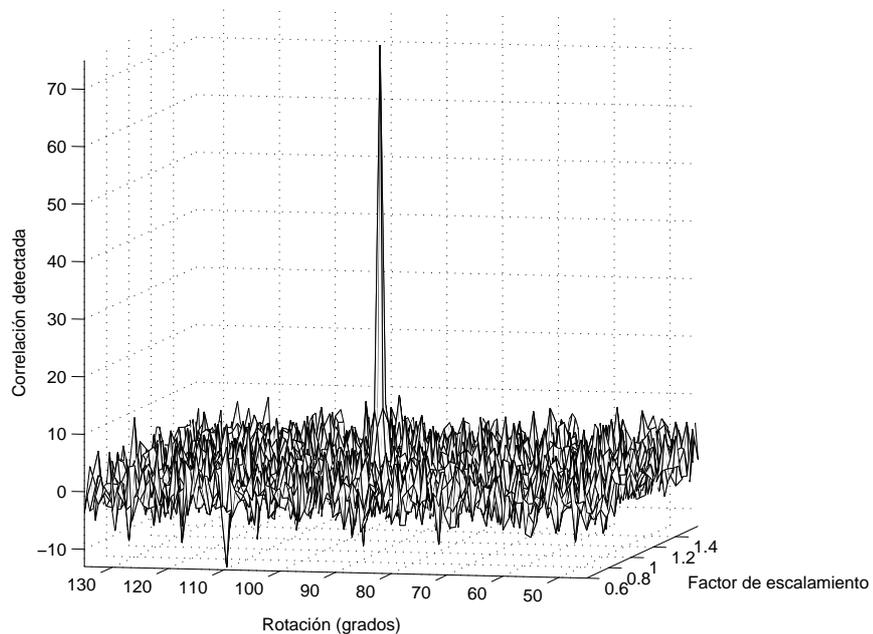


Figura 4.1: Medidas de correlación detectadas entre la imagen distorsionada y la marca de agua modificada por diferentes parámetros de rotación y escalamiento.

de agua insertada originalmente y la imagen analizada, en lugar de minimizar la diferencia entre dos imágenes. Se decidió utilizar un Algoritmo Genético (AG) binario, como método de optimización, por su capacidad para superar máximos locales que tanto afectan a los métodos basados en descenso de gradiente [Haupt98]. Además, en pruebas preliminares, se encontró que, utilizando una cantidad suficiente de bits para representar el vector de parámetros que forma cada gen, se logra una precisión equiparable a la que se obtiene con AG continuos, pero con una velocidad de convergencia mayor debido a la reducción del espacio de búsqueda<sup>2</sup>.

Con la estrategia propuesta en esta tesis se pretenden alcanzar las siguientes ventajas, comparado con otras estrategias:

- El espacio de búsqueda no se tiene que reducir, como en el caso de la búsqueda exhaustiva, pues la precisión y velocidad de convergencia se pueden controlar con

<sup>2</sup>Se realizaron experimentos para decidir el tipo de AG que convenía utilizar, pero sólo se reportan los resultados del AG binario, que fue el que mostró mejor desempeño.

el número de bits asignados a cada gen de los individuos que forman parte del AG binario.

- La sincronización no se basa en inserción de patrones que pueden ser fácilmente removidos por filtros especializados y ataques de colusión.
- No se depende de dominios invariantes o semi-invariantes que utilizan procesos de discretización e interpolación, los cuales causan distorsiones a las marcas de agua que pueden provocar detecciones erróneas.
- Además de la detección de la marca de agua, se encuentran los parámetros de RST con los que se atacó a la imagen, lo cual puede ser de utilidad en esquemas de marcas de agua semi-frágiles o de auto-restauración.

## 4.2. Descripción General de la Estrategia

El funcionamiento general de la estrategia propuesta en esta tesis se ilustra en la Figura 4.2. Suponga una imagen,  $f$ , que entra al proceso de inserción y es marcada con una señal  $w$ . La imagen marcada,  $f_w$ , se distribuye y es posteriormente distorsionada con parámetros de RST, generando una nueva imagen,  $\hat{f}_w$ . Cuando el propietario quiere demostrar que la imagen le pertenece proporciona  $\hat{f}_w$  al proceso de detección, basado en un AG cuya población está formada por individuos (cromosomas) que contienen diferentes parámetros (genes) de RST. Los genes del  $i$ -ésimo individuo se utilizan para transformar  $w$  y obtener una versión  $\hat{w}_i$ . El costo del  $i$ -ésimo individuo se calcula como la correlación entre  $\hat{w}_i$  y  $\hat{f}_w$ . El AG trata de maximizar el costo de su población, utilizando alguna estrategia para la formación de parejas, apareamiento y mutación, y detiene su curso después de  $N_{AG}$  generaciones. Finalmente, el algoritmo reporta la imagen como marcada sólo si el mejor costo es mayor que un umbral definido previamente.

A continuación se propone un esquema en donde se implementa la estrategia propuesta para restablecer la sincronización perdida por ataques de RST.

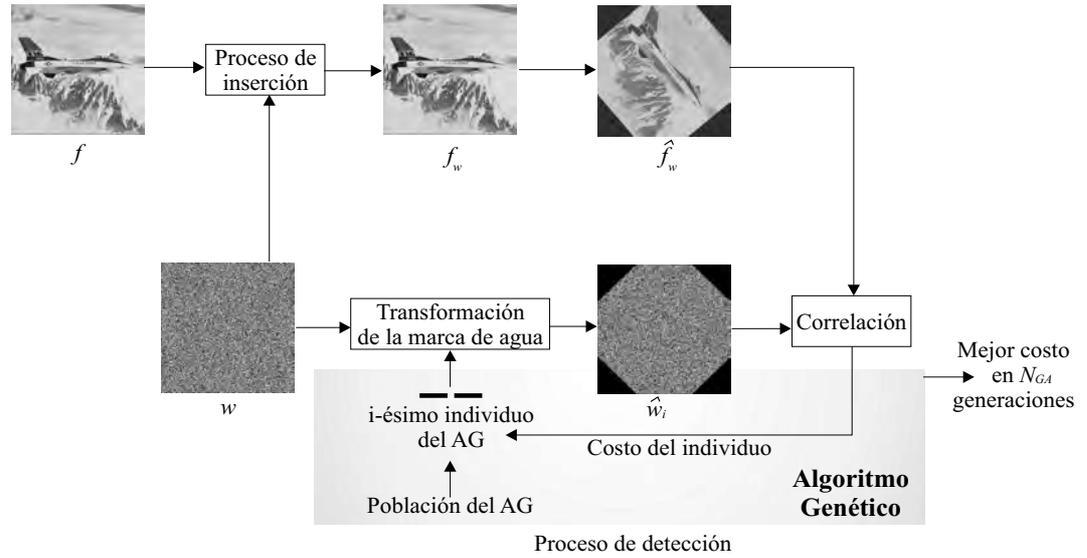


Figura 4.2: Descripción general de la estrategia propuesta.

### 4.3. Proceso de Inserción

Se propone utilizar un esquema de inserción simple en el dominio de Fourier, basado en SS, que permite controlar la robustez y la degradación de la imagen marcada. Las distorsiones causadas por la IDFT no son significativas, por lo que se espera tener una buena respuesta en la detección.

En la Figura 4.3(a) se muestra un diagrama de bloques del proceso de inserción propuesto, y en el Algoritmo 5 se enumeran los pasos a seguir. Suponga una imagen original  $f(x, y)$ , cuya magnitud y fase de Fourier se denotan como  $|F(k, l)|$  y  $\Phi_F(k, l)$ , respectivamente.

Se crea un patrón pseudoaleatorio,  $p_w(x, y)$ , con una distribución Gaussiana con media cero y varianza unitaria, del mismo tamaño de la imagen original, y diseñado con la misma simetría de la magnitud de Fourier.

A continuación se genera una marca de agua binaria,  $w(x, y)$ , por medio de la siguiente ecuación,

$$\begin{cases} w(x, y) = 1 & \text{si } p_w(x, y) > 0 \\ w(x, y) = -1 & \text{si } p_w(x, y) \leq 0 \end{cases} . \quad (4.1)$$

Para insertar la marca de agua, se modifica cada coeficiente  $|F(k, l)|$  por,

$$|F_w(k, l)| = |F(k, l)| e^{\alpha w(x, y)+1} , \quad (4.2)$$

donde el  $\alpha$  es un parámetro, definido por el usuario, con el cual se controla la energía de la marca de agua. La robustez de la marca es mayor cuando se incrementa el valor de  $\alpha$ , pero también se ocasiona mayor distorsión a la imagen marcada. Empíricamente se encontró que un valor de  $\alpha \approx 0.15$  es suficiente para obtener una robustez y calidad de la imagen marcada satisfactorias.

Observe que al insertar la marca utilizando la ecuación (4.2) se evitan cambios de dirección en la fase, lo cual generaría distorsiones severas en la imagen marcada.

Finalmente se calcula la parte real e imaginaria de la señal, utilizando la fase original  $\Phi F(k, l)$ , y se calcula la IDFT para obtener la imagen marcada  $f_w(x, y)$  (se conserva la parte real y la imaginaria se desecha).

El proceso de inserción propuesto es suficiente para los propósitos establecidos, pero creemos que se puede mejorar significativamente el desempeño del esquema si se utiliza un proceso de inserción informado, como el propuesto en [Chen00].

#### 4.4. Proceso de Detección

El esquema general del proceso de detección propuesto se ilustra en la Figura 4.3(b). Las propiedades de invariancia a traslación de la magnitud de Fourier, discutidas en la Sección 3.1.1, permiten resolver de manera implícita los ataques de traslación. Para resolver el escalamiento y rotación se propone utilizar un AG para maximizar la correlación entre la marca de agua y el logaritmo natural de la magnitud de Fourier de la imagen de entrada.

---

**Algoritmo 5** Proceso de inserción propuesto
 

---

ALGINSGA( $rImg$ ,  $marca$ )

1  $iImg \leftarrow$  LLENACEROS()

2  $[rImgFFT, iImgFFT] \leftarrow$  FFT( $rImg$ ,  $iImg$ )

3  $[mImgFFT, fImgFFT] \leftarrow$  CALCULAMAGFASE( $rImgFFT$ ,  $iImgFFT$ )

4  $mMarcadaFFT \leftarrow$  insertaMarca( $mImgFFT$ ,  $marca$ )

5  $[rMarcadaFFT, iMarcadaFFT] \leftarrow$  CALCULARREALIMAG( $mMarcadaFFT$ ,  $fImgFFT$ )

6  $[rMarcada, iMarcada] \leftarrow$  FFTINVERSA( $rMarcadaFFT$ ,  $iMarcadaFFT$ )

7 **regresar**  $rMarcada$

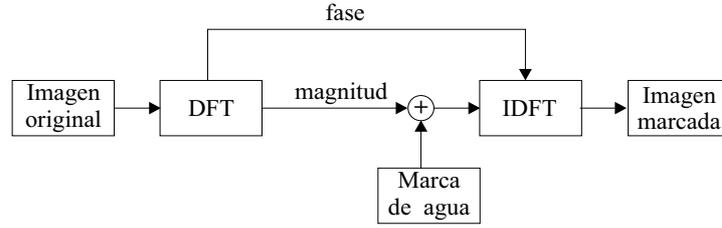
---

Sea  $\ln |\bar{F}(k, l)|$  el logaritmo natural de la magnitud de Fourier de una imagen de entrada  $\bar{f}(x, y)$ . Se genera la marca de agua buscada,  $w(x, y)$ , siguiendo el mismo procedimiento del proceso de inserción. Se traslada el origen de las señales  $w$  y  $\ln |\bar{F}|$  al centro de la imagen, y se les aplica el filtro descrito en la Sección 4.4.2 para mejorar la respuesta del detector. Finalmente, se ejecuta un algoritmo de búsqueda, basado en un AG (ver Sección 4.4.1), que busca maximizar la correlación entre ambas señales. Si, después de  $N_{AG}$  generaciones, la correlación del mejor individuo es mayor que un umbral,  $\tau$ , el detector reporta la presencia de la marca de agua y muestra los parámetros de rotación y escalamiento encontrados por el método de optimización.

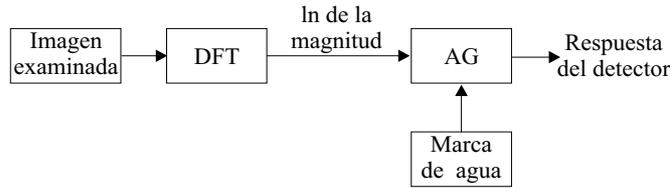
#### 4.4.1. Especificaciones del AG

Todos los individuos del AG contienen un cromosoma  $\Omega = [\phi, \sigma]$  de 32 bits, de los cuales, 16 bits están designados para el gen de rotación,  $\phi$ , y los 16 bits restantes para el gen de escalamiento,  $\sigma$ .

Puesto que la magnitud de Fourier es simétrica, el valor del gen  $\phi$  de cada individuo se define entre 0 y  $\pi$  radianes. Con los 16 bits correspondiente a este gen, se logra una



(a)



(b)

Figura 4.3: Esquemas de inserción y extracción propuestos. (a) Esquema de inserción. (b) Esquema de detección.

discretización menor a  $3.0 \times 10^{-4}$ . Por otro lado, el valor del gen  $\sigma$  de cada individuo está acotado entre  $\frac{1}{1.6}$  y  $\frac{1}{0.6}$ . Estos límites permiten encontrar ataques de escalamiento entre 0.6 y 1.6, pero se definen de esta manera por el efecto inverso que se tiene en el dominio de Fourier al aplicar escalamiento en el dominio espacial (ver Sección 3.1.1). Con los 16 bits designados para este gen, se logra una discretización menor a  $1.6 \times 10^{-5}$ .

El costo del  $i$ -ésimo individuo, cuyo cromosoma es  $\Omega_i = [\phi_i, \sigma_i]$ , se calcula como,

$$C_i = \frac{\hat{w}_i^T \ln |\bar{F}|}{\sqrt{\ln |\bar{F}|^T \ln |\bar{F}|}} , \quad (4.3)$$

donde,

$$\hat{w}_i(\phi_i, \sigma_i) = \mathcal{R}(\phi_i) \circ \mathcal{S}(\sigma_i) w(x, y) , \quad (4.4)$$

y donde  $\mathcal{R}(\phi_i)$  representa la transformación de rotación,  $\mathcal{S}(\sigma_i)$  representa la transformación de escalamiento y  $(\circ)$  denota la composición de dichas transformaciones. No importa el

orden en que se apliquen las transformaciones debido a que las dos aplicaciones lineales cuentan con la siguiente propiedad de conmutatividad:

$$\begin{aligned}
\mathcal{R}(\phi_i) \circ \mathcal{S}(\sigma_i) w(x, y) &= \mathcal{R}(\phi_i) w(\sigma_i x, \sigma_i y) \\
&= w(\sigma_i x \cos \phi_i - \sigma_i y \sin \phi_i, \sigma_i x \sin \phi_i + \sigma_i y \cos \phi_i) \\
&= \mathcal{S}(\sigma_i) w(x \cos \phi_i - y \sin \phi_i, x \sin \phi_i + y \cos \phi_i) \\
&= \mathcal{S}(\sigma_i) \circ \mathcal{R}(\phi_i) w(x, y)
\end{aligned}$$

Para acelerar la convergencia del AG utilizado en el detector de marcas de agua propuesto, se crea una población uniformemente distribuida<sup>3</sup> con incrementos de  $8.72 \times 10^{-3}$  radianes en  $\phi$ , y 0.005 en  $\sigma$ , tal como se muestra en la Figura 4.4. Por lo tanto, el AG inicia con una población de 72,561 individuos y se reduce a 800 después a partir de la segunda generación, pues, debido a la distribución de la población inicial, se considera que alguno o algunos de los mejores individuos de la población inicial deben estar suficientemente cerca del máximo global, de tal manera que el resto de las generaciones sólo servirán para mejorar la convergencia.

Las selección de parejas se realiza dando mayor peso a los individuos con mejor costo, es decir, un individuo tiene más probabilidad de reproducción cuando su costo es mayor. Se utilizó un proceso de reproducción convencional que genera dos nuevos individuos con información de ambos padres. Se decidió aplicar un esquema de mutación convencional al 20% de la población, que consiste en el cambio de un bit elegido aleatoriamente. Todos los individuos tienen la misma probabilidad de mutación, excepto el de costo más alto, cuya probabilidad de mutación es cero. El AG se configura para evolucionar durante 15 generaciones, pues se encontró empíricamente que este número de generaciones es suficiente para encontrar el máximo global en este problema en particular y utilizando una población inicial de 72,561 individuos.

---

<sup>3</sup>Una de las técnicas, que se mencionan en [Haupt98], para acelerar la convergencia de un AG, especialmente cuando la evaluación de la función de costo definida consume mucho tiempo de cómputo, consiste en distribuir la población inicial cubriendo uniformemente el espacio de búsqueda. Esta técnica permite lograr una convergencia más rápida hacia el máximo global y evita, además, la creación y evaluación de individuos con cromosomas iguales en la población inicial.

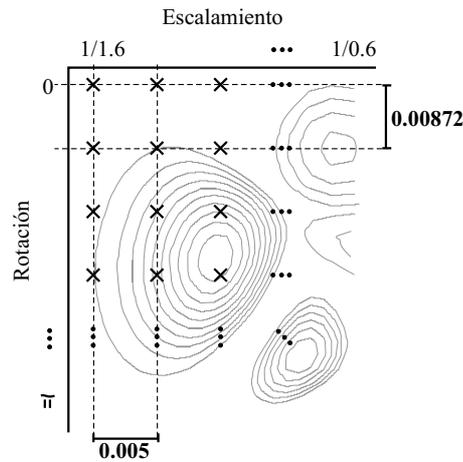


Figura 4.4: Distribución de la población inicial.

#### 4.4.2. Filtro para mejorar la correlación

De la teoría de detección se sabe que la correlación es un método óptimo para detectar la presencia de una señal en canales de AWGN. Sin embargo, las imágenes generalmente mantienen cierta correlación entre sus componentes de frecuencia, lo que hace que la correlación no resulte un método eficiente para verificar la presencia de una marca de agua. Depovere *et al.* [Depovere98] propusieron aplicar un filtro de diferencias de renglones en la marca de agua y la imagen antes de calcular su correlación. El filtro elimina la correlación existente en los elementos de la imagen y mejora significativamente la respuesta del detector. El filtro es conocido en inglés como *whitening filter*, puesto que, después de aplicar el filtro, la distribución de la señal se asemeja a una señal de AWGN.

Cox *et al.* [Cox02] propusieron posteriormente utilizar un filtro bidimensional con distribución elíptica Gaussiana, con un núcleo de tamaño  $11 \times 11$ , que mejora los resultados alcanzados por Depovere. No obstante, el filtrado resulta costoso con un núcleo no separable tan grande, pues requiere de  $N_R \times N_C \times M^2$  operaciones, donde  $N_R$  y  $N_C$  son el total de renglones y columnas de la imagen, respectivamente y  $M$  es la longitud del núcleo del filtro. Por ejemplo, para filtrar una imagen de tamaño  $256 \times 256$  se requieren  $256 \times 256 \times 11^2 = 7,929,856$  operaciones. Por lo tanto, el desempeño de un AG se vería afectado por la utilización de este filtro.

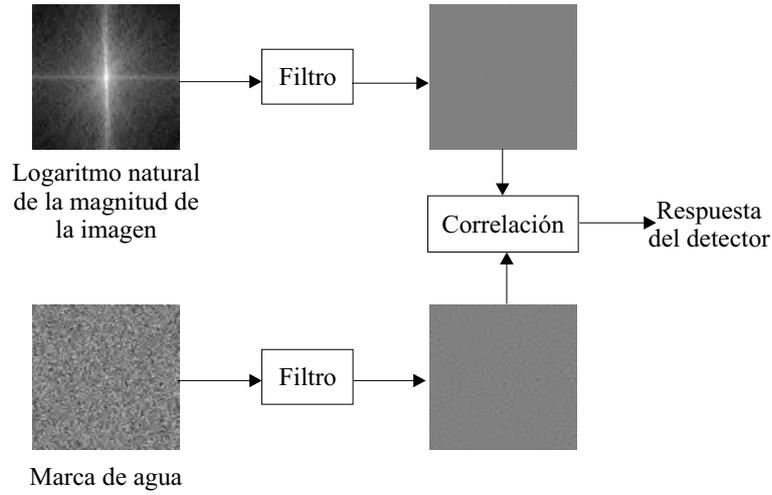


Figura 4.5: Funcionamiento del filtro para mejorar la correlación.

Puesto que se desea eliminar la correlación entre los elementos de la imagen, proponemos utilizar un filtro separable,  $\eta = [-1, 1]$ , que calcula las diferencias en los renglones y columnas, y denominamos Filtro Bidimensional de Diferencias Separable (SBD-WF, por sus siglas en inglés). De esta manera se elimina la correlación no sólo en los renglones, como lo propuso Depovere, sino además en las columnas, en donde también existe correlación. El cómputo del filtro separable no es costoso, pues se requieren  $2(N_R \times N_C) \times M$  operaciones. Por ejemplo, para filtrar una imagen de tamaño  $256 \times 256$  se requieren de  $2(256 \times 256) \times 2 = 262,144$  operaciones; sólo el 3% de las necesarias con el filtro de Cox.

Entonces, para calcular el costo del  $i$ -ésimo individuo del AG se sustituye la ecuación (4.3) por,

$$C_i = \frac{(\ln |\bar{F}| * \eta)^T (\hat{w}_i * \eta)}{\sqrt{(\ln |\bar{F}| * \eta)^T (\ln |\bar{F}| * \eta)}}, \quad (4.5)$$

donde  $(*)$  denota la operación convolución. La Figura 4.5 ilustra el proceso de filtrado y cálculo de correlación de la ecuación (4.5).

Las desventajas de utilizar este tipo de filtros es que si la imagen que contiene la marca agua tiene una distribución semejante a una señal AWGN (e.g. imágenes con estática), el filtro disminuye la medida de correlación, en lugar de mejorarla [Cox02]. Por esta razón,

en aplicaciones en donde es común encontrar este tipo de imágenes, no es recomendable la utilización de estos filtros.

## 4.5. Pasos del Proceso de Detección Propuesto

En el Algoritmo 6 se enumeran los pasos necesarios del proceso de detección propuesto en esta tesis. En las funciones *generaPoblacionInicial()*, *selParejas()*, *apareamiento()* y *mutacion()* se toman en cuenta las consideraciones discutidas en la Sección 4.4.1. Observe además que se aplica la función *SBD – WF()* como filtro para mejorar la correlación cuando se llama a la función *calculaCorrelacion()*. Note que el AG se deja evolucionar por 15 generaciones o hasta que la correlación del mejor individuo de la población sea mayor que el umbral establecido por el usuario.

---

**Algoritmo 6** Proceso de detección propuesto
 

---

```

ALGDETGA(rImg, marcaBuscada, umbral)
1  iImg ← LLENACEROS()
2  [rImgFFT, iImgFFT] ← FFT(rImg, iImg)
3  [mImgFFT, fImgFFT] ← CALCULAMAGFASE(rImgFFT, iImgFFT)
4  mImgFFTw ← SBD-WF(mImgFFT)
5  popIni ← GENERAPOBLACIONINICIAL()
6  popIni ← ORDENAPORCOSTO(popIni)
7  generac ← 0
8  repetir
9      parejas ← SELPAREJAS(pop)
10     popNueva ← APAREAMIENTO(parejas, pop)
11     popNueva ← MUTACION(popNueva, 20)
12     popNueva ← ORDENAPORCOSTO(popNueva)
13     si (generac = 0)
14         entonces pop ← REDUCEPOBLACION(popNueva)
15
16     sino      pop ← popNueva
17     mejor ← TRANSFORMAIMAGEN(marcaBuscada, pop[0])
18     mejorw ← SBD-WF(mejor)
19     corr ← CALCULACORRELACION(mejorw, mImgFFTw)
20     generac ← generac + 1
21     hasta (generac < 15 ó corr < umbral)
22 regresar corr

```

---



## Capítulo 5

# Resultados

Para analizar el desempeño del esquema propuesto en esta tesis se desarrollaron diferentes pruebas, organizadas de la siguiente manera. En la Sección 5.1 se muestra una comparación entre el filtro SBD-WF propuesto y tres diferentes filtros encontrados en la literatura. En la Sección 5.2 se define empíricamente un umbral, para el esquema propuesto, con una probabilidad pequeña de falsos positivos. En la Sección 5.3 se discuten diferentes pruebas aplicadas con una herramienta estándar. Finalmente, en la Sección 5.4 se muestran casos de estudio que sirven de comparación entre el desempeño del esquema propuesto en esta tesis y el esquema de Lin.

### 5.1. Filtro para Mejorar la Detección

Se realizaron comparaciones del desempeño del filtro SBD-WF, propuesto en esta tesis, con los resultados obtenidos al utilizar el filtro de diferencias en renglones propuesto en [Depovere98], un filtro de diferencias en columnas, y el filtro bidimensional propuesto por Cox *et al.* [Cox02].

Para los experimentos reportados en esta sección se utilizaron 1000 imágenes de origen diverso<sup>1</sup>. Primero se aplicó el esquema de detección propuesto (ver Sección 4.4) en las 1000 imágenes *sin marcar* utilizando los cuatro diferentes filtros. Posteriormente se repitió el

---

<sup>1</sup>El término *imágenes de origen diverso* se utilizará en lo subsecuente para hacer referencia a un conjunto de imágenes con características diversas, es decir, imágenes naturales, artificiales, con textura, lisas, etc.

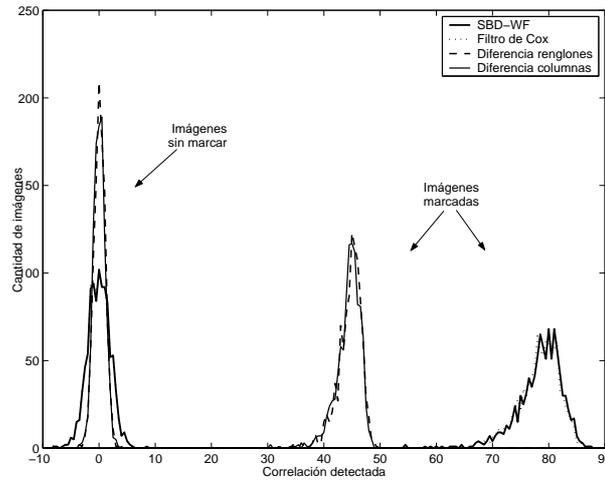


Figura 5.1: Correlación detectada utilizando cuatro diferentes filtros.

experimento, pero marcando previamente las 1000 imágenes con el esquema de inserción propuesto (ver Algoritmo 5).

En la Figura 5.1 se muestra un histograma con las medidas de detección obtenidas usando los diferentes filtros en ambos experimentos<sup>2</sup>. En la gráfica se puede observar que el comportamiento de los filtros de diferencias en renglones y columnas es similar, pero los valores detectados son menores que los que se obtienen con los otros dos filtros. Los resultados detectados con el filtro de Cox y el SBD-WF son semejantes con las imágenes marcadas y sin marcar, pero el SBD-WF tiene la ventaja de que es un filtro separable con un bajo costo computacional (ver Sección 4.4.2).

## 5.2. Definición del Umbral de Detección

Recuerde que el esquema de detección está diseñado para comparar la correlación encontrada con un umbral definido por el usuario. Si se detecta una correlación mayor a dicho umbral, el esquema de detección reporta una imagen como marcada, de lo contrario la reporta como no marcada. Por esta razón, la definición del umbral es importante para

<sup>2</sup>Los resultados obtenidos con el filtro de Cox se escalaron al mismo rango de valores que se obtuvieron con los demás filtros.

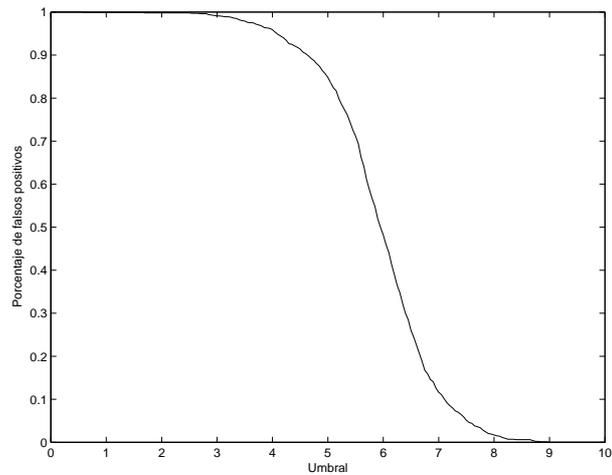


Figura 5.2: Probabilidad de falsos positivos dependiendo del umbral.

discriminar los resultados encontrados por el detector, de manera que se tengan la menor cantidad de *falsos positivos* y *falsos negativos*.

Gracias a la utilización del filtro SBD-WF (ver Sección 5.1), la correlación detectada en imágenes marcadas que no han sufrido distorsión alguna es suficientemente mayor que la correlación encontrada en imágenes sin marcar. Por lo tanto, la probabilidad de obtener falsos negativos depende de la pérdida de información que se sufre con las distorsiones aplicadas en las imágenes marcadas.

Debido la gran variedad de imágenes que pueden ser evaluadas por el esquema de detección, se asume que no es posible realizar un modelo matemático confiable para obtener la probabilidad de reportar falsos positivos. Por esta razón, se decidió buscar empíricamente un umbral con una probabilidad de falsos positivos cercana a cero. Para este experimento se utilizaron 1000 imágenes de origen diverso. Se registró la correlación encontrada por el proceso de detección entre una marca de agua aleatoria y cada una de las imágenes *sin marcar*. En la Figura 5.2 se muestra el porcentaje de falsos positivos que se encontraron dependiendo del umbral seleccionado. Con la información recopilada en este experimento se decidió establecer un umbral de 9.5, el cual ofrece una probabilidad de falsos positivos cercana a cero. Por lo tanto, una imagen se reporta como marcada sólo si el detector obtiene un valor de correlación mayor a 9.5.



Figura 5.3: Imágenes estándares utilizadas. (a) Pimientos  $512 \times 512$ . (b) Lena  $512 \times 512$ . (c) Barco  $512 \times 512$ .

### 5.3. Pruebas Estándares

Para comprobar la robustez del esquema propuesto ante diferentes tipos de ataques, se utilizó Stirmark 4.0 [Petitcolas98, Petitcolas00], que es una herramienta estándar diseñada específicamente para probar la robustez de esquemas de esteganografía y marcas de agua (ver Sección 2.3).

A continuación se describen las pruebas que se aplicaron en las tres imágenes estándares que se muestran en las Figuras 5.3(a)-(c). En todas las pruebas estándares, excepto las de la Sección 5.3.1, Stirmark estableció automáticamente un valor de  $\alpha \approx 2.5$ .

#### 5.3.1. Correlación usando diferentes valores de $\alpha$

Este primer experimento consistió en utilizar diferentes valores de  $\alpha$  en el esquema de inserción. El valor mínimo utilizado fue de  $\alpha = 0$ , que causa un PSNR de las imágenes marcadas que tiende a infinito (sin distorsión), y el máximo valor utilizado fue de  $\alpha = 0.5$ , que causa un PSNR en las imágenes marcadas alrededor de 20 dB (mucho distorsión). Ejemplos de la distorsión causada en las imágenes marcadas, dependiendo del parámetro  $\alpha$ , se pueden apreciar en las Figuras 5.4(a)-(c).



Figura 5.4: Imágenes creadas con diferentes valores de  $\alpha$ . (a)  $\alpha = 0.05$ , con PSNR  $\approx 40$  dB. (b)  $\alpha = 0.15$ , con PSNR  $\approx 32$  dB. (c)  $\alpha = 0.5$ , con PSNR  $\approx 20$  dB.

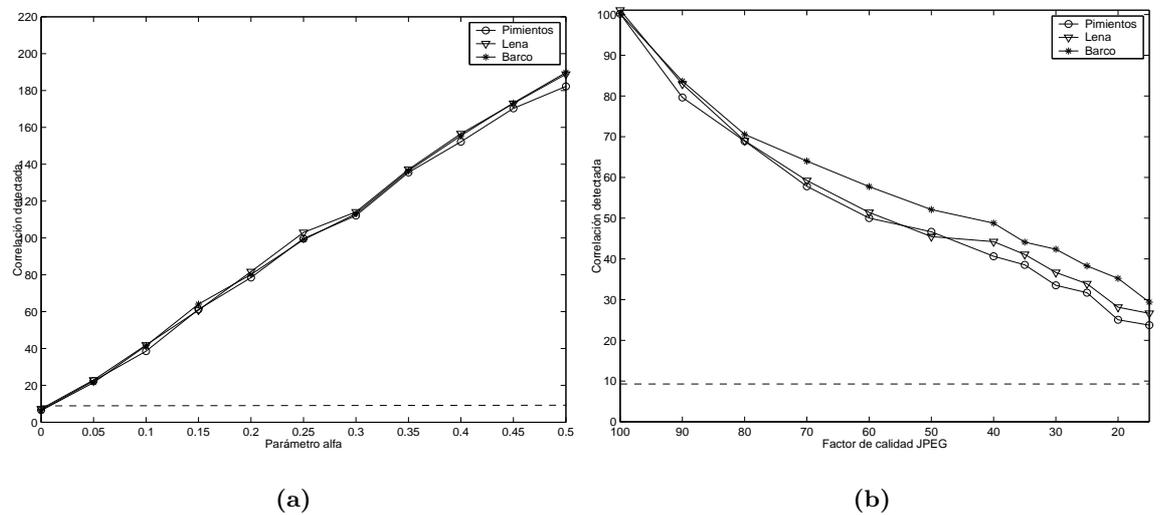


Figura 5.5: Resultados de pruebas de  $\alpha$  y compresión JPEG. (a) Medidas de correlación detectadas usando diferentes valores de  $\alpha$ . (b) Medidas de correlación detectadas después de aplicar compresión JPEG con diferentes factores de calidad.

En la gráfica de la Figura 5.5(a) se muestran los valores de detección obtenidos usando diferentes valores de  $\alpha$  en el proceso de inserción. Empíricamente se encontró que sintonizando el parámetro  $\alpha$  con un valor aproximado a 0.15 se logra buena robustez de la marca de agua ante la mayoría de los ataques que aquí se reportan, además que mantiene una buena calidad de la imagen.

### 5.3.2. Compresión con pérdida

En este experimento, las imágenes marcadas fueron comprimidas con el estándar JPEG utilizando diferentes factores de calidad. La Figura 5.5(b) muestra la correlación obtenida de las imágenes comprimidas, en la cual se observa que la marca de agua sobrevivió todas las tasas de compresión en las tres imágenes. Note que la correlación detectada es mayor que el umbral, incluso cuando se conserva sólo el 15 % de la calidad de las imágenes. Los efectos de la distorsión se pueden apreciar en las Figuras 5.6(a)-(c), donde se muestran las imágenes comprimidas con un factor de calidad de 15 %, 50 % y 100 %, respectivamente.

Estos resultados eran los esperados, puesto que la compresión con pérdida afecta generalmente a las frecuencias más altas del espectro de la imagen, modificando sólo una parte de la marca de agua, dependiendo de la tasa de compresión.

### 5.3.3. Adición de ruido

Este experimento consiste en añadir cierta cantidad de ruido a las imágenes marcadas. Primero se crea una imagen con valores aleatorios del mismo tamaño que la imagen que se va a distorsionar. Posteriormente, se establece un peso de la imagen aleatoria antes de sumarla a la imagen marcada. Por ejemplo, en la primera prueba se suma el 20 % de la imagen aleatoria (ruido) con el 80 % de la imagen marcada.

En la Figura 5.7(a) se presenta una gráfica de las medidas de correlación detectadas en imágenes después de agregar diferentes porcentajes de ruido. El ruido afecta severamente la detección de la marca de agua, pues la medida de correlación que se detecta es menor que el umbral, incluso en la prueba en donde se agregó sólo el 20 % del ruido. Sin embargo, la calidad de las imágenes se reduce significativamente después de aplicar la distorsión en



Figura 5.6: Imágenes comprimidas con JPEG. (a) con factor de calidad de 15 %. (b) con factor de calidad de 50 %. (c) con factor de calidad de 100 %.

todas estas pruebas. En las Figuras 5.8(a)-(c) se puede observar la adición de ruido a la imagen de Lena marcada utilizando diferentes pesos.

#### 5.3.4. Eliminación de líneas

Este experimento consiste en eliminar renglones y columnas (líneas) de las imágenes marcadas. La primera prueba consiste en eliminar una de cada 10 líneas de las imágenes, la segunda consiste en eliminar una de cada 20 líneas, y así sucesivamente. Los resultados del experimento se pueden observar en la gráfica de la Figura 5.7(b), y en las Figuras 5.9(a)-(c) se muestran las imágenes que resultaron al eliminar una de cada 10, 40 y 100 líneas. Las marcas de agua sobrevivieron este ataque en las tres imágenes, incluso perdiendo hasta el 10 % de la imagen.

#### 5.3.5. Convolución con diferentes filtros

En este experimento se desea comprobar la robustez del esquema propuesto ante filtros binomiales, de corrección de nitidez, de mediana.

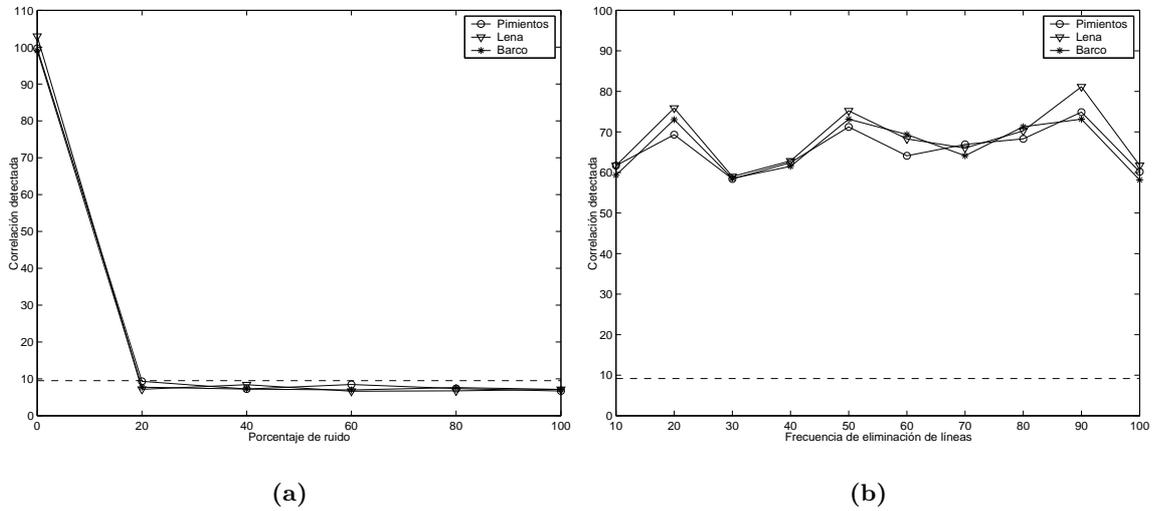


Figura 5.7: Resultados de pruebas de ruido y eliminación de líneas (a) Medidas de correlación detectadas en las imágenes distorsionadas con ruido. (b) Medidas de correlación detectadas después de eliminar líneas de las imágenes marcadas.

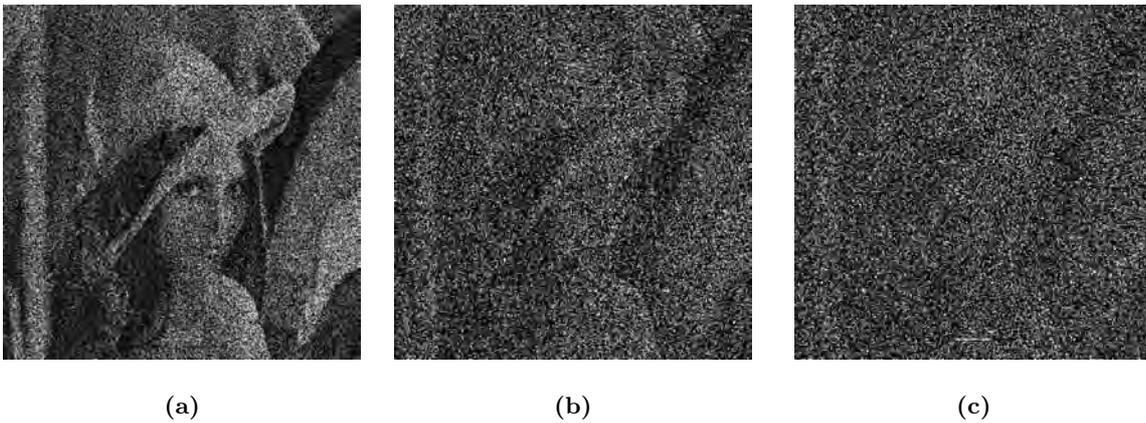


Figura 5.8: Imágenes marcadas a las que se les agregó ruido. (a) 20 % ruido + 80 % imagen marcada. (b) 60 % ruido + 40 % imagen marcada. (c) 100 % ruido.



Figura 5.9: Eliminación de renglones y columnas de las imágenes marcadas. (a) Imagen resultante de  $460 \times 460$ . (b) Imagen resultante de  $499 \times 499$ . (c) Imagen resultante de  $506 \times 506$ .

Los núcleos de los filtros binomial y de corrección de nitidez utilizados están definidos como,

Filtro binomial

Filtro de corrección de nitidez

$$\begin{pmatrix} \frac{1}{9} & \frac{2}{9} & \frac{1}{9} \\ \frac{2}{9} & \frac{4}{9} & \frac{2}{9} \\ \frac{1}{9} & \frac{2}{9} & \frac{1}{9} \end{pmatrix} \qquad \begin{pmatrix} 0 & -\frac{1}{9} & 0 \\ -\frac{1}{9} & \frac{5}{9} & -\frac{1}{9} \\ 0 & -\frac{1}{9} & 0 \end{pmatrix}$$

Note que los coeficientes de los dos filtros nos suman uno, con lo cual se modifica el rango dinámico de las imágenes. Para mejorar su visualización, se restauró el rango dinámico de las dos imágenes filtradas, tal como se muestran en Figuras 5.10(a) y 5.10(b).

A continuación se aplicaron filtros de mediana con ventanas de tamaño  $3 \times 3$ ,  $5 \times 5$ ,  $7 \times 7$  y  $9 \times 9$ . En la Tabla 5.1 se muestran las medidas de correlación detectadas en las tres imágenes atacadas con los diferentes filtros. Como se puede observar en los resultados, las marcas de agua sobreviven perfectamente el filtro binomial, de corrección de nitidez, y los primeros tres filtros de mediana, con medidas de correlación mayores a 15.0. En el caso del filtro de mediana con ventana de tamaño  $9 \times 9$ , la correlación se detectó debajo del umbral en la imagen de Pimientos (resaltada en negritas), pero su calidad se redujo considerablemente, como se aprecia en la Figura 5.10(d).

Tabla 5.1: Pruebas de convolución con diferentes filtros.

| Prueba                  | Pimientos   | Lena  | Barco |
|-------------------------|-------------|-------|-------|
| F. binomial             | 32.39       | 42.19 | 26.88 |
| F. nitidez              | 72.40       | 72.97 | 77.60 |
| F. Mediana $3 \times 3$ | 41.29       | 46.20 | 48.26 |
| F. Mediana $5 \times 5$ | 19.31       | 26.20 | 27.07 |
| F. Mediana $7 \times 7$ | 15.39       | 15.42 | 20.31 |
| F. Mediana $9 \times 9$ | <b>8.64</b> | 13.76 | 15.06 |



(a)



(b)



(c)



(d)

Figura 5.10: Imágenes distorsionadas con diferentes filtros. (a) Filtro binomial. (b) Filtro de corrección de nitidez. (c) Filtro de mediana de  $3 \times 3$ . (d) Filtro de mediana de  $9 \times 9$ .

### 5.3.6. Rotación y escalamiento

Este experimento consistió en aplicar diferentes tipos de distorsiones geométricas registrando, en la Tabla 5.2, las medidas de correlación detectadas en las tres imágenes.

Primero, se escalaron las imágenes a diferentes porcentajes del tamaño original, sin causar recortes en las imágenes. En las Figuras 5.11(a) y 5.11(b) se muestra la imagen de Lena escalada al 50 % y 200 %, respectivamente. La reducción en tamaño de una imagen causa pérdida de información y provoca a su vez que la disminución en las medidas de correlación detectadas, como se puede observar en los resultados, pero permanecen suficientemente arriba del umbral establecido en todas las pruebas de escalamiento realizadas.

Posteriormente, se aplicaron rotaciones sin pérdida con diferentes ángulos. En las Figuras 5.11(c) y Figura 5.11(d) se muestran la imagen de Lena rotada  $-45^\circ$  y  $-90^\circ$ , respectivamente. En los resultados de la Tabla 5.2 se puede observar que, mientras más cercana es la rotación a los  $\pm 45^\circ$ , menor es la correlación detectada. La causa de este fenómeno, discutida en [Lin01], es la pérdida de información debida a los efectos de la rotación en la DFT. Sin embargo, la correlación obtenida en este conjunto de pruebas es superior a la del umbral establecido, por lo cuál, no se tienen falsos negativos.

Finalmente se aplicaron rotaciones con pérdida con diferentes ángulos. Las Figuras 5.11(e) y 5.11(f) muestran la imagen de Lena rotada  $-0.25^\circ$  y  $2^\circ$ , respectivamente. En estas pruebas también se obtuvieron detecciones arriba del umbral establecido. De hecho, en las pruebas de rotación con pérdida se obtuvieron detecciones ligeramente menores a las obtenidas en las pruebas de rotación sin pérdida discutidas en el párrafo anterior.

Tabla 5.2: Pruebas de rotación y escalamiento.

| Prueba                     | Pimientos | Lena   | Barco  |
|----------------------------|-----------|--------|--------|
| Escalamiento 50 %          | 54.27     | 58.57  | 56.15  |
| Escalamiento 75 %          | 77.30     | 83.38  | 78.79  |
| Escalamiento 90 %          | 69.93     | 69.93  | 70.81  |
| Escalamiento 110 %         | 77.40     | 79.01  | 78.04  |
| Escalamiento 150 %         | 99.65     | 99.49  | 99.94  |
| Escalamiento 200 %         | 103.68    | 104.91 | 104.33 |
| Rotación $-0.25^\circ$     | 37.73     | 41.88  | 43.13  |
| Rotación $-0.75^\circ$     | 43.26     | 45.85  | 45.18  |
| Rotación $-1^\circ$        | 42.26     | 43.23  | 47.52  |
| Rotación $-2^\circ$        | 39.16     | 45.73  | 45.00  |
| Rotación $-5^\circ$        | 38.99     | 41.26  | 43.37  |
| Rotación $-10^\circ$       | 37.21     | 38.23  | 36.49  |
| Rotación $-15^\circ$       | 28.88     | 34.58  | 31.17  |
| Rotación $-30^\circ$       | 20.89     | 22.51  | 21.81  |
| Rotación $-45^\circ$       | 18.74     | 15.86  | 16.99  |
| Rotación $-90^\circ$       | 96.95     | 96.61  | 98.63  |
| Rotación $0.5^\circ$       | 39.21     | 44.70  | 46.58  |
| Rotación $0.25^\circ$      | 36.48     | 43.65  | 40.73  |
| Rotación $0.75^\circ$      | 40.44     | 46.92  | 49.90  |
| Rotación $1^\circ$         | 43.78     | 45.86  | 42.55  |
| Rotación $2^\circ$         | 37.35     | 45.41  | 45.28  |
| Rot./Recorte $-0.5^\circ$  | 40.12     | 45.86  | 46.41  |
| Rot./Recorte $-0.25^\circ$ | 37.11     | 39.96  | 42.84  |
| Rot./Recorte $-0.75^\circ$ | 42.86     | 46.17  | 45.99  |
| Rot./Recorte $-1^\circ$    | 40.17     | 45.28  | 47.61  |
| Rot./Recorte $-2^\circ$    | 39.70     | 43.53  | 46.28  |
| Rot./Recorte $0.5^\circ$   | 39.20     | 44.30  | 47.59  |
| Rot./Recorte $0.25^\circ$  | 36.29     | 40.96  | 40.62  |
| Rot./Recorte $0.75^\circ$  | 40.66     | 44.93  | 50.35  |
| Rot./Recorte $1^\circ$     | 42.36     | 42.15  | 44.42  |
| Rot./Recorte $2^\circ$     | 36.53     | 43.77  | 44.42  |

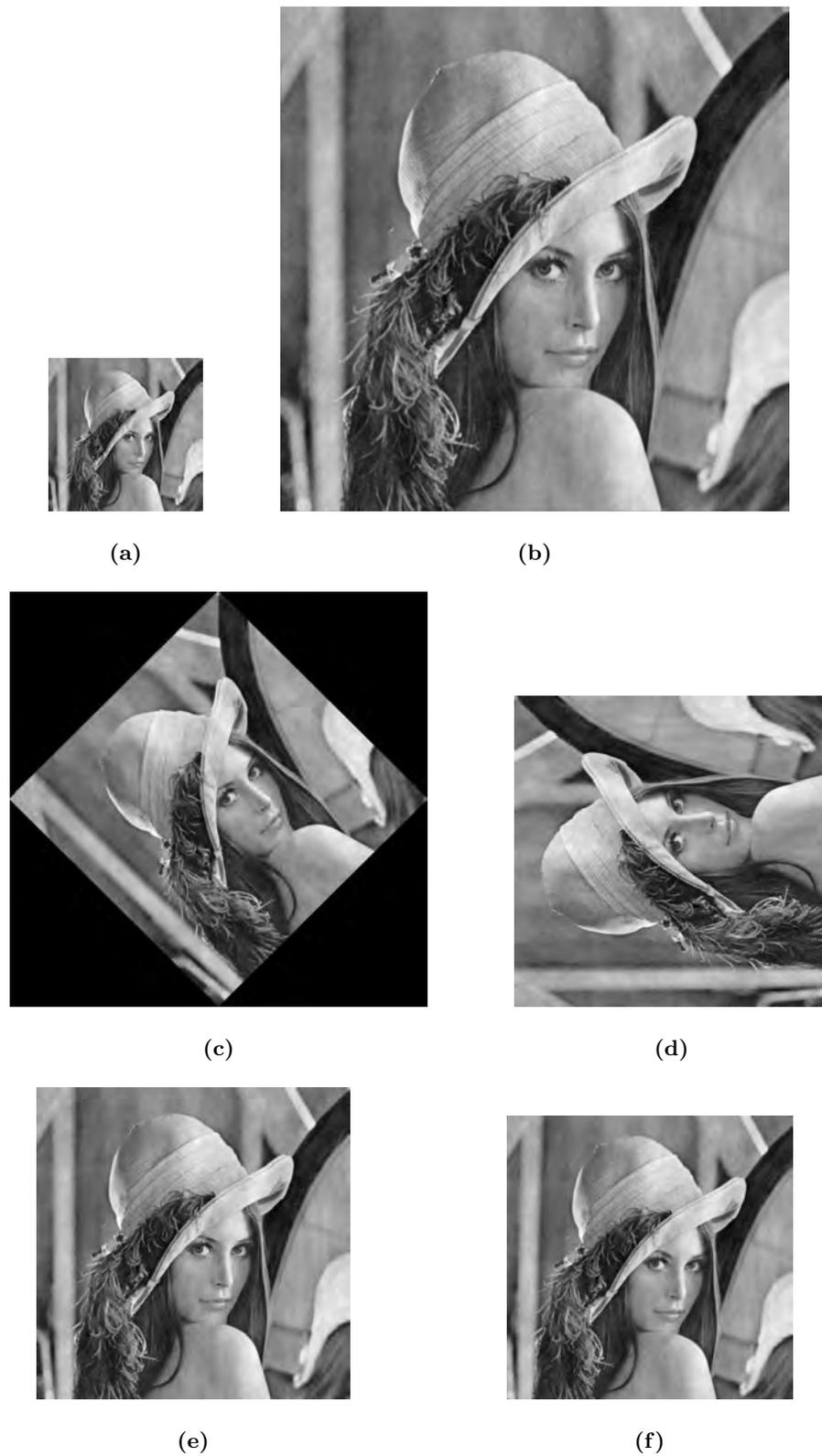


Figura 5.11: Ataques geométricos. Escalamiento sin pérdida (a) 50 % ( $256 \times 256$ ) y (b) 200 % ( $1024 \times 1024$ ). Rotación sin pérdida (c)  $-45^\circ$  ( $723 \times 723$ ) y (d)  $-90^\circ$  ( $512 \times 512$ ). Rotación con pérdida (e)  $-0.25^\circ$  ( $512 \times 512$ ) y (f)  $2^\circ$  ( $496 \times 496$ ).

## 5.4. Comparación de Resultados

Para mostrar más claramente el desempeño del esquema propuesto en esta tesis, se compararon los resultados con los obtenidos con el esquema de Lin *et al.* [Lin01]. Dicho esquema está basado en LPM y es uno de los algoritmos que han reportado mayor robustez ante diferentes distorsiones, incluyendo ataques de RST (ver Sección 3.3). Para mostrar los resultados del esquema de Lin, se utilizó el umbral de detección sugerido por los autores, 4.5, con el cual se logra una probabilidad de falsos positivos cercana a cero. Se evitaron marcar los coeficientes dentro de una ventana de longitud 5 alrededor de los coeficientes mayores y se aplicó un filtro de diferencias para mejorar la respuesta del proceso de detección.

En todos los experimentos reportados en esta sección, se asignó un valor de 1.3 al parámetro  $\alpha$  en el proceso de inserción del esquema propuesto en esta tesis, con el cual se logra buena robustez y se conserva una calidad satisfactoria de las imágenes marcadas.

### 5.4.1. Distorsión de las imágenes marcadas

Una característica importante en los esquemas de marcas de agua es la conservación de la calidad de las imágenes marcadas. Para este experimento se marcaron 1000 imágenes de origen diverso con ambos esquemas, y se midió su valor de PSNR.

En el histograma de la Figura 5.12 se puede observar que, en general, el esquema propuesto en esta tesis causa menos distorsión en las imágenes marcadas (mayores valores de PSNR), comparado con el esquema de Lin.

### 5.4.2. Casos de estudio

A continuación se presentan los resultados de diversas pruebas con ataques geométricos combinados, es decir, aplicando escalamiento, rotación y traslación, a las imágenes marcadas con ambos esquemas, las cuales se muestran en las Figuras 5.13(a)-(f). Note que el valor de PSNR que se obtuvo de las tres imágenes marcadas con el esquema propuesto en esta tesis es superior al obtenido de las imágenes marcadas con el algoritmo de Lin.

Los resultados de este experimento se muestran en la Tabla 5.3. Las detecciones debajo del umbral establecido para cada esquema están resaltadas en letras negritas.

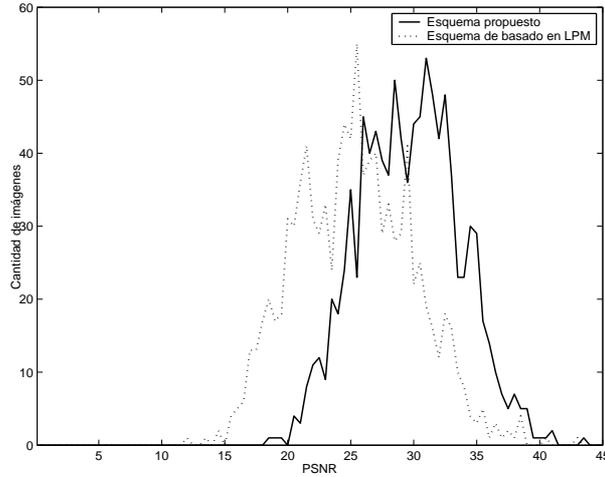


Figura 5.12: Comparación de la distorsión causada por los procesos de inserción.

Tabla 5.3: Casos de estudio.

$\phi$  = ángulo de rotación (grados).  $\sigma$  = factor de escala.

$T_x$  = traslación horizontal.  $T_y$  = traslación vertical.

| # | Pruebas |          |        |        | Esquema de Lin |             |             | Esquema propuesto |             |       |
|---|---------|----------|--------|--------|----------------|-------------|-------------|-------------------|-------------|-------|
|   | $\phi$  | $\sigma$ | $T_x$  | $T_y$  | Pimientos      | Lena        | Barco       | Pimientos         | Lena        | Barco |
| 1 | 45.5,   | 1.0,     | 50.0,  | 50.0,  | <b>0.34</b>    | <b>0.33</b> | <b>0.35</b> | 9.56              | <b>9.08</b> | 9.55  |
| 2 | 10.5,   | 0.7,     | 100.0, | 100.0, | <b>0.32</b>    | <b>0.35</b> | <b>0.32</b> | 14.49             | 11.91       | 10.75 |
| 3 | 25.5,   | 1.2,     | 100.0, | 0.0,   | <b>0.38</b>    | <b>0.36</b> | <b>0.34</b> | 10.62             | 13.73       | 11.52 |
| 4 | 25.5,   | 1.0,     | 0.0,   | 0.0,   | <b>0.44</b>    | <b>0.40</b> | <b>0.40</b> | 12.61             | 13.42       | 14.38 |
| 5 | 5.5,    | 1.0,     | 0.0,   | 0.0,   | 0.46           | <b>0.42</b> | <b>4.2</b>  | 20.83             | 21.75       | 25.40 |
| 6 | 0.5,    | 1.0,     | 0.0,   | 0.0,   | 0.52           | 0.47        | 0.44        | 24.11             | 25.47       | 25.40 |
| 7 | 20.0,   | 0.7,     | 0.0,   | 0.0,   | 0.72           | 0.72        | 0.72        | 11.27             | 14.74       | 11.87 |
| 8 | 45.5,   | 1.5,     | 0.0,   | 0.0,   | <b>0.42</b>    | <b>0.42</b> | <b>0.37</b> | <b>8.85</b>       | <b>9.29</b> | 9.93  |
| 9 | 2.5,    | 1.5,     | 0.0,   | 0.0,   | 0.52           | 0.47        | 0.50        | 18.67             | 19.96       | 13.14 |

En las primeras cuatro pruebas se obtuvo una sola falla con el esquema propuesto en esta tesis. En contraste, en las mismas pruebas, se encontraron fallas en todas las detecciones realizadas con el esquema basado en LPM. En la pruebas se obtuvieron detecciones erróneas con el esquema de Lin en la imagen de Lena y Barco, mientras el esquema propuesto tuvo un desempeño libre de fallas. En la prueba 8 el esquema de Lin falló en todas las imágenes, mientras el esquema basado en AG fue capaz de detectar la marca en Barco.

La dispersión de la marca de agua en el dominio de Fourier, dependiendo de la contribución de cada coeficiente en el mapa log-polar, hace que el esquema de Lin sea vulnerable a ciertas rotaciones, como en las primeras cuatro pruebas.

Por otro lado, la pérdida de información en la DFT, debida a la rotación [Lin01] y escalamiento, es la causa de las fallas en la detección usando el esquema propuesto en esta tesis; específicamente en las pruebas 1 y 8.

### 5.4.3. Comparación de tiempos

Puesto que para algunas aplicaciones es importante conocer el tiempo de cómputo necesario para que un esquema de detección reporte la presencia o ausencia de una marca de agua, se realizó una comparación de tiempos entre ambos esquemas, utilizando las tres imágenes estándares. Para este experimento se utilizó una computadora con un procesador Centrino a 1.4 GHz y 512 Mb de RAM.

El esquema de Lin es mucho más rápido. Debido a que las tres imágenes tienen dimensiones iguales ( $256 \times 256$ ), el esquema de detección, reportó un resultado en 1.65 segundos. En contraste, en las tres imágenes, el esquema propuesto en esta tesis requirió 1838.25 segundos (31.3 minutos) para evaluar la población inicial, y 15 segundos para evaluar cada una de las generaciones restantes, es decir, se requieren aproximadamente 34 minutos para conocer el mejor individuo de la decimoquinta generación.

Con los resultados que aquí se presentan se puede concluir que el esquema de Lin genera imágenes marcadas con menor calidad y menos robustas a ciertos ataques de RST, pero el tiempo que se requiere en la detección es mucho menor. Por otro lado, el esquema propuesto en esta tesis genera imágenes marcadas con mejor calidad y más robustas a ataques de RST, pero el tiempo de cómputo necesario en el proceso de detección resulta costoso.



(a)



(b)



(c)



(d)



(e)



(f)

Figura 5.13: Imágenes marcadas con el esquema propuesto en esta tesis y el basado en LPM. Imágenes marcadas con el esquema propuesto en esta tesis: (a) PSNR = 30.72, (c) PSNR=32.56 y (e) PSNR=35.94. Imágenes marcadas con el esquema de Lin: (b) PSNR = 28.74, (d) PSNR = 29.03 y (f) PSNR = 28.29.



## Capítulo 6

# Conclusiones

### 6.1. Conclusiones Generales

En esta tesis se presentó una nueva estrategia para resolver los problemas de sincronización en los esquemas de marcas de agua, la cual supera algunas de las debilidades encontradas en las estrategias propuestas anteriormente.

Se propuso un filtro para mejorar la detección, que denominamos SBD-WF, el cual supera los resultados alcanzados por Depovere [Depovere98] y Cox *et al.* [Cox02], con un costo computacional menor al del filtro bidimensional, no separable, propuesto por Cox.

La estrategia propuesta en esta tesis no utiliza patrones para restablecer la sincronización, los cuales son fácilmente removidos por ataques de colusión y filtros especializados, como los propuestos en [Craver00, Ergün99, Herrigel01, Licks03].

Se diseñó un esquema de marcas de agua simple para mostrar el desempeño de la estrategia propuesta en esta tesis ante ataques estándares (utilizando Stirmark 4.0). En estos resultados se mostró que el esquema es robusto a compresión con pérdida, filtros de mediana, de corrección de nitidez y binomiales, así como remoción de líneas, ataques de rotación, traslación y escalamiento. Además, se comparó el desempeño del esquema propuesto en esta tesis con el algoritmo de Lin *et al.* [Lin01], basado en LPM. Se presentaron casos de estudio en donde el esquema propuesto en esta tesis soporta ataques geométricos más severos que el esquema basado en LPM.

## 6.2. Trabajo Futuro

El esquema diseñado para implementar la estrategia propuesta en esta tesis utiliza un proceso de inserción simple, basado en SS, y los resultados fueron satisfactorios. Sin embargo, creemos que es posible mejorar el desempeño del esquema utilizando un proceso de inserción informado como el propuesto en [Chen00].

Se requieren futuras contribuciones sobre algoritmos en procesamiento de imágenes para extraer características robustas a ataques geométricos. Es posible implementar la estrategia propuesta en esta tesis en regiones robustas de la imagen para soportar ciertos ataques geométricos locales y reducir significativamente el costo computacional de la detección.

Una futura contribución podría incluir la estrategia de detección presentada en esta tesis en un esquema de marcas de agua semi-frágiles robusto a transformaciones de semejanza, los cuales podrían ser de utilidad en diferentes áreas como la medicina, astronomía, etc.

# Referencias

- [Alghoniemy00] Alghoniemy, M. y Tewfik, A. H. Geometric distortion correction through image normalization. *En IEEE International Conference on Multimedia and Expo (III)*, págs. 1291–1294. 2000.
- [Anand98] Anand, D. y Niranjana, U. C. Watermarking medical images with patient information. *En IEEE/EMBS Conference*, págs. 7003–706. Hong Kong, China, Oct. 1998.
- [Anastassopoulos02] Anastassopoulos, G. K. y Skodras, A.Ñ. Jpeg2000 roi coding in medical imaging applications. *En 2nd IASTED Int. Conf. on Visualisation, Imaging and Image Processing (VIIP2002)*, págs. 9–12. Malaga, España, Sep. 2002.
- [Bas02] Bas, P., Chassery, J., y Macq, B. Geometrically invariant watermarking using feature points, 2002.
- [Bloom99] Bloom, J. A., Cox, I. J., Kalker, T., Linnartz, J., y Miller, B. L. Copy protection for dvd video. *En Proceedings of the IEEE*, tomo 87. Jul. 1999.
- [Bravo03] Bravo, S. y Herrera, J. C. Esquema de marcas de agua frágiles aplicado sobre imágenes biomédicas. *En 2º Congreso Iberoamericano de Seguridad Informática, CIBSI'03*, págs. 120–135. Mexico D.F., Mexico, Oct. 2003.
- [Brown92] Brown, L. G. A survey of image registration techniques. *ACM Computing Surveys*, 24(4):325–376, 1992.

- [Chen00] Chen y Wornell. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding (1 page). *En ISIT: Proceedings IEEE International Symposium on Information Theory, sponsored by The Information Theory Society of The Institute of Electrical and Electronic Engineers*. 2000.
- [Coatrieux01] Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., y Collorec, R. Relevance of watermarking in medical imaging, 2001.
- [Cox97] Cox, I., Kilian, J., Leighton, T., y Shamoon, T. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 1997.
- [Cox02] Cox, I. J., Miller, M. L., y Bloom, J. A. *Digital Watermarking*. Morgan Kaufman, 1<sup>a</sup> ed<sup>ón</sup>., 2002.
- [Craver00] Craver, S., Periig, A., y Petitcolas, F. A. P. *Robustness of copyright marking systems*, cap. 7, págs. 149–174. Computer Security Series. Artech House, 1<sup>a</sup> ed<sup>ón</sup>., 2000.
- [deBurgós97] de Burgós, R. J. *Álgebra lineal*. McGraw-Hill, 1997.
- [Deguillaume02] Deguillaume, F., Voloshynovskiy, S., y Pun, T. A method for the estimation and recovering of general affine transform. US Patent Application, 2002.
- [Delannay01] Delannay, D., Delaigle, J., Macq, B. M., y Barlaud, M. Compensation of geometrical deformations for watermark extraction in digital cinema application. *En Proc. SPIE Vol. 4314, p. 149-157, Security and Watermarking of Multimedia Contents III, Ping Wah Wong; Edward J. Delp; Eds.*, págs. 149–157. 2001.
- [Delannay02] Delannay, D. y Macq, B. A method for hiding synchronization marks. in scale and rotation resilient watermarking schemes. *En SPIE Electronic*

- Imaging 2002, Security and Watermarking of Multimedia Contents IV.*, San José, CA. EE.UU.AA., Feb. 2002.
- [Depovere98] Depovere, G., Kalker, T., y Linnartz, J.-P. M. G. Improved watermark detection reliability using filtering before correlation. *En ICIP (1)*, págs. 430–434. 1998.
- [Devars99] Devars, J., Achard-Rouquet, C., y Bigorgne., E. Un detecteur de point carateristiques sur des images multispectrales. extension vers un detecteur subpixellique. *En GRETSI 99*, págs. 627–630. Sep. 1999.
- [Dong02] Dong, P. y Galatsanos, N. P. Affine transformation resistant watermarking based on image normalization. *En Proceedings of the IEEE International Conference on Image Processing (ICIP-02)*. Rochester, NY, EE. UU. AA., Sep. 2002.
- [Ergün99] Ergün, F., Kilian, J., y Kumar, R. A note on the limits of collusion-resistant watermarks. *En EUROCRYPT*, págs. 140–149. 1999.
- [Faugeras01] Faugeras, O., Luong, Q.-T., y Papadopoulou, T. *The Geometry of Multiple Images: The Laws That Govern The Formation of Images of A Scene and Some of Their Applications*. MIT Press, Cambridge, MA, EE. UU. AA., 2001. ISBN 0262062208.
- [Feng02] Feng, Y. y Izquierdo, E. Robust local watermarking on salient image areas. *En H. K. F.A.P. Petitcolas, ed., Digital Watermarking: First International Workshop, IWDW 2002*, págs. 180–201. Seúl, Korea, Nov. 2002.
- [Fleet97] Fleet, D. J. y Heeger, D. J. Embedding invisible information in color images. *En IEEE Signal Processing Society 1997 International Conference on Image Processing (ICIP'97)*. Santa Barbara, California, Oct. 1997.
- [Harris88] Harris, C. y Stephens, M. A combined corner and edge detector. *En Proceedings of the Fourth Alvey Vision Conference (Manchester University,*

- 31st August–2nd September*), págs. 147–152. The University of Sheffield Printing Unit, 1988.
- [Haupt98] Haupt, R. L. y Haupt, S. E. *Practical genetic algorithms*. John Wiley & Sons, Inc., Nueva York, NY, EE. UU. AA., 1998. ISBN 047-1188735.
- [Herrigel01] Herrigel, A., Voloshynovskiy, S., y Rytsar, Y. The watermark template attack. en Proc. SPIE Security and Watermarking of Multimedia Contents III, vol. 4314, pp. 394-405, San José, CA., 2001.
- [Kim02] Kim, B.-S., Choi, J.-G., y Park, K.-H. Image normalization using invariant centroid for rst invariant digital image watermarking. *En IWDWDigital Watermarking, First International Workshop, IWDW 2002, Seúl, Korea*, págs. 202–211. 2002.
- [Kundur97] Kundur, D. y Hatzinakos, D. A robust digital image watermarking scheme using the wavelet-based fusion. *En IEEE Signal Processing Society 1997 International Conference on Image Processing (ICIP'97)*. Santa Barbara, CA, EE. UU. AA., Oct. 1997.
- [Kutter98] Kutter, M. Watermarking resisting to translation, rotation and scaling. en Proc. SPIE Security and Watermarking of Multimedia Contents, Noviembre, 1998.
- [Kutter99] Kutter, M., Bhattacharjee, S., y Ebrahimi, T. Towards second generation watermarking schemes. *En Proceedings of the 6th International Conference on Image Processing (ICIP99)*, tomo 1, págs. 320–323. Oct. 1999.
- [Kutter00] Kutter, M. y Hartung, F. *Introduction to Watermarking Techniques*, cap. 5, págs. 97–120. Computer Security Series. Artech House, 1ª ed<sup>ón</sup>., 2000.
- [Licks03] Licks, V. y Jordan, R. Geometric attacks on image watermarking systems: A survey, Feb. 2003. Disponible en:  
<<http://www.eece.unm.edu/~vlicks/docs/survey.pdf>>.

- [Lin01] Lin, C.-Y., Wu, M., Bloom, J. A., Cox, I. J., Miller, M. L., y Lui, Y. M. Rotation, scale, and translation resilient watermarking for images. *IEEE Transactions on Image Processing*, 10(5):767–782, 2001.
- [Loo99] Loo, P. y Kingsbury, N. G. Digital watermarking using complex wavelets (trimmed version). Inf. téc., Department of Engineering, Cambridge University, Gran Bretaña, 1999.
- [Loo00] Loo, P. y Kingsbury, N. G. Digital watermarking using complex wavelets. *En ICIP*. 2000.
- [Miaou00] Miaou, S. G., Hsu, C., Tsai, Y. S., y Chao, H. M. Secure data hiding technique with heterogeneous data-combining capability for electronic patient records. *En IEEE-EMB, ed., World Congress on Medical Physics and Biomedical Engineering Session Electronic Healthcare Records*. Chicago, EE.UU.AA., Jul. 2000.
- [Minzer97] Minzer, F., Braudaway, G. W., y Yeung, M. M. Effective and ineffective digital watermarks. *En IEEE ICIP'97*, tomo 3, págs. 9–12. Santa Barbara, CA, EE. UU. AA., Oct. 1997.
- [O' Ruanaidh97] O' Ruanaidh, J. J. K. y Pun, T. Rotation, scale and translation invariant digital image watermarking. *En Proceedings of ICIP 97, IEEE International Conference on Image Processing*, págs. 536–539. Santa Barbara, CA, Oct. 1997.
- [Pei95] Pei, S.-C. y Lin, C.-N. Image normalization for pattern recognition. *Image Vision Comput.*, 13(10):711–723, 1995.
- [Pereira99a] Pereira, S., Ó Ruanaidh, J. J. K., Deguillaume, F., Csurka, G., y Pun, T. Template based recovery of fourier-based watermarks using log-polar and log-log maps. *En IEEE Multimedia Systems 99, International Conference on Multimedia Computing and Systems*, tomo 1, págs. 870–874. Florencia, Italia, 7-11 Jun. 1999.

- [Pereira99b] Pereira, S. y Pun, T. Fast robust template matching for affine resistant image watermarking, 1999.
- [Pereira00] Pereira, S. y Pun, T. An iterative template matching algorithm using the chirp-z transform for digital image watermarking. *Pattern Recognition*, 33(1):173–175, 2000.
- [Pereira01a] Pereira, S., Voloshynoskiy, S., y Pun, T. Optimal transform domain watermark embedding via linear programming. *Signal Process.*, 81(6):1251–1260, 2001.
- [Pereira01b] Pereira, S., Voloshynovskiy, S., Madueno, M., Marchand-Maillet, S., y Pun, T. Second generation benchmarking and application oriented evaluation. En I. S. Moskowitz, ed., *Information Hiding*, tomo 2137 de *Lecture Notes in Computer Science*, págs. 340–353. Springer, 2001.
- [Petitcolas98] Petitcolas, F. A. P., Anderson, R. J., y Kuhn, M. G. Attacks on copyright marking systems. En *Information Hiding*, págs. 218–238. 1998.
- [Petitcolas99] Petitcolas, F. A. P. y Anderson, R. J. Evaluation of copyright marking systems. En *IEEE Multimedia Systems (ICMCS'99)*, págs. 574–579. Florencia, Italia, Jun. 1999.
- [Petitcolas00] Petitcolas, F. A. P. Watermarking scheme evaluation. *IEEE Signal Processing*, 17(5):58–64, Sep. 2000.
- [Smith95] Smith, S. M. y Brady, J. M. SUSAN – A new approach to low level image processing. Inf. téc., Chertsey, Surrey, Gran Bretaña, 1995.
- [Tang03] Tang, C.-W. y Hang, H.-M. A feature-based robust digital image watermarking scheme. *Signal Processing*, 51(4):950–959, Abr. 2003.
- [vanSchyndel94] van Schyndel, R. G., Tirkel, A. Z., y Osborne, C. F. A digital watermark. En *International Conference on Image Processing*, tomo 2, págs. 86–90. Austin, TX, EE. UU. AA., 1994.

- 
- [Zelniker93] Zelniker, G. y Taylor, F. J. *Advanced Digital Signal Processing: Theory and Applications*. Marcel Dekker, Inc., Nueva York, NY, EE. UU. AA., 1993. ISBN 0824791452.
- [Zheng03] Zheng, D., Zhao, J., y Saddik, A. E. Rst-invariant digital image watermarking based on log-polar mapping and phase correlation. *IEEE Trans. Circuits Syst. Video Techn.*, 13(8):753–765, 2003.



# Glosario

**AG** (Algoritmo Genético) Técnica de optimización basada en la evolución natural.

**Ataque accidental-** Ataques que se aplican a una imagen marcada sin el propósito de eliminar la marca de agua. La compresión con pérdida, y algunos filtros se consideran ataques accidentales.

**Ataque de colusión-** Propuesto en [Craver00, Ergün99]. Consiste en promediar un conjunto de imágenes protegidas iguales que contienen marcas de agua diferentes, eliminando así cualquier información oculta.

**Ataque de mosaico-** Consiste en dividir una imagen en fragmentos pequeños, que pueden ser fácilmente acomodados por un navegador de Internet para simular la imagen completa.

**Ataque geométrico compuesto-** Aplicación de más de un ataque geométrico en una misma imagen.

**Ataque geométrico global-** Distorsiones geométricas que se aplican a toda la imagen.

**Ataque geométrico local-** Distorsiones geométricas que se aplican a una o más regiones dentro de una imagen.

**Ataque incidental-** Ataques que se aplican a una imagen marcada con el propósito de modificar o eliminar la marca de agua que contiene.

**Ataque-** Distorsiones aplicadas a una imagen marcada. *véase* Ataque accidental e incidental.

**AWGN** por las siglas del término en inglés: Additive White Gaussian Noise (ruido aditivo blanco Gaussiano).

**CSS** por las siglas del término en inglés: Curvature Scale-Space (curvatura de escala-espacio).

**CWT** por las siglas del término en inglés: Complex Wavelet Transform (transformada wavelets compleja).

**DFT** por sus siglas del término en inglés: Discrete Fourier Transform (transformada discreta de Fourier).

**Distorsión bilineal-** Distorsión que se utiliza para afectar la sincronización de los esquemas de marcas de agua, la cual consiste en desplazar las esquinas de una imagen en cantidades aleatorias.

**Distorsión radial-** Distorsión que modela el efecto de los lentes en la adquisición de imágenes.

**DVD** Disco Versatil Digital.

**Esteganografía-** Transmisión de información que se oculta en datos que no levantan sospechas en posibles receptores intermedios.

**Falso negativo-** Es cuando un detector reporta una imagen como no marcada, cuando en realidad sí lo está.

**Falso positivo-** Es cuando un detector reporta una imagen como marcada, cuando en realidad no lo está.

**Filtro pasa-bajas-** Procesamiento que se utiliza para eliminar frecuencias medias y altas de una señal.

**IDFT** por las siglas del término en inglés: Inverse Discrete Fourier Transform (transformada discreta de Fourier inversa).

**ILPM** por las siglas del término en inglés: Inverse Log-Polar Mapping (proyección log-polar inversa).

**Imagen original-** Imagen sin marcar.

**Imagen protegida-** Imagen marcada.

**Inserción ciega-** *véase* Inserción privada.

**Inserción informada-** Método de inserción en donde se diseña una marca de agua tomando en cuenta las características particulares de la imagen a marcar.

**Inserción informada-** Proceso de inserción que utiliza las características de la imagen para insertar una marca de agua más robusta y/o menos perceptible.

**Inserción no ciega-** *véase* Inserción informada.

**Inserción privada-** Proceso de inserción que no analiza la imagen para insertar la marca de agua.

**Interpolación bilineal-** Método de interpolación comúnmente utilizado en imágenes digitales, en donde se calcula el valor de un píxel con coordenadas no enteras, utilizando pesos en cuatro píxeles vecinos.

**LPM** por las siglas del término en inglés: Log-Polar Mapping (proyección a un mapa Log-Polar). La principal propiedad de un mapa log-polar es que la rotación y escalamiento en el dominio espacial son simples traslaciones en el dominio log-polar.

**Marca de agua frágil-** Esquema utilizado con fines de autenticación, diseñado para insertar marcas de agua que se modifiquen o destruyan cuando la imagen protegida sufre cualquier distorsión.

**Marca de agua semi-frágil-** Esquema utilizado con fines de autenticación. A diferencia de una marca de agua frágil, una marca de agua semi-frágil se diseña para soportar distorsiones que no afectan la calidad o información de la imagen, y destruirse ante cualquier otro tipo de distorsión.

**Pérdida de sincronización-** Ocasionada principalmente al aplicar ataques geométricos a una imagen marcada, los cuales no destruyen la marca de agua, pero cambian su posición a una localidad desconocida para el detector.

**Proceso de detección-** Proceso en donde se trata de detectar una marca de agua en una señal digital analizada.

**Proceso de extracción-** Proceso especialmente utilizado en los esquemas con detección ciega, en donde se trata de extraer una marca de agua de una señal digital analizada.

**Proceso de inserción-** Proceso en donde se oculta una marca de agua en una señal digital.

**PSNR** por las siglas del término en inglés: Peak Signal-to-Noise Ratio (relación mayor de señal a ruido). Medida utilizada para comparar la distorsión causada por diferentes esquemas de marcas de agua.

**RST** por las siglas de los términos en inglés: Rotation, Scaling and Rotation (rotación, escalamiento y rotación).

**SBD-WF** por las siglas del término en inglés: Separable Bidirectional Difference-Whitening Filter. ver *Whitening filter*.

**SS** por las siglas del término en inglés: Spread Spectrum (espectro esparcido). Técnica de comunicación que consiste en transmitir información por un canal, utilizando una secuencia secreta de frecuencias, las cuales son parte de un espectro amplio.

**Transformación proyectiva-** Transformación lineal que proyecta una imagen en un plano diferente. Esta transformación no necesariamente conserva el paralelismo de las imágenes.

**Transformación afín-** Transformación lineal que se caracteriza por conservar el paralelismo y el centro de masa de las imágenes.

**Transformación de semejanza-** Transformación lineal que se caracteriza por conservar los ángulos y la relación de distancia de los objetos dentro de una imagen.

**Transformación Euclidiana-** Transformación lineal que se caracteriza por conservar las distancias de los objetos dentro de una imagen.

**Whitening filter-** Nombre en inglés por el que se conoce a los filtros que se utilizan eliminar la auto-correlación existente en una señal, con el objeto de mejorar la detección en algunos esquemas de marcas de agua.



# Índice

- AG, 47, 48, 50, 51, 53–56, 73
- Algoritmo genético, 47
- Algoritmo genético binario, 47
- Algoritmo genético continuo, 47
- Apareamiento, 48
- Aplicaciones lineales, 15, 53
- Ataque geométrico compuesto, 39, 40, 43
- Ataque geométrico simple, 40, 42
- Ataques
  - accidentales, 9–12
  - adición de ruido, 12–14, 64, 65
  - cambio de formato, 9, 10, 12
  - colusión, 2–4, 9–11, 17, 18, 46, 48, 77
  - compresión, 4, 9, 10, 12–14, 20, 33, 63, 64, 77
  - conversión A/D y D/A, 9, 10
  - corrección de color, 9
  - corrección de contraste, 9, 10
  - corrección de nitidez, 10, 65, 67, 68, 77
  - distorsión bilineal, 15
  - distorsión radial, 15
  - eliminación de líneas, 13, 65, 66
  - filtro binomial, 65, 67, 68, 77
  - filtro de mediana, 10, 13, 65, 67, 68, 77
  - filtros óptimos *véase* filtros especializados, 17
  - filtros especializados, 2–4, 46, 48, 77
  - geométricos, 1, 3, 12, 14, 16, 17, 19–21, 40, 42, 43, 46, 71, 72, 77, 78
  - geométricos globales, 16
  - geométricos locales, 16
  - incidentales, 9–11
  - mosaico, 9, 10
  - RST, 2–4, 19, 20, 23, 27, 29, 31, 33, 41, 46, 48, 72, 74
  - ruido aditivo *véase* adición de ruido, 9, 10
  - ruido multiplicativo, 9
  - tipos de, 10
- Autenticación de imágenes, 12
- Auto-correlación, 18
- Auto-restauración, 48
- Auto-sincronización, 18, 45
- AWGN, 38, 54, 55
  
- Búsqueda exhaustiva, 16, 45, 47
- Bordes de las imágenes, 28
  
- Centroide invariante, 19
- Checkmark, 13
- Cizallamiento, 15, 18
- Comparación de tiempos, 74
- Componente de fase, 24
- Contribuciones, 45
- Correlación, 29, 38, 46, 50, 54, 55, 64, 67
- Costo, 48, 53
- Cromosoma, 48, 51, 52
- CSS, 21
- Curvatura de escala-espacio, 21
- CWT, 19
  
- dB, 12, 62
- DCT, 10
- Derechos de autor, 11
- Descenso de gradiente, 47
- Detector de bordes
  - Achard-Rouquet, 20
  - Harris, 20
  - SUSAN, 20
- DFT, 10, 23, 36, 69, 74
- Discretización, 20, 28, 41, 46, 48, 52

- Distorsión bilineal, 15  
 Distorsión radial, 15  
 Distribución elíptica Gaussiana, 54  
 Distribución Gaussiana, 38, 49  
 Dominio invariante, 19, 46, 48  
 Dominio semi-invariante, 19, 46, 48  
 DVD, 11  
 DWT, 10
- Escalamiento, 15, 69  
 Espectro esparcido, 46  
 Esquemas de marcas de agua  
   auto-sincronización, 2, 18, 45  
   búsqueda exhaustiva, 16, 45, 47  
   dominio invariante, 2, 19, 46  
   dominio semi-invariante, 2, 19, 46  
   extracción de características, 3, 20, 46  
   patrones de sincronización, 17, 45  
 Esteganografía, 62  
 Extracción de características, 3, 20, 46
- Falsos negativos, 13, 61, 69  
 Falsos positivos, 13, 61  
 Filtro bidimensional de diferencias separable, 55  
 Filtro binomial, 65, 67, 68, 77  
 Filtro de corrección de nitidez, 67, 68  
 Filtro de mediana, 10, 13, 65, 67, 68, 77  
 Filtro para mejorar la correlación, 54, 59  
 Filtro pasa-bajas, 28, 40, 41  
 Formación de parejas, 48  
 Fourier-Mellin, 2, 4, 19, 23, 27–29, 31, 32, 41  
 Función de mezclado, 36
- Gen, 47, 48, 51  
 Generación, 48, 51, 53, 56
- IDFT, 28, 29, 36, 49, 50  
 ILPM, 27–29, 31, 41  
 Individuo, 48, 51, 53, 56  
 Inserción de patrones, 48  
 Interpolación, 20, 25, 28, 34, 41, 46, 48  
 Interpolación bilineal, 34  
 Invariancia, 19, 50
- JPEG, 10, 13, 20, 63–65  
 JPEG2000, 13
- Log-log, 17  
 Log-polar, 17, 20, 23, 24, 27, 33–35, 37, 38  
 LPM, 25, 28, 31, 40, 41, 72, 73, 77
- Máximo global, 53  
 Máximos locales, 47  
 Magnitud de Fourier, 24, 27, 29, 33, 37, 46, 49, 50  
 Mapa log-polar, 20, 23, 24, 27, 33–35, 37, 38, 74  
   discusión, 28  
 Marca de agua, 8, 34, 38, 49  
 Marca de agua binaria, 49  
 Marcas de agua digitales  
   aplicaciones, 9, 11  
   definición, 1, 7  
   en audio, 7  
   en video, 7  
   evaluación, 12  
   frágiles, 12  
   general, 7  
   proceso de detección, 8  
   proceso de extracción, *véase* Proceso de detección  
   proceso de inserción, 8  
   requerimientos, 9  
   segunda generación, 20  
   semi-frágiles, 12  
 Marcas de agua frágiles, 12  
 Marcas de agua semi-frágiles, 12, 48, 78  
 Mutación, 48, 53
- Normalización de imágenes, 2, 19
- Objetivos de la tesis, 3
- Pérdida de sincronización, 1, 2, 4, 14, 16, 23  
 Patrones de sincronización, 17, 18, 45  
 Planteamiento del problema, 3  
 Población, 48, 53  
 Población inicial, 53  
 Población uniformemente distribuida, 53

- Proceso de detección
  - ciego, 8
  - general, 8
  - no ciego, 8
  - público, *véase* Proceso de detección ciego
  - privado, *véase* Proceso de detección no ciego
  - semi-ciego, 8
  - semi-privada, *véase* Proceso de detección semi-ciego
- Proceso de inserción
  - ciego, 8
  - general, 8
  - informado, 8, 36, 50
  - no ciego, *véase* Proceso de inserción informado
- Protección de copias, 11
- Proyección inversa log-polar, 27
- Proyección log-polar, 25
- PSNR, 12, 62, 72
- Rango dinámico, 67
- Rastreo de copias, 11
- Reflexión, 15
- Registro de imágenes, 1, 16, 46
- Reproducción, 53
- Revisión de esquemas, 23
- Robustez, 2, 3, 10, 11, 13, 14, 17–21, 23, 35, 40, 46, 49, 50
- Rotación, 15, 69
- RST, 2, 23, 29, 31, 33, 41, 46, 48, 72, 74
- Ruido blanco aditivo Gaussiano, 38
- Ruido Gaussiano, 38
- SBD-WF, 55, 56, 59–61, 77
- Semilla, 38
- Sincronización, 1–4, 14, 16, 17, 23, 24, 29, 45, 46, 48, 77
- Sistema visual humano, 13
- Sombrero mexicano, 20, 21
- SS, 46, 49
- Stirmark, 13, 20, 21, 62
- Teselado de Delaunay, 20
- Transformación afín, 2, 15
- Transformación de semejanza, 15
- Transformación Euclideana, 15
- Transformación proyectiva, 15
- Transformaciones lineales, 15
- Transformada
  - de cosenos discreta, 10
  - de Fourier discreta, 10, 23
    - propiedades, 23
  - de Fourier-Mellin, 19, 23, 27, 29, 31, 41
  - de Fourier-Mellin inversa, 28
  - de wavelets discreta, 10
  - discreta de Fourier inversa, 28
  - Hough/Radon, 18
  - log-log, 17
  - log-polar, 17
  - wavelets compleja, 19
- Traslación, 15
- Umbral, 36, 38, 48, 51, 56, 59–61, 64, 67, 69, 72
- Whitening filter, 38, 54