



**INSTITUTO POLITÉCNICO NACIONAL.**

---

---

**ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA.**

**SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN.**

**UNIDAD CULHUACAN.**

**“ESQUEMAS ROBUSTOS DE MARCA DE  
AGUA APLICADOS A IMAGENES  
DIGITALES”**

**T E S I S**  
QUE PARA OBTENER EL GRADO ACADÉMICO DE  
DOCTOR EN COMUNICACIONES Y ELECTRÓNICA  
PRESENTA  
M. EN C. MANUEL CEDILLO HERNÁNDEZ

**ASESOR: DRA. MARIKO NAKANO MIYATAKE.**



**MÉXICO, D.F. ENERO 2011**



Con agradecimiento  
y amor a  
Antonieta y Alejandra

Manuel Cedillo Hernández



## **Agradecimientos**

Al Instituto Politécnico Nacional, por toda mi formación recibida.

Un agradecimiento especial a la Dra. Mariko Nakano Miyatake y al Dr. Héctor Manuel Pérez Meana, por haber confiado en mí para el logro de este trabajo, haberlo guiado de principio a fin y por todo el apoyo brindado desde el comienzo.

A la Sección de Estudios de Posgrado e Investigación de la ESIME, Unidad Culhuacan, por brindarme la oportunidad de ser un miembro más de tan importante centro de estudios.

A los apoyos económicos por parte del Consejo Nacional de Ciencia y Tecnología (CONACYT) y del Programa Institucional de Formación de Investigadores (PIFI-SIP-IPN).

A mi esposa e hija, por su compañía, apoyo y tolerancia que me han brindado desde el principio de este trabajo.

A mi padre y a mi madre, por la unión que hay entre nosotros y por el apoyo que me han dado durante toda mi vida.

A mis hermanos, por sus consejos, su compañía y apoyo que me han brindado durante toda mi vida.

Finalmente, a todas mis amistades que me han acompañado a lo largo de estos años, por brindarme su confianza y amistad.



## **Resumen**

En este trabajo se proponen tres métodos de marca de agua robustos a distorsiones geométricas y otros tipos de procesamiento de señales. El primer método está aplicado a imágenes en escala de grises y hace uso de una técnica de normalización de imágenes para obtener características invariantes de la imagen ante las distorsiones geométricas. Los procesos de inserción y detección de la marca de agua son realizados en el dominio de la Transformada Discreta del Coseno (DCT). Una clasificación de texturas basada en el dominio de la DCT es usada para clasificar cada bloque de la imagen a fin de poder insertar una marca de agua fuerte, manteniendo al mismo tiempo la imperceptibilidad de la misma. El método propuesto es de tipo público, en el cual, la imagen original no está disponible en el proceso de detección de la marca de agua. Los resultados experimentales muestran la imperceptibilidad de la marca de agua y su robustez ante las distorsiones geométricas, como son rotación, escalamiento, transformaciones Affine, y otros tipos de procesamiento de señales, tales como compresión JPEG, contaminación de imagen por ruido Gaussiano e impulsivo.

El segundo esquema propuesto está aplicado en imágenes a color. Está basado en dos modificaciones realizadas a histogramas de dos dimensiones (2D) obtenidos de la imagen. En la primera modificación, una región del histograma en dos dimensiones compuesto por las componentes de color rojo y verde (R-G) obtenidas de la imagen, es modificada de acuerdo al patrón de marca de agua. En la segunda modificación, un histograma en dos dimensiones compuesto por la componente de color azul (B) y la componente de color rojo filtrada (R) es particionado dinámicamente para insertar el

patrón de marca de agua. Los resultados experimentales muestran la robustez del método ante diversas distorsiones geométricas, operaciones comunes de procesamiento de señales y algunos ataques combinados. También se realiza la comparación con métodos reportados previamente que muestra un mejor comportamiento de los métodos propuestos.

El tercer método está aplicado a imágenes en escala de grises. Inicialmente, la imagen original es normalizada por medio de un proceso de normalización de imágenes y posteriormente se extraen los puntos característicos de la imagen normalizada aplicando un detector de esquinas de Harris. Así mismo, se obtienen los puntos característicos más estables y son usados para generar diversas regiones circulares no superpuestas. Para obtener una mejor imperceptibilidad de la marca de agua, se utiliza un clasificador de texturas de imagen basado en la DCT. La marca de agua es insertada y detectada dentro de las regiones clasificadas por medio del dominio DCT. En el detector la marca de agua puede ser obtenida sin hacer uso de la imagen original. Los resultados experimentales muestran la robustez de la marca de agua ante distorsiones geométricas tales como rotación, escalamiento y diversas transformaciones Affine, así como procesamientos de señales comunes como la compresión JPEG y la contaminación por ruido.

## **Abstract**

In this thesis, three image watermarking methods are proposed, which are robust against geometric distortions and common signal processing. The first method is applied to grayscale images and image normalization is used to get geometric invariant feature and watermark embedding and detection are carried out in the Discrete Cosine Transform (DCT) domain. Texture based image block classification in DCT domain is also used to get major watermark imperceptibility and robustness. The proposed watermarking scheme is a public watermarking, where the original image is not available in the watermark detection stage. The experimental results show the watermark imperceptibility and robustness against geometric distortion such as rotation, scaling and various other Affine Transformation, and common signal processing attacks, such as JPEG compression and noise contamination.

The second method is applied to color images, which is based on two modifications introduced in the 2D histograms. In the first modification, a selected region of 2D histogram composed by red and green (R-G) color components is modified according to the watermark pattern. In the second modification, another 2D histogram composed by blue (B) component and filtered red (R) component is dynamically partitioned to embed the watermark pattern. The experimental results show robustness against several geometric distortions, common signal processing operations and some combined attacks. Also, the comparison with the previously reported methods shows the better performance of the proposed methods.

Finally, the third method presents a robust image watermarking method against geometric distortions and several attacks of signal processing. Initially, the original image is normalized and the feature points are then extracted. Furthermore, the locally most stable feature points are obtained and used to generate several non-overlapped circular regions. Texture-based image block classification in Discrete Cosine Transform (DCT) domain is also used to get watermark imperceptibility. The watermark is embedded and extracted into classified regions using the DCT domain. In the detector stage, the watermark can be obtained without the original image. The experimental results show the watermark robustness against geometric distortion such as rotation, scaling and various other Affine Transformation, and common signal processing attacks, such as JPEG compression and noise contamination.

---

---

## Prefacio

*El Propietario de Derechos de Autor de información en forma digital necesita, para obtener una justa remuneración económica por la información que produce, de medios tecnológicos adecuados que permitan la autenticación de dicha información, así como el seguimiento de copias ilegalmente distribuidas.*

*En plena era de la información, las posibilidades que brinda Internet como medio de comunicación ha permitido a los autores que tiene su información en forma digital a utilizar Internet para promocionar, publicar y difundir sus obras. Cualquier usuario, desde su casa y de una manera muy fácil puede acceder a estas obras intelectuales en cuestión de segundos.*

*La posibilidad de digitalización de cualquier tipo de información (imágenes, vídeo, audio, texto, etc.) junto con la existencia de Internet permite realizar copias perfectas de la información digitalizada. Los procesos criptográficos permiten proteger la adquisición legal de la información, pero una vez obtenida la información se pueden revender copias exactas. Por lo tanto, surge la necesidad de un sistema de seguimiento de copias para la protección de los Derechos de Autor, que también se utilice en el caso de adquisición legal para distribución fraudulenta (copias ilegales).*

*Ante estos riesgos, legislar resulta insuficiente, y por ello se debe hacer uso de otros mecanismos que aseguren y protejan derechos fundamentales como es el derecho de propiedad intelectual. Las marcas de agua digitales han sido propuestas como una solución eficiente para la protección de los derechos de copia y propiedad de los archivos de datos multimedia, posibilitando la identificación de la fuente, autor, propietario, distribuidor o consumidor autorizado, de imágenes digitales, grabaciones de audio o video.*

---

*La principal ventaja de los sistemas de marca de agua consiste en que la marca es inseparable del contenido del archivo. Sin embargo, existen algunas cuestiones que necesitan ser resueltas, antes de que estas técnicas puedan ser eficazmente aplicadas en los escenarios reales de trabajo.*

*El desarrollo de un sistema de marcas de aguas digitales requiere la particularización a un tipo de señal determinado, en el caso de esta Tesis el tipo de señal son imágenes digitales, teniendo en cuenta además, que una marca de agua debe ser robusta, no ambigua e imperceptible. Algunos esquemas de marcas de agua aplicados a imágenes digitales consideran ataques para comprobar la robustez de la marca de agua, como son el filtrado, contaminación por ruido y compresión JPEG, dichos esquemas suelen resultar robustos frente a la mayoría de los ataques descritos anteriormente.*

*Un problema que presenta la robustez de las marcas de aguas son los ataques que dan lugar a una interpolación de la señal digital que representa la información. En el caso de imágenes digitales, estos ataques pueden realizarse mediante rotación, traslación de un número no entero de píxeles, cambios de escala y recortes. Una distorsión geométrica en una imagen marcada provoca que se elimine la sincronización con la cual la marca de agua fue insertada originalmente. Esta pérdida de sincronización ocasiona errores en la detección de la marca de agua cuando se aplica el proceso de detección correspondiente. Por lo tanto, los ataques geométricos se consideran ataques agresivos ante los cuales es muy difícil que una marca de agua logre sobrevivir. Tomando en cuenta los hechos mencionados anteriormente, los ataques geométricos deben ser considerados de alta prioridad cuando se lleva a cabo el diseño de un algoritmo de marca de agua cuyo objetivo es proteger el derecho de autor y/o controlar la réplica o copias del material digital por personas no autorizadas.*

---

---

# Objetivo

**Proponer y evaluar técnicas de marca de agua digitales que logren resolver el problema de sincronización en la etapa de detección, proceso que se ve afectado por distorsiones geométricas en los esquemas de marca de agua.**

# Justificación

Hasta la fecha se han propuesto una gran cantidad de algoritmos de marca de agua aplicados a imágenes digitales, la gran mayoría de ellos garantizan robustez en contra de ataques tales como la compresión de imágenes usando el método JPEG, la contaminación de imágenes por ruido y el filtrado.

Sin embargo, pocos algoritmos consideran la robustez contra distorsiones o ataques geométricos, tales como la rotación, el escalamiento, recorte de imagen, cambios de aspecto, entre otros. Estos ataques o distorsiones geométricas pueden ser aplicados fácilmente usando herramientas de software, además que para un video digital, las distorsiones geométricas ocurren frecuentemente de una manera natural. Una distorsión geométrica en una imagen marcada provoca que se elimine la sincronización con la cual la marca de agua fue insertada originalmente.

Esta pérdida de sincronización ocasiona errores en la detección de la marca de agua cuando se aplica el proceso de detección correspondiente. Por lo tanto, los ataques geométricos se consideran ataques agresivos ante los cuales es muy difícil que una marca de agua logre sobrevivir.

---

Tomando en cuenta los hechos mencionados anteriormente, los ataques geométricos deben ser considerados de alta prioridad cuando se lleva a cabo el diseño de un algoritmo de marca de agua cuyo objetivo es proteger el derecho de autor y/o controlar la réplica o copias del material digital por personas no autorizadas.

Las debilidades identificadas en las estrategias reportadas en la literatura para resolver la sincronización de los esquemas de marcas de agua, hacen de este un campo abierto para nuevas contribuciones.

## Metas

Las metas que se llevarán a cabo en esta tesis son:

- Desarrollo de un primer esquema de marca de agua basado en normalización de imágenes y clasificación de texturas, orientado a imágenes en escala de grises.
- Desarrollo de un segundo esquema de marca de agua basado en modificación de histograma de dos dimensiones, orientado a imágenes de color.
- Desarrollo de un tercer esquema de marca de agua basado en la detección de puntos característicos de la imagen y normalización de imágenes, orientado a imágenes en escala de grises.
- Evaluación de desempeño de los esquemas propuestos desde un punto de vista de robustez, imperceptibilidad y no ambigüedad de marca de agua.
- Comparar los resultados de las estrategias propuestas con esquemas reportados en la literatura con anterioridad.

---

---

# Aportaciones

Las aportaciones que se generaron en los tres métodos de marca de agua de esta tesis son:

## **Esquema de marca de agua basado en normalización de imágenes y clasificación de texturas, orientado a imágenes en escala de grises.**

- *Implementación de un clasificador de texturas que mejora al mismo tiempo la imperceptibilidad y la robustez del método de marca de agua presentado.*
- *Aumento de la cantidad útil de marca de agua que permite la inserción de patrones pseudo-aleatorios y pequeños logotipos binarios en la imagen original, en comparación con métodos reportados con anterioridad.*
- *Incremento de la robustez de la marca de agua ante una mayor cantidad de distorsiones geométricas y de tipo procesamiento de señales.*

## **Esquema de marca de agua basado en modificación de histograma de dos dimensiones, orientado a imágenes de color.**

- *Implementación de una técnica de modificación de histogramas de dos dimensiones obtenidos del modelo RGB de la imagen original, que permite alterar los histogramas de una imagen de modo que esta modificación represente una secuencia de marca de agua binaria.*
- *Aumento de la cantidad útil de marca de agua en comparación con métodos reportados con anterioridad.*
- *Incremento de la robustez de la marca de agua ante distorsiones geométricas que involucran recortes de imagen, tales como rotación con recorte, recorte de imagen con y sin escalamiento, comparando los resultados con métodos reportados con anterioridad.*

## **Esquema de marca de agua basado en la detección de puntos característicos de la imagen y normalización de imágenes, orientado a imágenes en escala de grises.**

- *Implementación de una rutina que permite detectar los puntos característicos de Harris de una imagen que son invariantes al escalamiento de imagen y contaminación por ruido Gaussiano e impulsivo, distorsiones ante las cuales los puntos de Harris presentan sensibilidad.*
- *Implementación de un clasificador de texturas que mejora al mismo tiempo la imperceptibilidad y la robustez del método de marca de agua presentado.*
- *Incremento de la robustez de la marca de agua ante una mayor cantidad de distorsiones geométricas y de tipo procesamiento de señales.*

---

---

# Organización de Tesis

El primer capítulo contiene una revisión del estado del arte de las marcas de agua, conceptos básicos, algunas de sus aplicaciones y requerimientos.

El segundo capítulo comprende el marco teórico, se describen algunas de las distorsiones geométricas más comunes aplicadas a imágenes digitales y se hace una revisión bibliográfica acerca de las estrategias propuestas hasta ahora para resolver el problema de sincronización en los esquemas de marcas de agua digitales.

En el tercer capítulo, se realiza el desarrollo y la evaluación del desempeño de un esquema de marca de agua basado en normalización de imágenes y clasificación de texturas, orientado a imágenes en escala de grises. Se describen los procesos de inserción y detección del esquema propuesto, así como la comparación de los resultados con esquemas reportados anteriormente.

En el cuarto capítulo, se realiza el desarrollo y la evaluación del desempeño de un esquema de marca de agua basado en modificación de histograma de dos dimensiones, orientado a imágenes de color. Se describen los procesos de inserción y detección del esquema propuesto, así como la comparación de los resultados con esquemas reportados anteriormente.

En el quinto capítulo, se realiza el desarrollo y la evaluación del desempeño de un esquema de marca de agua basado en puntos característicos y normalización de imágenes, orientado a imágenes en escala de grises. Se describen los procesos de inserción y detección del esquema propuesto, así como la comparación de los resultados con esquemas reportados anteriormente.

---

En el sexto capítulo se comentan las conclusiones generales del trabajo y se menciona el trabajo a futuro correspondiente a cada estrategia propuesta.

# Contenido

## CAPITULO 1.

### **Marcas de agua en Imágenes Digitales.**

Introducción	1
1.1 Historia y Definición de Marca de Agua Digital	1
1.2 Requerimientos y Aplicaciones de Marca de Agua Digital	3
1.3 Tipos de Ataques	6
1.4 Evaluación de Esquemas de Marca de Agua.	9
Conclusiones	11

## CAPITULO 2.

### **Marco teórico.**

Introducción	13
2.1 Clasificación de los algoritmos robustos ante los ataques geométricos	15
2.1.1 Búsqueda exhaustiva	15
2.1.2 Inserción en el dominio invariante a RST	16
2.1.3 Re-sincronización de marca de agua usando "plantilla"	19
2.1.4 Uso de puntos característicos de la imagen para su sincronización	21
2.1.5 Uso de normalización de imágenes	24
2.1.6 Uso de histogramas como dominio invariante	25
2.2 Distorsiones geométricas	26
2.3 Momentos geométricos	29
2.3.1 Momentos simples	29
2.3.2 Momentos centrales	29
2.3.3 Momentos centrales normalizados	30
2.3.4 Momentos de orden 0	31
2.3.5 Momentos de orden 1	31
2.3.6 Momentos de orden 2	32
2.3.7 Momentos de orden 3	33
2.4 Transformada de Coseno Discreta	34
2.5 Modelo de color RGB	36
2.6 Histograma de dos dimensiones (2D)	38
2.7 Detector de esquinas de Harris	41
Conclusiones	42

## CAPITULO 3.

### **Técnica Robusta de Marca de Agua Basada en Normalización de Imágenes.**

3.1 Introducción	45
3.2 Normalización de imágenes	47
3.2.1 Momentos invariantes y procedimiento de normalización de imágenes	48
3.3 Proceso de inserción	56
3.4 Proceso de extracción	62
3.5 Resultados experimentales	63

3.5.1 Imperceptibilidad de la señal de la marca de agua	63
3.5.2 Ambigüedad de marca de agua extraída	69
3.5.3 Robustez de marca de agua	68
Conclusiones	75

## CAPITULO 4.

### **Esquema Robusto de Marca de Agua Basado en Modificación de Histograma.**

4.1 Introducción	77
4.2 Proceso de inserción	79
4.2.1 Modificación de histograma 2D R-G	80
4.2.2 Modificación de histograma 2D B-Rw filtrada	82
4.3 Proceso de detección	85
4.4 Resultados experimentales	86
4.4.1 Determinación de parámetros	87
4.4.2 Imperceptibilidad de Marca de Agua	92
4.4.2.1 Espacio de color CIELAB	92
4.4.2.2 Cambio de color en la imagen	93
4.4.2.3 Diferencia de Color Normalizada (NCD)	96
4.4.2.4 Fidelidad de la Información Visual (VIF)	97
4.4.3 Robustez de marca de agua	99
4.4.4 Capacidad del Detector	104
Conclusiones	106

## CAPITULO 5.

### **Esquema Robusto de Marca de Agua Basado en Puntos Característicos y Normalización de Imagen.**

5.1 Introducción	109
5.2 Trabajos relacionados	110
5.3 Detector de esquinas de Harris	112
5.4 Normalización de imágenes	113
5.5 Selección de puntos característicos invariantes	113
5.6 Proceso de inserción	115
5.7 Proceso de detección	118
5.8 Resultados experimentales	119
5.8.1 Imperceptibilidad de marca de agua	119
5.8.2 Robustez de marca de agua	120
Conclusiones	121

## CAPITULO 6.

### **Conclusiones Generales y Trabajo a Futuro.**

6.1 Conclusiones generales	123
6.2 Trabajo a futuro	126

## Referencias

129



# Lista de Figuras y Tablas

## CAPITULO 1.

### Marcas de Agua en Imágenes Digitales.

- Figura 1.1** Diagrama a bloques de un esquema de marca de agua general. 3
- Figura 1.2.** Dependencia mutua entre requerimientos básicos de marca de agua. 5
- Tabla 1.1** Ataques contemplados en Stirmark Benchmark 4.0 11

## CAPITULO 2.

### Marco teórico.

- Figura 2.1.** Esquema general de inserción de marca de agua en un dominio invariante. 17
- Figura 2.2.** Esquema general de inserción de marca de agua basado en el uso de "plantilla". 20
- Figura 2.3.** Esquema general de inserción de marca de agua basado en el uso de puntos característicos. 22
- Figura 2.4.** (a) Imagen original. (b) Reflexión. (c) Traslación. (d) Rotación. (e) Shearing. (f) Escalamiento. 28
- Figura 2.5.** Bandas de frecuencias en un bloque DCT de tamaño 8 x 8. 35
- Figura 2.6.** Modelo de color RGB. 36
- Figura 2.7.** Notación en el modelo de color RGB. 37
- Figura 2.8.** Conjunto de imágenes de color con su respectivo histograma de dos dimensiones, compuesto por los componentes de color rojo R y verde G de cada imagen. 40
- Figura 2.9** (a) Imagen Original. (b) Imagen con puntos característicos de Harris usando un valor umbral  $Th=10$ . (c) Imagen con puntos característicos de Harris usando un valor umbral  $Th=100$ . 42

## CAPITULO 3.

### Técnica Robusta de Marca de Agua Basada en Normalización de Imágenes.

- Figura 3.1** Ejemplo del proceso de normalización de imagen. (a) Imagen original. (b) Imagen distorsionada y (c) imagen normalizada obtenida tanto de (a) como de (b).3.2 Normalización de imágenes 55
- Figura 3.2** Ejemplo del proceso inverso de normalización de imagen. (a) Imagen original. (b) Imagen normalizada y (c) imagen recuperada PSNR = 15.68 dB. 55
- Figura 3.3** Matriz de cuantificación Q. Factor de calidad  $F_c = 50$ . 57

- Tabla 3.1** Número de bloques promedio con textura fuerte para valores umbral T1 y T2. 58
- Figura 3.4** Ejemplo de clasificación de texturas. (a) Imagen original, (b) clasificación de texturas fuertes (bloques en color blanco). 59
- Figura 3.5** Diagrama del proceso de inserción de marca de agua. 61
- Figura 3.6** Diagrama del proceso de extracción de marca de agua. 63
- Tabla 3.2** Relación promedio entre la tasa de bits erróneos (BER) y la relación señal a ruido pico (PSNR). 65
- Figura 3.7** Relación entre la energía de marca de agua  $\alpha_2$  y la imperceptibilidad de la marca de agua en el esquema propuesto y el esquema de Dong. et al. 65
- Figura 3.8** Imágenes originales (a), (d), (g), (j) e (m). Versiones marcadas (b), (e), (h), (k), y (n), respectivamente. Imágenes de Error (c), (f), (i), (l) y (o). 67
- Figura 3.9** Relación entre la energía de marca de agua  $\alpha_2$  y la BER en el esquema propuesto y el de Dong et al. 68
- Tabla 3.3** Comparativo de tasa de bits erróneos promedio, máxima y mínima entre el método propuesto y el de Dong. et al., insertando una marca de agua de 64 bits y usando un factor de energía de marca de agua= 0.03 70
- Figura 3.10** Logotipo original y versión marcada de imagen Lena con ataques (a)-(n), con su correspondiente logotipo recuperado. 72
- Tabla 3.4** Correlación normalizada obtenida de la imagen Lena. 73
- Tabla 3.5** Comparación de rendimiento con métodos basados en diferentes estrategias 74

## CAPITULO 4.

### Esquema Robusto de Marca de Agua Basado en Modificación de Histograma.

- Figura 4.1.** Ejemplo de un histograma de color en dos dimensiones. (a) Imagen original. (b) Histograma de color 2D obtenido de (a). 79
- Figura 4.2.** Proceso de inserción de marca de agua. 81
- Figura 4.3.** Modificación de histograma B-Rw filtrada, por movimiento interno de bins . 84
- Figura 4.4.** Proceso de detección de marca de agua. 87
- Tabla 4.1** PSNR promedio de las componentes de color y número de bits extraídos correctamente de las imágenes marcadas con compresión JPEG QF = 50 y rotación de  $7^\circ$ .  $L = 16$  y  $r = 12$ . 88

<b>Figura 4.5.</b> PSNR promedio con factor L variable.	89
<b>Figura 4.6.</b> Cantidad promedio de bits extraídos correctamente de un conjunto de imágenes con un valor de radio r variable.	90
<b>Figura 4.7.</b> Imágenes de prueba originales (a-f) y sus versiones marcadas (g-l).	91
<b>Tabla 4.2</b> Porcentaje de píxeles con una delta $e > 1.0$ en las imágenes Lena, Peppers, Tiffany, Lake, Airplane y House	94
<b>Figura 4.8.</b> Imágenes originales (a), (d) y (g). Versiones marcadas (b), (e) y (h). Imagen de diferencia de color (c), (f) y (i).	95
<b>Tabla 4.3</b> Diferencia de Color Normalizada (NCD)	97
<b>Tabla 4.4</b> Fidelidad de la Información Visual (VIF)	98
<b>Tabla 4.5</b> Número promedio de bits extraídos correctamente de imágenes marcadas y no marcadas atacadas por diversas distorsiones geométricas y de procesamiento de señal con 128 bits de marca de agua insertados. Valor umbral T = 89	100
<b>Tabla 4.6</b> Número promedio de bits extraídos correctamente de imágenes marcadas y no marcadas atacadas por diversas distorsiones geométricas y de procesamiento de señal con 256 bits de marca de agua insertados. Valor umbral T = 179	101
<b>Figura 4.9.</b> (a) Imagen marcada, (b) versión rotada por $45^\circ$ con auto-recorte y escalamiento, (c) versión recortada.	103
<b>Tabla 4.7</b> Comparación de rendimiento	103
<b>Tabla 4.8</b> Probabilidades de éxito para tres tipos de ataques combinados	105
<b>Figura 4.10.</b> Gráfica de curvas ROC para tres probabilidades de éxito.	106

## CAPITULO 5.

### **Esquema Robusto de Marca de Agua Basado en Puntos Característicos y Normalización de Imagen.**

<b>Figura 5.1</b> (a) Imagen Original. (b) Puntos característicos obtenidos con un valor umbral 10. (c) Puntos característicos obtenidos con un valor umbral 100.	113
<b>Figura 5.2</b> Extracción de puntos característicos de Harris invariantes.	115
<b>Figura 5.3</b> Regiones circulares obtenidas a partir de puntos característicos invariantes de Harris. (b) Regiones circulares no traslapadas.	116
<b>Figura 5.4</b> (a) Imagen original de Lena. (b) Imagen marcada. (c) Diferencia entre (a) y (b).	119
<b>Tabla 5.1</b> PSNR promedio de imágenes de Lena, Peppers y House	120
<b>Tabla 5.2</b> Correlación normalizada de la marca de agua extraída	121

# Capítulo 1

## Marcas de Agua en Imágenes Digitales

### **Introducción**

Los esquemas de marca de agua describen técnicas que se utilizan para insertar información en materiales de forma imperceptible para los sentidos humanos [1]. 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 copias digitales (especialmente imágenes, audio y vídeo [1], [2]).

En este capítulo se presenta el estado del arte sobre las marcas de agua digitales organizado de la siguiente manera. En la sección 1.1 se presenta una breve reseña histórica así como la definición de marca de agua digital. Los principales requerimientos y aplicaciones de las marcas de agua se discuten en la sección 1.2. La clasificación de distorsiones se presenta en la sección 1.3. Finalmente, en la sección 1.4 se describe como evaluar los esquemas de marcas de agua utilizando herramientas y procedimientos estándares.

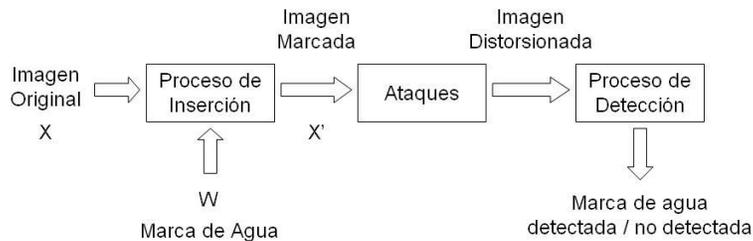
### **1.1 Historia y Definición de Marca de Agua Digital**

El uso de marcas de agua como sistema de protección es casi tan antiguo como la fabricación de papel. Durante cientos de años, cualquiera que tuviera en su poder ó fabricará un documento u obra de arte valioso lo marcaba con un sello de identificación ó

marca de agua (visible o no), no sólo para establecer su propiedad, origen o autenticidad, sino para desalentar a aquellos que pudieran intentar robarlo [2]. La posibilidad de digitalización de cualquier tipo de información (imágenes, vídeo o audio) junto al uso global de Internet permite realizar copias perfectas de la información digitalizada. Los procesos criptográficos permiten proteger la adquisición legal de la información, pero una vez obtenida la información se pueden revender copias exactas. Por lo tanto, surge la necesidad de una técnica complementaria para la protección de los derechos de autor, que también se utilice en el caso de adquisición legal para distribución fraudulenta (copias ilegales). Las propias características de la información digital (facilidad de réplica, facilidad de transmisión y uso múltiple, facilidad de tratamiento y modificación, equivalencia de las copias digitales, etc.) facilitan la agresión contra los derechos de autor del propietario de dicha información, lo que hace necesaria la existencia de un sistema de protección robusto. Por todo esto se ha expandido el concepto de marcas de aguas al mundo digital. Las técnicas de marcas de agua son utilizadas para la autenticación, así como para el seguimiento de copias, ya que permiten la identificación del autor, propietario, distribuidor y/o consumidor autorizado de un documento digital.

Una *marca de agua digital* es un código de identificación que se inserta en un archivo digital de manera que pueda ser detectada por una computadora pero que no sea perceptible para el ojo u oído humanos, la cual se encuentra permanentemente insertada en la información (no desaparece después de la decodificación). Esta señal generalmente contiene información relacionada con el contenido del archivo, como datos sobre sus dueños o creadores, restricciones de distribución u otra información adicional [2]. Su función no es evitar que el archivo pueda ser modificado, sino dar información sobre si ha sido modificado o sobre quién es el autor o titular del derecho de autor de la obra. Aunque no impide que el archivo sea modificado, eso no significa que se pueda eliminar esta marca, entre otras cosas, porque permanece oculta al usuario. 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 y/o extracción.

En la figura 1.1 se muestra el proceso general de inserción y detección de un esquema de marcas de agua. La marca de agua utilizada como entrada del proceso, puede ser un patrón pseudo-aleatorio de una o dos dimensiones u otro tipo de información visual como por ejemplo un logotipo.



**Figura 1.1** Diagrama a bloques de un esquema de marca de agua general.

## 1.2 Requerimientos y Aplicaciones de Marca de Agua Digital

Existen diversas publicaciones [1], [2], [8], [13], [14], [17] en las que se discuten los requerimientos que deben cumplir las marcas de agua. Entre los requerimientos básicos que un sistema de marcas de agua debe contener, se encuentran la robustez, imperceptibilidad, carga útil y no ambigüedad al momento de detectar la marca de agua [1], [2].

Entre los principales requerimientos de marca de agua se encuentran:

**Robustez:** Los archivos digitales de imágenes, audio y video, están expuestos a muchos tipos de modificaciones o ataques como son las pérdidas por compresión, los cambios producidos por el mejoramiento de imágenes, transformaciones geométricas, (recorte, rotación, escalamiento, traslación) etc.

Una marca de agua se considera robusta si se conserva después de esos ataques. Esto quiere decir que la marca debe estar presente en los archivos y debe ser detectada después de las distorsiones [3] [4].

La robustez significa resistencia frente a aquellas modificaciones producidas por las operaciones comunes a las que estarán expuestos los archivos multimedia [1] [2].

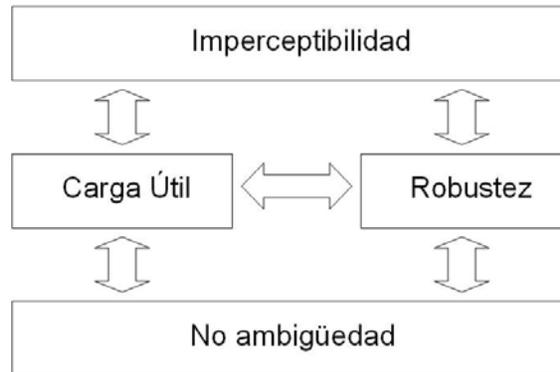
**Imperceptibilidad:** La imperceptibilidad o transparencia de la marca de agua en imágenes tiene como base el comportamiento del sistema visual humano. Una marca de agua es imperceptible, si la degradación que causa en los archivos donde se ha insertado es muy difícil de apreciar. En algunas aplicaciones se puede aceptar una pequeña degradación de los datos, a cambio de lograr mayor robustez o menor costo del sistema [2].

**Carga Útil:** La carga útil de marca de agua hace referencia a la cantidad de información que puede contener una marca de agua, y está depende del tipo de aplicación.

**No Ambigüedad:** En la mayoría de los sistemas de marcas de agua es muy importante distinguir entre los archivos que contienen una marca y los que no. La probabilidad de error al detectar una marca debe ser muy pequeña. Se denomina probabilidad de falso negativo a la probabilidad de que, habiendo estado presente una marca en determinado archivo, el detector asuma que no hay tal marca. Por otro lado, la probabilidad de falso positivo es la probabilidad de que no estando la marca presente en un archivo, el detector asuma que la marca está presente. Este requisito debe ser tomado muy en cuenta, si se quiere que el sistema pueda ser utilizado en disputas legales [1].

La dependencia mutua entre los requerimientos básicos de marca de agua digital, se muestra en la figura 1.2.

A continuación se describen algunas de las aplicaciones propuestas en [2], [5], y algunos de sus requerimientos.



**Figura 1.2.** Dependencia mutua entre requerimientos básicos de marca de agua.

Por su parte, entre las principales aplicaciones de marca de agua digitales se encuentran:

**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, intencionales y no intencionales (se describen en la sección 1.3). Además, es necesario que los esquemas de este tipo utilicen medidas de seguridad para evitar inserciones no autorizadas en imágenes protegidas.

**Rastreo de copias.** Este tipo de aplicación contempla el hecho de insertar 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, conocido como *fingerprinting*.

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, remoción de las marcas de agua utilizando otras copias de la imagen (conocido como ataque de colusión [6], [7]).

**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 a los dispositivos electrónicos si se permite o no la copia de ese volumen [8]. 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, cambio de formato, etc. Los esquemas que se han diseñado con estas características se conocen como de marcas de agua semi-frágiles [1], [2].

### 1.3 Tipos de Ataques

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 marcada se degrade hasta

perder su utilidad [2], [5]. 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 utilizar 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, entre otros [1], [2].

Algunas de las distorsiones más comunes son [5]:

- Mejoramiento de la imagen (corrección de nitidez, color, contraste y gamma).
- Ruido aditivo y multiplicativo (Gaussiano, impulsivo).
- Filtrado lineal (filtros pasa-bajas, pasa-altas, pasa-banda).
- Filtrado no lineal (filtro de mediana).
- Compresión (como compresión JPEG).
- Transformaciones afines globales y locales (traslación, rotación, escalamiento, recorte de imagen).
- Reducción de la imagen (recorte, modificación del histograma).
- Composición de la imagen (inserción de logo, composición de la escena).
- Cambio de formato (JPEG - BMP).
- Conversión D/A y A/D (imprimir y digitalizar, transmisión por televisión analógica).
- Inserción de varias marcas de agua.
- Ataques de colusión [6], [7].

Una vez que la marca de agua ha sido insertada en una imagen digital, es susceptible a una gran variedad de ataques que la distorsionarán, así como degradar la calidad del material marcado. Según la causa y objetivo que los origina, éstos se pueden agrupar en ataques no intencionados e intencionados.

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 no intencionados. Dependiendo de la aplicación, los ataques no intencionales incluyen la compresión, cambio de formato, corrección de la imagen, etc.

Los ataques intencionados son las manipulaciones que realiza un intruso sobre la imagen marcada con el fin de eliminar la protección de derechos de autor.

Los objetivos fundamentales son dos:

- Manejar información libre de cualquier marca de agua.- Este punto tiene como objetivo manipular la imagen para distorsionar la marca de agua insertada en la imagen, de manera que ésta sea indetectable. Por lo tanto, la marca de agua debe ser más resistente que la misma imagen, esto es, que la degradación de la imagen debe ocurrir mucho antes que la marca de agua se distorsione y como consecuencia la marca sea indetectable.
- Insertar su propia marca de agua.- Este punto tiene como objetivo confundir en la determinación de la propiedad de los derechos de autor. La finalidad del agresor es insertar su propia marca de agua para reclamar que el es propietario de la imagen. Por lo que se comprueba que la robustez no es suficiente para garantizar una adecuada protección de los derechos de autor.

Las técnicas utilizadas para el diseño de esquemas de marca de agua son diversas, pero algunos esquemas han demostrado más robustez contra diferentes ataques, intencionales y no intencionales, 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) [9], [10], [11], [12].

## 1.4 Evaluación de Esquemas de Marca 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 [14]. Para evaluar la degradación causada en las imágenes, debido a la inserción de una marca de agua, se pueden utilizar medidas de distorsión cuantitativas. Un ejemplo es la Relación Señal a Ruido Pico (Peak Signal to Noise Ratio, por sus siglas en inglés). La PSNR es una medida en decibeles (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 la PSNR no es una medida de comparación basada en algún modelo del sistema visual humano, es una medida que ha sido ampliamente aceptada [23], [26], [27], [29], para comparar la distorsión provocada por diferentes esquemas de marcas de agua.

Además, existen otro tipo de medidas de distorsión cuantitativas basadas en el modelo del sistema visual humano HVS (Human System Model, por sus siglas en inglés), como por ejemplo, la Fidelidad de la Información Visual VIF (Visual Information Fidelity, por sus siglas en inglés), la cual es una medida de la calidad visual de una imagen basada en el dominio de la transformada wavelet que permite medir con mayor precisión la calidad de una imagen después de que esta ha sido procesada [54].

Por otro lado, cuando se trata de imágenes de color, existen medidas cuantitativas para medir el cambio de colores, entre las que se encuentra la Diferencia de Color Normalizada NCD (Normalized Color Difference, por sus siglas en inglés) [52], [53], la cual es una medida representada por un único número y se utiliza para medir el cambio de color entre dos imágenes. Está basada en el espacio de color CIELAB [50][51], el cual proporciona una útil representación tridimensional de los estímulos perceptuales del color.

Finalmente, como respuesta a la necesidad de establecer puntos de comparación para evaluar la robustez de los esquemas de marca de agua, se han propuesto herramientas estándares que aplican diversas distorsiones en las imágenes marcadas.

Las herramientas más utilizadas con este propósito son Stirmark [13], [14], la cual es una herramienta de ataque que ha sido utilizada para determinar la robustez de las marcas de agua. Sin embargo, con la falta de un estándar de referencia que lleve a cabo la evaluación y certificación oficial de los sistemas de marca de agua, una comunidad científica dedicada al tema denominado proyecto Europeo Certimark (CERTIFICATION for waterMARK) ha dado a conocer una aplicación llamada Checkmark [15], la cual está orientada a la evaluación de los sistemas de marcas de agua que incluye nuevas funcionalidades que no se habían tenido en cuenta en el Stirmark.

Ambas herramientas aplican ataques como: recortes, rotación, escalamiento, filtros de mediana, contaminación de imagen con ruido Gaussiano, distorsiones geométricas aleatorias, eliminación de líneas, compresión JPEG, entre otros.

La tabla 1.1 muestra los ataques que contempla la versión 4.0 de Stirmark Benchmark, herramienta que será utilizada para evaluar la robustez de los algoritmos de marca de agua propuestos en esta tesis. En la actualidad, las técnicas de marcas de agua presentan robustez ante diversos ataques. Sin embargo, las técnicas de marca de agua deben mejorar la robustez ante los ataques que dan lugar a una interpolación de la señal digital que representa la información. En el caso de imágenes estos ataques pueden realizarse mediante rotación, traslación de un número no entero de píxeles y cambios de escala.

TABLA 1.1  
ATAQUES CONTEMPLADOS EN STIRMARK BENCHMARK 4.0

ATAQUE	RANGO APLICADO
Test_PSNR	0 - 100
Test_EmbedTime	5
Test_AddNoise	20, 40, 60, 80, 100
Test_JPEG	QF = 15 – 100
Test_MedianCut	Ventana de 3, 5, 7, 9
Test_ConvFilter	1, 2
Test_SelfSimilarities	1, 2, 3
Test_RemoveLines	10 – 100
Test_Cropping	1, 2, 5, 10, 15, 20, 25, 50, 75
Test_Rescale	0.5, 0.75, 0.90, 1.1, 1.5, 2.0
Test_Rotation	-2° hasta 90°
Test_RotationCrop	-2 ° hasta 2 °
Test_RotationScale	-2 ° hasta 2 °
Test_Affine	1- 8
Test RBA	0.95, 1, 1.05, 1.1

## Conclusiones

En los últimos años se ha incrementado el interés de la comunidad científica por el establecimiento de las definiciones preliminares de los requisitos que deben cumplir los esquemas de marca de agua eficaces con vistas a su estandarización. Sin embargo, aún queda mucho por hacer antes de que pueda hablarse de la adopción definitiva de un estándar para algunas aplicaciones, en el caso de las imágenes, la música y el video se han experimentado diversas iniciativas con resultados positivos. Es aún largo el camino por recorrer dentro del campo, sin embargo se continúa trabajando al respecto en investigaciones como las presentadas en esta tesis, teniendo en mente como idea principal el presentar nuevas propuestas que ayuden al desarrollo del campo.



# Capítulo 2

## Marco Teórico

### Introducción

Existen diversos ataques para remover marcas de agua en los materiales marcados digitalmente, entre ellos se encuentran los ataques geométricos, los cuales son considerados los ataques más agresivos que se pueden hacer en un material con marca de agua y en ocasiones está no puede sobrevivir ante dichas manipulaciones.

A grandes rasgos, los algoritmos de marca de agua se pueden dividir en dos grupos, el primero de ellos es el de marca de agua privada o también conocido como detección no ciega, en el cual, el proceso de detección hace uso de la imagen original, es decir, la imagen original es disponible; el segundo es el grupo de marca de agua pública o también llamado de detección a ciegas, en donde el proceso de detección se lleva a cabo sin tener disponible la imagen original.

El primer grupo de algoritmos de marca de agua es más adecuado y confiable en cuestión de protección de derechos de autor, ya que tanto el error de detección como el error de falsa alarma pueden ser minimizados. En este grupo, los factores de distorsión geométrica se pueden obtener usando técnicas de re-sincronización, esto es comparando la imagen distorsionada y la imagen original.

El segundo grupo de algoritmos de marca de agua en el cual la imagen original no está disponible, se tiene una mayor aplicación comparado con el primer grupo, ya que dichos algoritmos pueden ser usados para el control de copias de material digital o el monitoreo de distribución, solo que en dichos procesos la imagen original no puede estar disponible, por cuestiones de seguridad, de carga de transmisión (velocidad de transmisión) y de carga de almacenamiento, entre otros aspectos.

Sin embargo, en los algoritmos que pertenecen al segundo grupo es más difícil de obtener robustez ante las distorsiones geométricas, ya que no se tiene ninguna referencia para re-sincronizar la marca de agua provocadas por la distorsión geométrica. Algunas técnicas reportan errores en la detección de marcas de agua en imágenes marcadas que han sufrido alguna transformación geométrica. A este problema se le conoce en la literatura como pérdida de sincronización [16], ya que las distorsiones geométricas no eliminan las marcas de agua, solo cambian su posición a localidades desconocidas para los detectores. Cuando la imagen original está disponible para el detector, la sincronización se puede restaurar utilizando técnicas de registro de imágenes [17].

En aplicaciones reales los esquemas de marcas de agua son utilizados en disputas legales, por lo tanto, difícilmente se tiene acceso a la imagen original para llevar a cabo la detección en caso de fotografía digital y en la protección de videos digitales como el DVD, ya que estos dispositivos dependen de una serie de imágenes las cuales pueden tener una pérdida de sincronización (un ejemplo es cuando las imágenes se ajustan automáticamente a cierto tamaño, etc.). 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.

En este capítulo se realiza una breve revisión bibliográfica sobre los algoritmos que son robustos ante ataques de tipo geométrico, sin descuidar los ataques de tipo procesamiento de señal, tales como compresión, filtrado, entre otros, desde el punto de vista de su funcionamiento, sus ventajas y desventajas de cada algoritmo. Posteriormente, se describen algunas de las distorsiones geométricas más comunes aplicadas a imágenes digitales.

También se describen algunas propiedades de los elementos base utilizados para el desarrollo de las técnicas que se proponen en esta tesis en los capítulos 3, 4 y 5 dichos elementos son: los momentos geométricos utilizados en la técnica basada en normalización de imágenes del capítulo 3, así como las características de la

Transformada de Cosenos Discreta utilizada para realizar el esquema de marca de agua del capítulo 3. Seguidamente, se realiza una revisión del modelo RGB de color utilizado en la técnica propuesta en el capítulo 4, así como el concepto de histograma de dos dimensiones. Finalmente se realiza una breve introducción acerca del detector de puntos característicos de Harris, el cual es base del algoritmo presentado en el capítulo 5.

## **2.1 Clasificación de los algoritmos robustos ante los ataques geométricos**

Las técnicas de marca de agua robustas ante ataques geométricos se pueden clasificar básicamente en seis grupos dependiendo del método o técnica utilizada.

Los seis grupos se pueden clasificar de la siguiente manera:

- Búsqueda exhaustiva.
- Inserción de marca de agua en un dominio invariante ante los ataques geométricos.
- Re-sincronización usando una señal llamada plantilla.
- Uso de puntos característicos de la imagen para su sincronización.
- Uso de normalización de imágenes.
- Uso de histograma de imagen como dominio invariante.

A continuación se realiza una revisión de los métodos propuestos en la literatura que pertenecen a cada grupo.

### **2.1.1 Búsqueda exhaustiva**

Una solución directa de re-sincronización de la marca de agua es realizar una búsqueda exhaustiva para obtener factores de distorsión geométrica, tales como ángulo de rotación, número de píxeles en ambos ejes de traslación y factor de escalamiento.

En el proceso de detección, si la imagen original está disponible, la búsqueda se realiza de una manera más rápida. Por otro lado, para el esquema de detección a

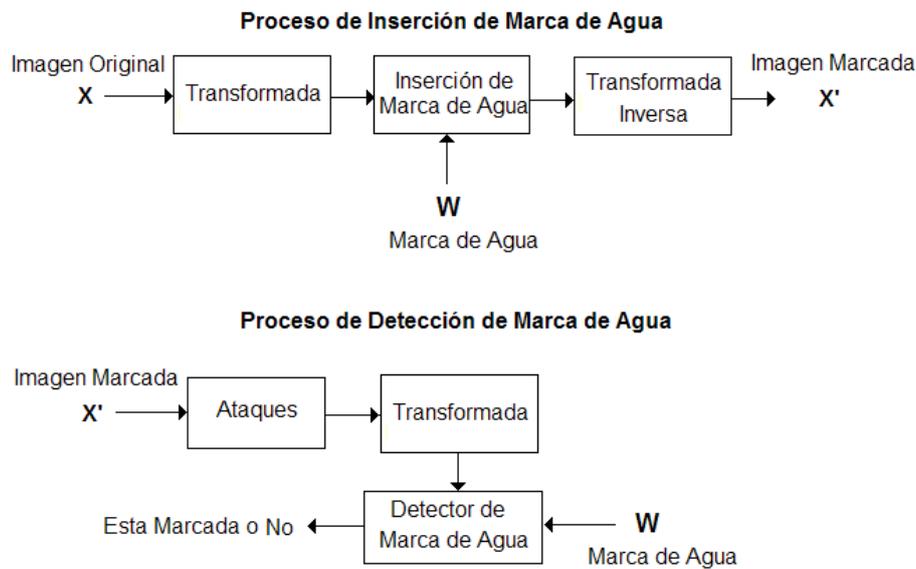
ciegas (imagen no disponible), se requiere de una alta complejidad computacional, además la probabilidad de error de falso positivo, es decir, donde el detector detecta la presencia de una marca de agua cuando en realidad no existe (o esta marcada por otra marca de agua), es alta lo cual no es aceptable en un sistema de marca de agua [16]. Una alternativa de este método ante dichas desventajas es tratar de disminuir el tamaño del espacio de búsqueda que se tiene que realizar, por ejemplo Nikolaidis y Pitas [18] propusieron un método de inserción de marca de agua en el dominio espacial, segmentando la imagen en varias regiones que tienen las mismas características de texturas.

El método realiza el proceso de detección a ciegas; sin embargo, el principal problema de este método es la alta complejidad computacional para realizar una segmentación adecuada de la imagen además de tener vulnerabilidad ante el ataque de contaminación de ruido que produce un error de segmentación en el proceso de detección. Las principales desventajas de este método son las siguientes [16]:

1. Complejidad computacional alta, por lo que no resulta práctico para aplicaciones en donde la detección se tiene que realizar en un tiempo razonable, como por ejemplo el control de copias.
2. Alta tasa de error de falso positivo.

### **2.1.2 Inserción en el dominio invariante a RST.**

La idea básica de este método es realizar la inserción y detección de marca de agua en algún dominio invariante a las modificaciones geométricas, tales como rotación, escalamiento y traslación (*RST Rotation, Scaling, Traslation*). En el campo de reconocimiento de objetos e imágenes y registro de imágenes se han investigado diversos dominios de transformación (Log-Polar, Fourier-Mellin), cuyos coeficientes son invariantes ante estas modificaciones [19] [20] [21]. Usando estos conocimientos, se diseña el algoritmo de marca de agua, donde la marca insertada es invariante ante los ataques geométricos. El esquema general de este método se muestra en la figura 2.1.



**Figura 2.1.** Esquema general de inserción de marca de agua en un dominio invariante.

Ruanaidh y Pun presentaron una propuesta de inserción y detección de marca de agua que se realiza en el dominio de la Transformada Fourier-Mellin, y mostraron que una marca de agua insertada en este dominio presenta robustez ante los ataques RST [12], [22]. Esta propuesta es teóricamente ideal, sin embargo debido a que la Transformada Log-Polar y su inversa son usadas dentro de la Transformada Fourier-Mellin, en ella se realiza un mapeo de un píxel de la imagen hacia muchos píxeles y de muchos píxeles hacia un píxel junto con un método de interpolación, lo cual provoca en la imagen marcada una distorsión visible. Los autores de esta propuesta [12] sugieren que la inserción de marca de agua no debe realizarse en el dominio de la Transformada Fourier-Mellin, debido al mapeo Log-Polar utilizado, de modo que la inserción se debe realizar en otro dominio, como es de la Transformada de Fourier Discreta (DFT).

Solachidis y Pitas en su artículo [10] propusieron un método de inserción de marca de agua con simetría circular en el dominio bi-dimensional de la Transformada DFT, aprovechando que la magnitud de la DFT es invariante a la traslación y la forma circular de la marca de agua reemplaza al mapeo polar que se realiza en la Transformada log-polar, reduciendo así el rango de búsqueda exhaustiva en los ángulos de rotación a 180° grados (debido a la propiedad de simetría que conserva la marca de agua), al mismo tiempo evitando la distorsión provocada por la Transformada Log-Polar y su inversa.

De manera semejante se realiza una búsqueda exhaustiva para la deformación causada por los ataques de escalamiento. El método realiza una detección a ciegas, ya que en el proceso de detección no se hace uso de la imagen original. La propuesta de Solachidis y Pitas se puede describir como una combinación del método basado en la inserción en un dominio invariante y el método de búsqueda exhaustiva, reduciendo así el espacio de búsqueda, esto debido a que se hace uso de la propiedad de simetría circular que preserva la marca de agua.

Zeng, et. al. [23] propusieron un algoritmo de inserción de marca de agua en el dominio de la transformada DFT, usando la magnitud de DFT y considerando el mapeo Log-Polar en este dominio. La técnica es muy parecida a la propuesta por Solachidis [10], solo que la principal diferencia o contribución de este trabajo sobre Solachidis [10] es la estimación del ángulo de rotación y el factor de escalamiento el cual se realiza usando la información de fase de DFT. Sin embargo, esta estimación requiere la información de fase de DFT de la imagen original y este hecho limita el uso de este método en aplicaciones de video, control de copias, y monitoreo de distribución, entre otros.

Usando la misma filosofía que en los trabajos propuestos en [10] y [23], Lin et.al. [24] propusieron un algoritmo de marca de agua robusto a los ataques geométricos. En este algoritmo, la inserción de la marca de agua se realiza sobre un vector generado por la proyección en 1-D del radio de coordenadas log-polar de la magnitud de DFT de la imagen original. Para generar la imagen marcada se introduce una distorsión visible en la imagen provocada por la Transformada Log-Polar inversa. Para evitar este problema se hace uso de una interpolación adaptiva a los valores de la magnitud de DFT, sin embargo no se puede evitar totalmente la distorsión en la imagen marcada.

Este método de inserción garantiza que la marca sea invariante a la traslación (debido a la característica de la magnitud de la Transformada DFT) y al escalamiento debido a la proyección en el eje de radio en el mapa de coordenadas log-polar. Para los ataques de rotación se realiza una búsqueda exhaustiva a 90° grados de los ángulos. La detección es llevada a cabo sin el uso de la imagen original.

S. Bravo en [25], utiliza una inserción de marca de agua en la magnitud del dominio de la Transformada DFT. En el proceso de detección se usa un Algoritmo Genético (AG) para realizar la búsqueda exhaustiva. En esta propuesta, la búsqueda exhaustiva se realiza de una manera sistemática, sin embargo, para estimar los factores de distorsión geométrica como son ángulo de rotación y factor de escalamiento, el factor de traslación no se requiere estimar debido a la invariación a la traslación de la magnitud de la Transformada DFT. Hay que esperar que el algoritmo genético AG llegue a su convergencia. Por lo tanto, en aplicaciones en las cuales se requiere detectar la marca de agua en tiempo real, tales como el control de copias y el monitoreo de distribución, podría ser inconveniente.

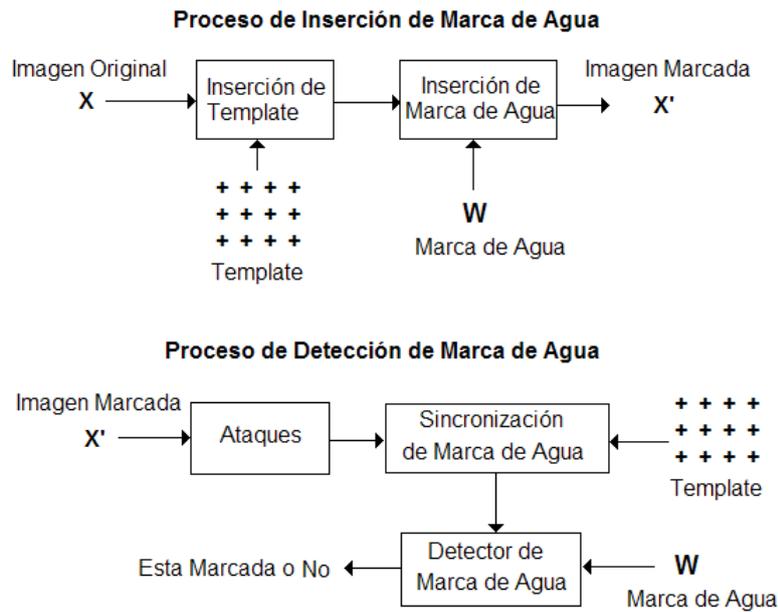
Una desventaja de este método es:

- En este método se dificulta extender la inserción de marcas de agua de múltiples-bits, tales como un mensaje o una marca de agua visualmente reconocible como los logotipos.

### **2.1.3 Re-sincronización de marca de agua usando “plantilla”.**

La “plantilla” es una señal (generalmente bi-dimensional) que no contiene ninguna información relacionada a la protección de derechos de autor ni al control de copias. Esta señal se usa solamente para obtener información de alguna distorsión geométrica (ángulo de rotación, factor de escalamiento, etc.) antes de realizar la detección de la marca de agua.

En este método, el proceso de detección de marca de agua primero busca la señal “plantilla”, una vez recuperada, se utiliza su información para calcular factores de distorsión geométrica y finalmente la marca de agua que se encuentra insertada en la imagen marcada se re-sincroniza. Es decir, se usan estos factores para que la marca de agua insertada tenga la geometría original con la cual fue insertada. La vista esquemática del método general de “plantilla” se muestra en la figura 2.2.



**Figura 2.2.** Esquema general de inserción de marca de agua basado en el uso de “plantilla”.

Existen varias propuestas basadas en “plantilla” [26],[27]. Pereira y Pun [26] propusieron un método basado en la inserción de marca de agua usando una “plantilla”, en el cual, primero se inserta una marca de agua en la magnitud del dominio DFT de la imagen original, posteriormente se insertan 14 puntos como “plantilla” en el mismo dominio. Estos 14 puntos se distribuyen en dos líneas de forma uniforme (7 puntos por cada línea distribuidos de una manera uniforme). Cada línea forma un ángulo respecto a una línea horizontal del plano de la magnitud y la intersección de las dos líneas forman un ángulo. Cada punto de los dos líneas indica un radio (tomado en cuenta la distancia del punto hacia el centro del plano de la magnitud) [26].

En el proceso de detección, usando estos 14 puntos, se determinan el ángulo de rotación y el factor de escalamiento. Una vez que estos factores de distorsión geométrica son detectados, se re-sincroniza la marca de agua para ser detectada. El principal problema de este método es que la inserción del “plantilla” aunque sea solo de 14 puntos, interfiere en la inserción de la marca de agua.

Kang, et al. [27] tomaron la propuesta de Pereira y Pun [26], e hicieron una modificación en su trabajo, en el cual el proceso de inserción de la marca de agua se realiza en el dominio DWT, mientras que la inserción de la “plantilla” se realiza en la magnitud de DFT, igual que en el artículo de Pereira y Pun [26]. Este método aumenta la robustez de la marca de agua contra ataques no geométricos, tales como compresión, filtrado, etc. debido a que el dominio DWT es más robusto a estos ataques, y además la señal de marca de agua y la señal “plantilla” no interfieren una con la otra.

Generalmente los métodos basados en “plantilla” tienen varias desventajas, las cuales son:

1. Pérdida de fidelidad en la imagen marcada inevitable, debido a que las dos señales insertadas en la imagen (“plantilla” y marca de agua), interfieren entre sí.
2. Requieren de una búsqueda exhaustiva para la estimación de “plantilla”.
3. Alto costo computacional en la re-sincronización de la imagen en el proceso de detección.
4. Vulnerabilidad de la señal “plantilla”, ocasionando su pérdida por algún tipo de ataque y pérdida de robustez del sistema.

Estas desventajas limitan el uso de este método [16], [28].

#### **2.1.4 Uso de puntos característicos de la imagen para su sincronización.**

Para solucionar las desventajas provocadas por la inserción de una señal “plantilla”, como se menciona en la sección 2.1.3, la cual es usada para re-sincronizar la marca de agua, algunas técnicas proponen el uso de las características más relevantes de la imagen misma para utilizarlas como señal de re-sincronización. El esquema global de este método se muestra en la figura 2.3.

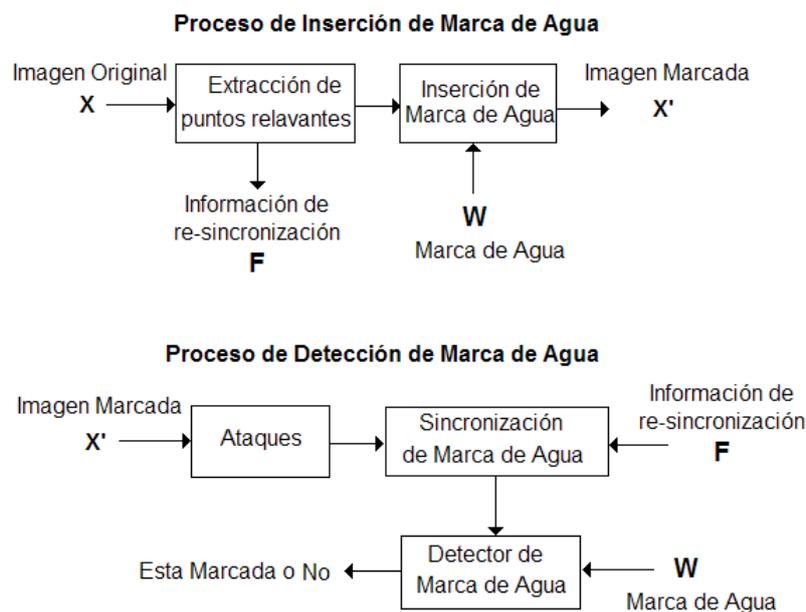
El método de puntos característicos da solución a las dos desventajas más significativas que se presentan en el método de “plantilla”, las cuales son:

1. Pérdida de fidelidad en la imagen marcada inevitable, debido a que las dos señales insertadas en la imagen (“plantilla” y marca de agua), interfieren entre sí.

La solución propuesta es: no insertar ninguna señal adicional para la re-sincronización de la marca de agua, evitando así la pérdida de fidelidad en la imagen marcada.

2. Vulnerabilidad de la señal “plantilla”, ocasionando su pérdida por algún tipo de ataque y pérdida de robustez del sistema.

La solución propuesta es: al no existir ninguna señal adicional para llevar a cabo la re-sincronización, este problema no se presenta en el método.



**Figura 2.3.** Esquema general de inserción de marca de agua basado en el uso de puntos característicos.

Diversos trabajos que se basan en las características de este esquema se han reportado en la literatura, tal como lo propusieron Tang y Hang [29], en el cual se

propone un algoritmo de marca de agua que es robusto ante los ataques geométricos. La técnica propuesta extrae varios puntos característicos de la imagen usando la transformada Wavelet. Usando una posición relativa de los puntos característicos, se estiman los factores de distorsión geométrica, tales como el ángulo de rotación ( $\theta$ ), el factor de escalamiento ( $s$ ) y los vectores de traslación ( $dx, dy$ ).

Este algoritmo realiza la detección de la marca de agua sin la presencia de la imagen original (detección a ciegas), sin embargo, el proceso de extracción de características relevantes de la imagen presenta una alta complejidad computacional, además de que este proceso es muy dependiente de la imagen original. Para el caso de algunas imágenes, no se pueden extraer suficientes puntos característicos para poder determinar los factores de distorsión geométrica.

Izquierdo [30] propuso un método de marca de agua robusto ante los ataques geométricos, en el cual se extraen los puntos más relevantes de la imagen original en el dominio espacial y la marca de agua se inserta en el dominio DCT. Para poder insertar la marca de agua con mayor energía sin provocar una distorsión en la imagen marcada, se usa el concepto de JND (Just Noticeable Difference). En el proceso de detección el esquema utiliza la imagen original para estimar los factores de distorsión geométrica. La principal desventaja de este método es que se requiere la imagen original en el proceso de detección, lo que limita su uso en diversas aplicaciones.

Las principales desventajas que se presentan en los métodos basados en puntos característicos de la imagen son las siguientes [16]:

1. Generalmente los métodos son heurísticos; por lo tanto, se dificulta el análisis teórico para determinar el funcionamiento de los métodos.
2. El funcionamiento de los métodos depende de la imagen a proteger.
3. Generalmente tienen una alta complejidad computacional para extraer las características relevantes.

### 2.1.5 Uso de normalización de imágenes.

Esta categoría usa la técnica de normalización de imágenes basada en momentos invariantes introducido por [31]. Esta categoría esta basada en un concepto en el cual, la versión normalizada de una imagen y sus versiones distorsionadas geométricamente son exactamente iguales. Usando este concepto, la inserción y la detección de marca de agua se realizan en la versión normalizada de la imagen, teóricamente el problema de pérdida de sincronización entre ambos procesos no ocurre.

Alghoniemy y Tewfik en [32] proponen un algoritmo basado en normalización de imágenes, en el cual la marca de agua es insertada en la versión normalizada obtenida de la imagen original. El esquema presenta una complejidad computacional baja, realiza una detección a ciegas y muestra gran robustez ante diversas distorsiones geométricas, sin embargo, para obtener dicha robustez, se sacrifica la calidad de las imágenes marcadas, ya que se obtienen cambios visibles en el contraste de las imágenes marcadas.

Dong et al., propusieron dos algoritmos [33], uno de ellos esta basado en la normalización de imágenes y detección de la marca de agua a ciegas; mientras que el otro algoritmo esta basado en un grafo elástico para una técnica de marca de agua privada. En el primer algoritmo de Dong et al. [33], para evitar una degradación de la calidad en la imagen marcada, la señal de marca de agua se normaliza en lugar de la imagen y se inserta a la imagen en el dominio espacial. El algoritmo de Dong et al. mostró robustez de la marca de agua ante varias distorsiones geométricas, sin embargo, para obtener una tasa de bits erróneos (BER) razonablemente baja en el proceso de detección, la energía de la señal de marca de agua se tiene que aumentar y como consecuencia de esto, la distorsión de la imagen marcada no se puede evitar.

Las principales desventajas que se presentan en los métodos basados en normalización de imágenes son las siguientes:

1. En la práctica, debido a que el proceso de normalización contiene interpolación, la imagen marcada sufre una distorsión visual considerable cuando la inserción

de la marca de agua se realiza en la versión normalizada obtenida de la imagen original.

2. Presentan una fuerte debilidad ante los recortes de imagen, problema común en los métodos basados en normalización de imagen.

### **2.1.6 Uso de histogramas como dominio invariante.**

La sexta y última categoría hace uso del histograma de la información de la imagen, debido a que el histograma es inherentemente invariante a los procesamientos geométricos. El uso de histogramas de imagen como dominio de inserción de marca de agua ha sido previamente reportado en [34-37].

Coltuc y Bolon en su trabajo [34], proponen insertar marcas de agua por medio de una especificación exacta del histograma. La técnica es aplicada en imágenes de escala de grises y los histogramas utilizados son de una dimensión. El objetivo de la técnica es modificar completamente el rango de niveles de escala de grises del histograma e insertar marcas de agua de una forma periódica. El método es robusto a diversas manipulaciones geométricas y procesamientos de señales como compresión, filtrado, entre otros. Sin embargo, la implementación del método en aplicaciones que requieran insertar información en forma de texto o logotipo puede verse afectada, ya que la carga útil de marca de agua del método es limitada.

Chareyron et al., en [35], extienden la especificación de histograma propuesta en [34] para histogramas cromáticos e histogramas de color en tres dimensiones. El método reporta dos técnicas e inserta la secuencia de marca de agua en un plano cromático de dos y tres dimensiones de la imagen de color. Presenta robustez a una gran variedad de distorsiones geométricas.

Roy y Chang en [36] utilizan un histograma de color basado en una implementación reducida de Earth Mover's Distance (EMD), la cual es una medida matemática utilizada para calcular la distancia entre dos distribuciones dadas y es usada en [36] para optimizar la modificación de la imagen de acuerdo a un histograma dado.

La marca de agua es insertada en un histograma de dos dimensiones compuesto por las componentes cromáticas Cb-Cr del modelo YCbCr. El método presenta robustez a rotación, escalamiento, recorte, compresión JPEG y contaminación de imagen con ruido Gaussiano. Una desventaja del método, es que no se reporta robustez a combinación de ataques, por ejemplo, compresión JPEG-distorsión geométrica.

Lin et al., en [37] proponen un método basado en propiedades de histograma que son usadas para medir numerosas características globales de todos los píxeles que componen la imagen, de modo que permita construir un espacio característico de tres dimensiones para insertar la marca de agua. El método presenta robustez a una gran variedad de distorsiones geométricas y procesamientos de señal tales como compresión, filtrado, etc., además de incluir combinación de ataques. Una desventaja del método es su poca tolerancia ante ataques de rotación y recorte de imagen.

Casi todos los trabajos citados previamente basados en modificación de histograma muestran robustez ante las distorsiones geométricas; sin embargo, no proporcionan suficiente robustez ante procesamiento de señales comunes y algunas combinaciones entre ataques geométricos- operaciones de procesamiento de señal.

## 2.2 Distorsiones geométricas.

Distorsiones geométricas tales como la traslación, rotación, escalamiento, deformación en planos paralelos (comúnmente conocido como *shearing*), y reflexión, son transformaciones lineales utilizadas comúnmente en imágenes digitales [38]. Se tiene una imagen cualquiera  $f(x,y)$ , donde las coordenadas cartesianas  $x,y$  se encuentran en los intervalos  $0 < x < N_C$  y  $0 < y < N_R$ ,  $N_C$  y  $N_R$  representan el total de columnas y renglones respectivamente.

Estas distorsiones geométricas están definidas por las ecuaciones 2.1-2.5

$$f_{\text{traslación}}(x, y) = f(x + x_0, y + y_0) \text{ donde } x_0, y_0 \text{ son parametros de traslación en } x, y, \quad (2.1)$$

$$f_{rotación}(x, y) = f(x \cos \theta + y \sin \theta, -x \sin \theta + y \cos \theta) \text{ donde } 0 \leq \theta < 2\pi, \quad (2.2)$$

$$f_{escalamiento}(x, y) = f(x\sigma_1, y\sigma_2) \text{ donde } \sigma_1, \sigma_2 > 0, \sigma_1, \sigma_2 < 0 \quad (2.3)$$

$$f_{shearing}(x, y) = f(x + y\gamma_1, y + x\gamma_2) \text{ donde } \gamma_1, \gamma_2 \text{ factor de shearing,} \quad (2.4)$$

$$f_{reflexión}(x, y) = f(N_C - x + 1, N_R - y + 1). \quad (2.5)$$

A las transformaciones definidas por las ecuaciones (2.1)-(2.5), 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 [25].

La traslación, el escalamiento, la rotación, la reflexión de imagen y todas sus posibles composiciones son conocidas también como transformaciones de semejanza, ya que conservan los ángulos y la proporción de las distancias en las imágenes, para el caso de escalamiento  $\sigma_1 = \sigma_2$ .

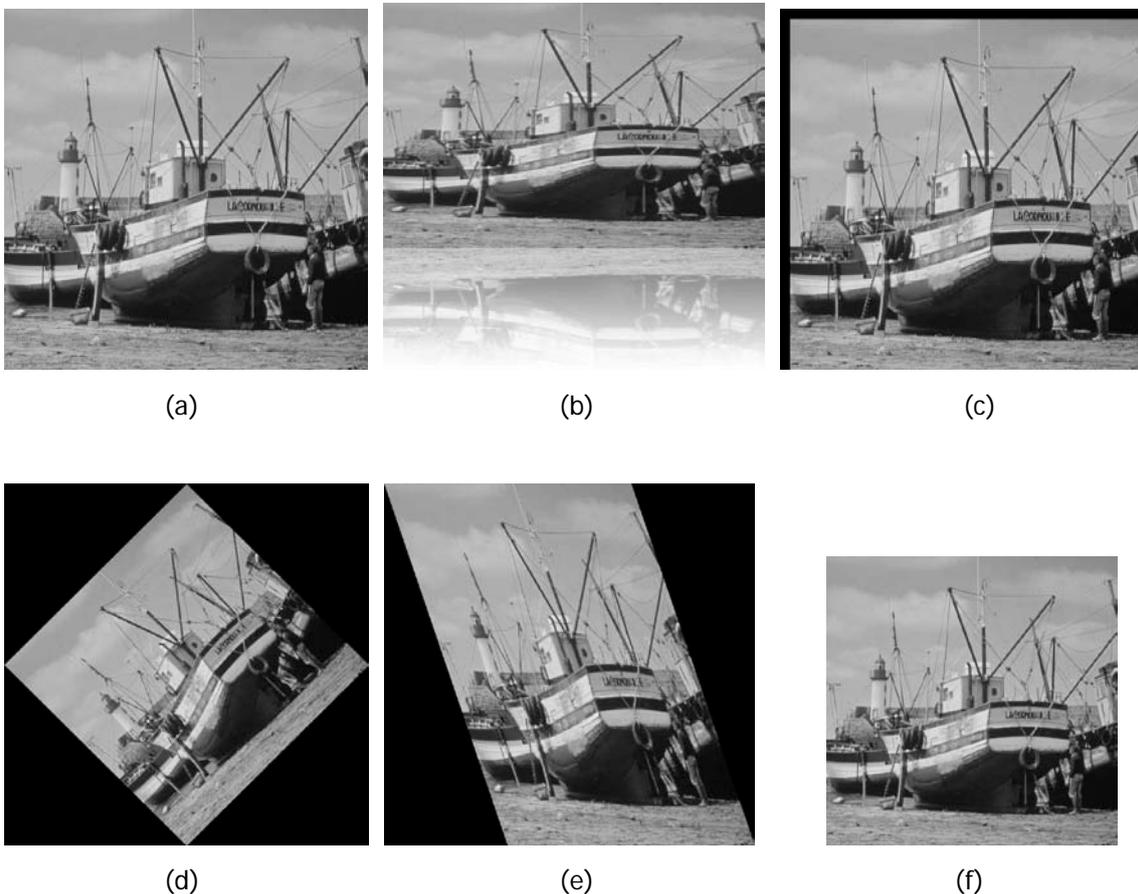
Finalmente, la reflexión, la traslación y la rotación, así como todas sus posibles composiciones, se les conoce como transformaciones euclidianas, ya que se caracterizan por conservar las distancias dentro de las imágenes. En la figura 2.4 se ilustran las transformaciones (2.1)-(2.5) aplicadas a la imagen Boat.

Por otro lado, existen otro tipo de transformaciones denominadas proyectivas, las cuales proyectan una imagen en otro plano y 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 [39], 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.

En la literatura se conocen dos categorías diferentes de ataques geométricos, los globales y los locales [16]. 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.



**Figura 2.4.** (a) Imagen original. (b) Reflexión. (c) Traslación. (d) Rotación. (e) Shearing. (f) Escalamiento.

## 2.3 Momentos geométricos.

Los momentos geométricos son propiedades numéricas que se pueden obtener de una determinada imagen. El uso de momentos geométricos permite conocer bastante información de una imagen y tienen la ventaja de que no solo usa los bordes de una imagen, sino que tiene en cuenta todos los píxeles de la misma. Se usan principalmente para reconocer una forma en una imagen.

### 2.3.1 Momentos simples.

La teoría de los momentos proporciona una interesante y útil alternativa para la representación de formas de objetos. Si tenemos un objeto  $f(x,y)$  en una región, el cual viene dado por los puntos en los que  $f(x,y) > 0$ , el momento de orden  $p,q$  en forma continua se puede definir como [31], [33], [59]:

$$m_{pq} = \iint x^p y^q f(x, y) dx dy \quad \text{para } p, q = 0, 1, 2, \dots \quad (2.6)$$

El teorema de representación de los momentos nos dice que el conjunto infinito de momentos  $m_{p,q}$  para  $p, q = 0, 1, \dots$  determinan unívocamente  $f(x,y)$  y viceversa. Por lo tanto, en una imagen digital definida por la función  $f(x,y)$ , donde  $(x,y)$  son las coordenadas de un punto y  $f(x,y)$  el valor de ese punto, el momento de orden  $(p+q)$  en forma discreta se define como [31], [33], [59]:

$$m_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q f(x, y). \quad (2.7)$$

### 2.3.2 Momentos centrales.

La aplicación más útil de los momentos son las funciones que se pueden extraer de ellos, que son invariantes a transformaciones geométricas tales como traslación, escalamiento y rotación. Los momentos centrales se usan para reconocer una imagen independientemente de su situación en un eje de coordenadas. Para calcular los momentos centrales se usa el centroide de la imagen.

La representación continua de los momentos centrales se define por:

$$\mu_{pq} = \iint (x - \bar{x})^p (y - \bar{y})^q f(x, y) dx dy. \quad (2.8)$$

La representación discreta es:

$$\mu_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (x - \bar{x})^p (y - \bar{y})^q f(x, y), \quad (2.9)$$

donde  $p, q = 1, 2, \dots$ , y  $(\bar{x}, \bar{y})$  es el centroide de la imagen que se obtiene mediante los momentos de orden 1 y de orden 0 :

$$\bar{x} = \frac{m_{10}}{m_{00}}, \bar{y} = \frac{m_{01}}{m_{00}}.$$

El centroide o centro de masas de una imagen viene determinado por las coordenadas  $(\bar{x}, \bar{y})$ , de forma que el área de la imagen que queda a la derecha e izquierda del punto  $\bar{x}$  es la misma, al igual que el área que queda por encima y por debajo del punto  $\bar{y}$ .

### 2.3.3 Momentos centrales normalizados.

Los momentos simples son comúnmente utilizados para obtener el área de una figura dentro de una imagen, a manera de ejemplo, si la figura dentro de la imagen se invierte, esto no es limitante para reconocerla haciendo uso de los momentos simples. Por otro lado, los momentos centrales sirven para distinguir una figura dentro de una imagen no importando si esta se encuentra desplazada; además, con los momentos centrales se podrán reconocer figuras [31] dentro de una imagen independientemente de su tamaño. Los momentos centrales normalizados [40], [41], están denotados por la siguiente ecuación:

$$N\mu_{pq} = \frac{\mu_{pq}}{\mu_{pq}^{\beta}(0,0)}, \quad (2.10)$$

donde:

$$\beta = \frac{(p+q)}{2} + 1.$$

### 2.3.4 Momentos de orden 0.

Los momentos simples de orden 0 en imágenes binarias representan la suma de todos los píxeles cuyo valor es uno, es decir los que son distinto de blanco, por tanto, se obtiene el cálculo del área de una figura dentro de una imagen binaria.

En términos generales, los momentos simples de orden 0 representan el área de una figura en imágenes binarias y la superficie en imágenes de escala de grises. Es la suma de los valores de todos los píxeles, como se muestra en la ecuación 2.11:

$$m_{00} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^0 y^0 f(x, y) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y). \quad (2.11)$$

### 2.3.5 Momentos de orden 1.

Los momentos simples de orden 1 son utilizados principalmente para hallar el centro de masas de una figura, y están definidos por las ecuaciones 2.12 y 2.13:

$$m_{10} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^1 y^0 f(x, y) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} xf(x, y) , \quad (2.12)$$

$$m_{01} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^0 y^1 f(x, y) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} yf(x, y) . \quad (2.13)$$

Por otro lado, los momentos centrales de orden 1 son 0 por definición [40], [41], como se muestra a continuación:

$$\begin{aligned} \mu_{10} &= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (x - \bar{x})^1 (y - \bar{y})^0 f(x, y) \\ &= m_{10} - \frac{m_{10}}{m_{00}} m_{00} \end{aligned} \quad (2.14)$$

$$\begin{aligned} \mu_{01} &= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (x - \bar{x})^0 (y - \bar{y})^1 f(x, y) \\ &= m_{01} - \frac{m_{01}}{m_{00}} m_{00} \end{aligned} \quad (2.15)$$

### 2.3.6 Momentos de orden 2.

Los momentos centrales de orden 2 sirven para realizar el análisis de las imágenes mediante el reconocimiento de formas, los momentos centrales son de vital importancia cuando se requiere realizar el cálculo de los momentos centrales de orden 2. La densidad de la figura se multiplica por distancias al cuadrado desde el centro de masas o centroide (conocida también como inercia).

Las características de los momentos centrales de orden 2 son:

Momento central de orden 2 con  $p = 2$  y  $q = 0$  denotado por  $\mu_{20}$ .- Su valor aumentará cuanto mayor sea la componente horizontal de una figura.

Momento central de orden 2 con  $p = 0$  y  $q = 2$  denotado por  $\mu_{02}$ .- Su valor aumentará cuando mayor sea la componente vertical de una figura.

Momento central de orden 2 con  $p = 1$  y  $q = 1$  denotado por  $\mu_{11}$ .- Hace uso de las componentes horizontal y vertical. Su valor puede ser positivo o negativo dependiendo la localización de la componente vertical; es decir, si la componente vertical se encuentra en los cuadrantes 2º y 4º, entonces será negativo, por el contrario, si se localiza en los cuadrantes 1º y 3º entonces será positivo.

Tomando en cuenta los hechos antes mencionados, se deduce que en una imagen simétrica respecto a los ejes, el momento central  $\mu_{11}$  será 0.

### 2.3.7 Momentos de orden 3.

Estos momentos sirven para calcular los momentos invariantes. A partir de los momentos centrales normalizados de orden 2 y 3 se obtienen los siete momentos invariantes de acuerdo a [31] [40] [41]. Estos momentos definidos por (2.16)-(2.22), como su propio nombre indica, se mantienen invariantes ante rotaciones, traslaciones y cambios de escala.

$$I_1 = N\mu_{20} + N\mu_{02}, \quad (2.16)$$

$$I_2 = (N\mu_{20} - N\mu_{02})^2 + 4(N\mu_{11})^2, \quad (2.17)$$

$$I_3 = (N\mu_{30} - 3N\mu_{12})^2 + (3N\mu_{21} - N\mu_{03})^2, \quad (2.18)$$

$$I_4 = (N\mu_{30} + N\mu_{12})^2 + (N\mu_{21} + N\mu_{03})^2, \quad (2.19)$$

$$I_5 = (N\mu_{30} - 3N\mu_{12})(N\mu_{30} + N\mu_{12})[(N\mu_{30} + N\mu_{12})^2 - 3(N\mu_{21} + N\mu_{03})^2] \\ + (3N\mu_{21} - N\mu_{03})(N\mu_{21} + N\mu_{03})[3(N\mu_{30} + N\mu_{12})^2 - (N\mu_{21} + N\mu_{03})^2], \quad (2.20)$$

$$I_6 = (N\mu_{20} - N\mu_{02})[(N\mu_{03} + N\mu_{12})^2 - (N\mu_{21} + N\mu_{03})^2] \\ + 4N\mu_{11}(N\mu_{30} + N\mu_{12})(N\mu_{21} + N\mu_{03}), \quad (2.21)$$

$$I_7 = (3N\mu_{21} - N\mu_{03})(N\mu_{30} + N\mu_{12})[(N\mu_{30} + N\mu_{12})^2 - 3(N\mu_{21} + N\mu_{03})^2] \\ + (3N\mu_{12} - N\mu_{30})(N\mu_{21} + N\mu_{03})[3(N\mu_{30} + N\mu_{12})^2 - (N\mu_{21} + N\mu_{03})^2]. \quad (2.22)$$

En esta sección se realizó una descripción acerca de los momentos geométricos y sus propiedades. En el capítulo 3, se realiza una descripción detallada del proceso de normalización de imágenes que hace uso de estos momentos geométricos.

## 2.4 Transformada de Coseno Discreta.

La Transformada de coseno discreta (DCT del inglés *Discrete Cosine Transform*) es una transformada basada en la Transformada de Fourier discreta (DFT del inglés *Discrete Fourier Transform*), pero utilizando únicamente coeficientes reales. Para una imagen de tamaño  $M \times N$ , la DCT para dos dimensiones está dada por:

$$F(u, v) = \left(\frac{2}{M}\right)^{\frac{1}{2}} \left(\frac{2}{N}\right)^{\frac{1}{2}} C_u C_v \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f(i, j) \cos\left(\frac{(2i+1)u\pi}{2M}\right) \cos\left(\frac{(2j+1)v\pi}{2N}\right), \quad (2.23)$$

donde:

$F(u, v)$  : Valor del coeficiente DCT de la fila  $u$ , columna  $v$ .

$f(i, j)$  : Valor de intensidad del píxel en la fila  $i$  y columna  $j$ .

$M$  : Ancho de la imagen.

$N$  : Alto de la imagen.

$i, j$  : Índices de la imagen de tamaño  $M \times N$ .

Los términos  $C_u$  y  $C_v$  se definen como:

$$C_u, C_v = \frac{1}{\sqrt{2}} \quad \text{para } u=0, v=0,$$

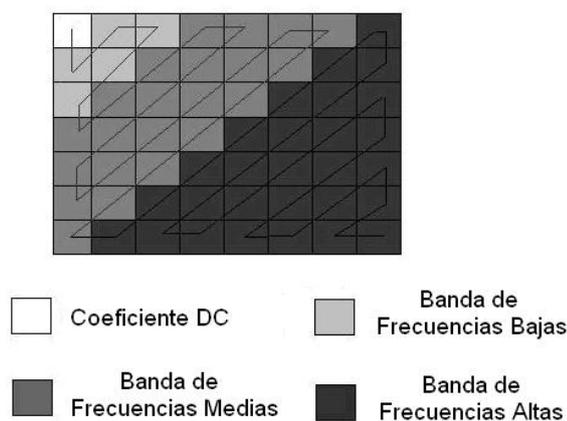
$$C_u, C_v = 1 \quad \text{para cualquier otro caso.}$$

La Transformada de coseno discreta expresa una secuencia finita de varios puntos como resultado de la suma de distintas señales sinusoidales (con distintas frecuencias y amplitudes). Como la Transformada Discreta de Fourier (DFT) la DCT trabaja con una serie de números finitos, pero mientras la DCT trabaja con cósenos, la DFT lo hace con exponenciales complejas.

Está transformada es utilizada como base en la compresión de tipo JPEG y el tamaño de bloque utilizado en la compresión tiene dimensiones de 8x8. Al realizar la transformada, se busca convertir la mayor cantidad posible de valores menos significativos en ceros, entendiendo por estos valores como aquellos de los cuales una imagen puede prescindir sin perder el significado y el tamaño del archivo se logra reducir, aunque de cierta manera se llega a sacrificar la calidad de la imagen.

Por otro lado, la DCT permite separar la imagen en bandas de frecuencia, conocidas como frecuencias altas, medias y bajas. En una imagen, las frecuencias bajas tienen una mayor probabilidad de ocurrencia en comparación con las altas frecuencias, así, al realizar la transformación de una imagen al dominio de la frecuencia, se pueden quitar una gran cantidad de coeficientes de alta frecuencia con la finalidad de reducir la cantidad de datos necesarios para describir la imagen sin que está pierda su significado y sin degradar demasiado la calidad de la imagen [42].

El primer coeficiente (1,1) es llamado el coeficiente DC el cual contiene el valor de luminancia promedio del bloque, siendo el coeficiente de mayor magnitud del bloque, los demás componentes son llamados coeficientes de AC. En la figura 2.5, se ilustran las frecuencias de la DCT, así como el primer coeficiente DC.



**Figura 2.5.** Bandas de frecuencias en un bloque DCT de tamaño 8 x 8.

En esta sección se describió de una forma general la transformada de coseno discreta, la cual será utilizada para llevar a cabo la inserción de la marca de agua en el esquema propuesto en el capítulo 3, así como la clasificación de texturas utilizada en dicho esquema.

## 2.5 Modelo de color RGB.

El modelo de color RGB (del inglés *Red, Green, Blue*; "rojo, verde, azul") está basado en la síntesis aditiva, con el que es posible representar un color mediante la mezcla por adición de los tres colores primarios, que son el rojo, verde y azul. Cabe señalar que el modelo de color RGB no define por sí mismo lo que significa exactamente rojo, verde o azul, razón por la cual los mismos valores RGB pueden mostrar colores notablemente diferentes en diferentes dispositivos que usen este modelo de color. Aunque utilicen un mismo modelo de color, sus espacios de color pueden variar considerablemente. Los colores obtenidos directamente naturalmente por descomposición de la luz solar o artificialmente mediante focos emisores de luz de una longitud de onda determinada se denominan colores aditivos. No es necesaria la unión de todas las longitudes del espectro visible para obtener el blanco, ya que si mezclamos solo rojo, verde y azul obtendremos el mismo resultado. Este modelo se ilustra en la figura 2.6.



**Figura 2.6.** Modelo de color RGB.

Por este motivo, estos colores son denominados colores primarios, porque la suma de los tres produce el blanco. Además, todos los colores del espectro pueden ser obtenidos a partir de ellos.

Los colores aditivos son usados en gráficos de computadora por medio de monitores de equipos de cómputo, ya que, el monitor produce los puntos de luz partiendo de tres tubos de rayos catódicos, uno rojo, otro verde y otro azul. Por este motivo, el modelo de definición de colores usado en trabajos digitales es el modelo RGB. Todos los colores que se visualizan en el monitor están en función de las cantidades de rojo, verde y azul utilizadas. Por ello, para representar un color en el modelo RGB se asigna un valor entre 0-255 (notación decimal) o entre 00-FF (notación hexadecimal) para cada una de las componentes rojo, verde y azul que lo forman. Los valores más altos de RGB corresponden a una cantidad mayor de luz blanca. Por consiguiente, entre más altos son los valores RGB, más claros son los colores.

De esta forma, un color será representado en el modelo RGB mediante la sintaxis decimal  $(R,G,B)$  o mediante la sintaxis hexadecimal #RRGGBB. El color rojo puro, por ejemplo, se especifica como (255,0,0) en notación RGB decimal y #FF0000 en notación RGB hexadecimal, mientras que el color rosa claro dado en notación decimal por (252,165,253) se corresponde con el color hexadecimal #FCA5FD. La figura 2.7, muestra un ejemplo de notaciones tanto decimal como hexadecimal.

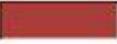
Notaciones RGB		
hexadecimal		decimal
#A52A2A		165, 42, 42
#DEB887		222, 184, 135
#5F9EA0		95, 158, 160
#7FFF00		127, 255, 0
#D2691E		210, 105, 30
#FF7F50		255, 127, 80
#6495ED		100, 149, 237

Figura 2.7. Notación en el modelo de color RGB.

Por otro lado, los ojos humanos tienen dos tipos de células sensibles a la luz o fotorreceptores: los bastones y los conos. Los conos son los encargados de aportar la información de color. Para saber como el ser humano percibe un color, hay que tener en cuenta que existen tres tipos de conos con respuestas frecuenciales diferentes, y que tienen máxima sensibilidad a los colores que forman la terna RGB, rojo, verde y azul. Mientras los conos que reciben información del verde y el rojo tienen una curva de sensibilidad similar, la respuesta al color azul es una vigésima (1/20) parte de la respuesta a los otros dos colores. Este hecho lo aprovechan algunos sistemas de codificación de imagen y vídeo, como el JPEG o el MPEG, "perdiendo" de manera consciente más información de la componente azul, ya que la visión humana no percibirá esta pérdida.

La sensación de color se puede definir como la respuesta de cada una de las curvas de sensibilidad al espectro radiado por el objeto observado. De esta manera, obtenemos tres respuestas diferentes, una por cada color.

El hecho de que la sensación de color se obtenga de este modo, hace que dos objetos observados, radiando un espectro diferente, puedan producir la misma sensación. Basado en esta limitación de la visión humana, el modelo de síntesis del color obtiene a partir de estímulos visuales estudiados y con una mezcla de los tres colores primarios, el color de un objeto con un espectro determinado.

En este apartado se describió de forma general el modelo RGB, el cual será la base del esquema de marca de agua del capítulo 4.

## **2.6 Histograma de dos dimensiones (2D)**

En gráficos de computadora y fotografía digital, un histograma de color es una representación de la distribución de colores en una imagen, derivado de contar el número de píxeles de cada color. Estas representaciones pueden ser presentadas en una (1D), dos (2D) y tres 3(D) dimensiones.

En particular, el histograma 2D es utilizado para representar la probabilidad de la co-ocurrencia, es decir, aparición simultánea de dos valores de niveles de gris cuando sus pixeles correspondientes se encuentran separados a una distancia específica.

Este se puede definir como una matriz  $H_{2D}$  que contiene información del nivel de gris de cada píxel y del nivel de gris promedio de la vecindad de un píxel dentro de la escala utilizada, esto es:

$$H_{2D}(i,j) \leftarrow \text{Número de píxeles que cumplen } R(m_1,m_2)=j \ \& \ B(n_1,n_2)=i \quad , \quad (2.24)$$

donde:

$$n_1, m_1=1 \dots N$$

$$n_2, m_2=1 \dots M$$

$N \times M = \text{Tamaño de la imagen}$

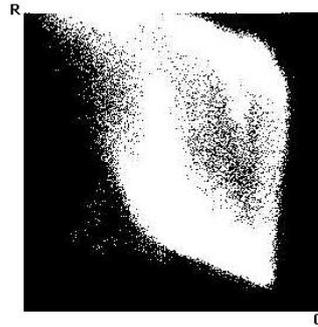
$$0 \leq i, j \leq L-1, L=2^8$$

En un histograma 2D los valores promedios locales representan la información espacial, sin tener una representación del punto preciso de la información que refleja cada píxel que compone la imagen, aunque permite tener una idea de la distribución espacial de los pixeles asociados a ciertas regiones en la imagen.

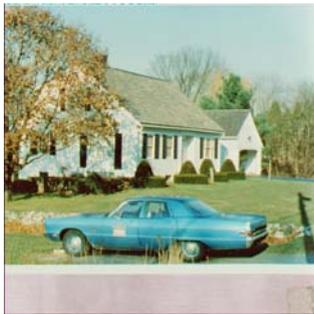
En la figura 2.8 se muestra un conjunto de 4 imágenes de color y su histograma 2D correspondiente. Para obtener los histogramas se hace uso de las componentes de color rojo  $R$  y verde  $G$  de cada imagen.



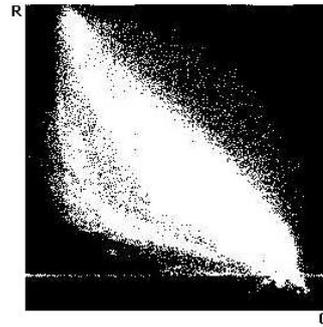
(a)



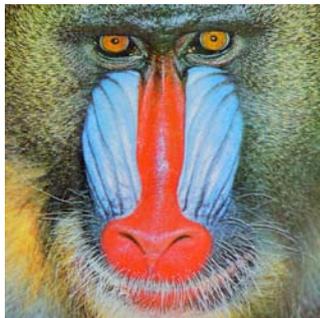
(b)



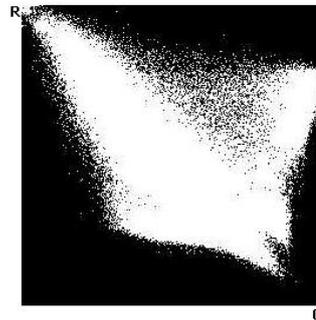
(c)



(d)



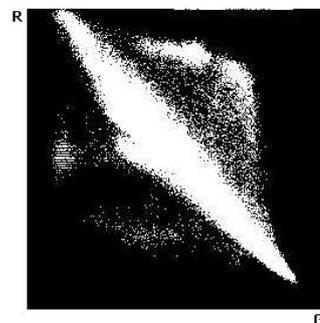
(e)



(f)



(h)



(i)

**Figura 2.8.** Conjunto de imágenes de color con su respectivo histograma de dos dimensiones, compuesto por los componentes de color rojo  $R$  y verde  $G$  de cada imagen.

## 2.7 Detector de esquinas de Harris

El detector de esquinas de Harris [55] es, probablemente, el más comúnmente usado, debido a que es altamente invariante al escalamiento, rotación, cambios de iluminación y ruido en la imagen. El detector de esquinas de Harris hace uso de un gradiente en direcciones horizontal y vertical, llamado gradiente direccional. El gradiente direccional ha sido utilizado como detector de bordes, debido a que el gradiente horizontal es un detector de borde horizontal y el gradiente vertical es un detector de borde vertical. Para llevar a cabo el diseño del detector de Harris, se hace uso de una matriz llamada matriz de segundo momento (Second Moment Matrix), la cual se define como:

$$M = \begin{bmatrix} A & C \\ C & B \end{bmatrix} = \begin{bmatrix} \left( \frac{\partial f(x, y)}{\partial x} \right)^2 * \omega & \left( \frac{\partial f(x, y)}{\partial x} \right) \left( \frac{\partial f(x, y)}{\partial y} \right) * \omega \\ \left( \frac{\partial f(x, y)}{\partial x} \right) \left( \frac{\partial f(x, y)}{\partial y} \right) * \omega & \left( \frac{\partial f(x, y)}{\partial y} \right)^2 * \omega \end{bmatrix}, \quad (2.25)$$

donde  $\omega$  es una función Gaussiana la cual es usada como ventana. Para evitar el cálculo de los valores propios de la matriz  $M$ , se hace uso de un nuevo criterio usando un trace  $Tr$  y un determinante de la matriz  $M$ , los cuales están definidos por (2.26) y (2.27) respectivamente:

$$Tr(M) = \lambda_1 + \lambda_2 = A + B = \left( \frac{\partial f(x, y)}{\partial x} \right)^2 * \omega + \left( \frac{\partial f(x, y)}{\partial y} \right)^2 * \omega, \quad (2.26)$$

$$Det(M) = \lambda_1 \lambda_2 = AB - C^2, \quad (2.27)$$

de tal forma, que la respuesta del detector es:

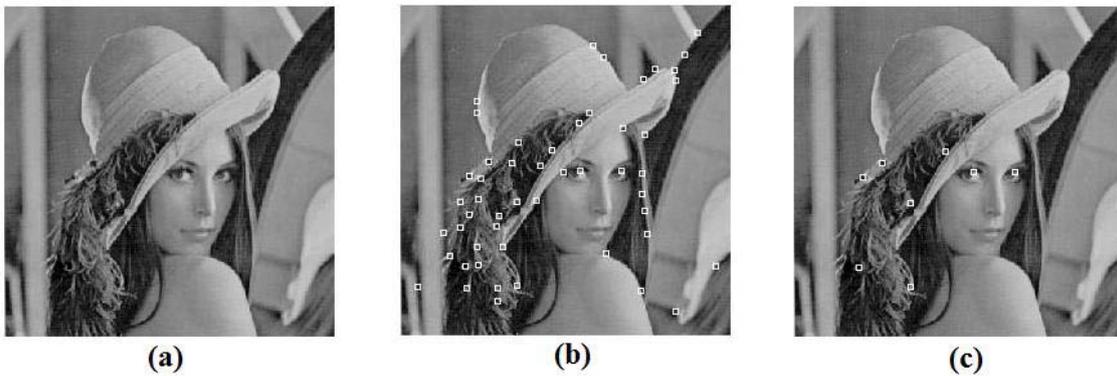
$$R_H = Det(M) - kTr^2(M), \quad (2.28)$$

donde  $k$  es un constante que debe ser seleccionada dentro de un rango  $[0.04, 0.15]$ .

En (2.29), cada región  $\Omega$ , se selecciona un punto en el cual la respuesta del detector  $R_H$  es máxima y rebasa el valor umbral  $Th$ .

$$R_H(i, j) > Th \ \& \ \max_{(i, j) \in \Omega} R_H(i, j) \quad (2.29)$$

Finalmente, los puntos seleccionados son los puntos de esquina o puntos característicos de la imagen. El valor umbral  $Th$  es muy importante para obtener estos puntos, si el valor umbral  $Th$  es pequeño, el número de puntos característicos aumenta; en cambio, si el valor umbral  $Th$  es grande, el número de puntos característicos disminuye. En la figura 2.9 se muestra un ejemplo de puntos característicos obtenidos aplicando el detector de esquinas Harris a la imagen Lena con diferentes valores  $Th$ .



**Figura 2.9** (a) Imagen Original. (b) Imagen con puntos característicos de Harris usando un valor umbral  $Th=10$ . (c) Imagen con puntos característicos de Harris usando un valor umbral  $Th=100$ .

## Conclusiones

En esquemas de marca de agua digital aplicados en imágenes existen diversos ataques para remover marcas de agua en los materiales marcados digitalmente, entre ellos se encuentran los ataques geométricos, los cuales son considerados los ataques más agresivos que se pueden hacer sobre un material con marca de agua y en ocasiones está no puede sobrevivir ante dichas manipulaciones. A este problema se le conoce en la literatura como pérdida de sincronización, ya que las distorsiones geométricas no eliminan las marcas de agua, solo cambian su posición a localidades desconocidas para

los detectores. Ante esta problemática, en la literatura se han propuesto diversas iniciativas para combatir dicho ataques, estas pueden clasificarse básicamente en seis grupos: búsqueda exhaustiva, inserción de marca de agua en un dominio invariante ante los ataques geométricos, re-sincronización usando una señal llamada plantilla, uso de puntos característicos de la imagen para su sincronización, uso de normalización de imágenes y finalmente el uso del histograma de una imagen como dominio invariante.



# Capítulo 3

## Técnica Robusta de Marca de Agua Basada en Normalización de Imágenes

### 3.1. Introducción

Distorsiones geométricas, tales como traslación, escalamiento, rotación y cualquier transformada Affine, son algunos de los principales factores causantes de la pérdida de sincronización en los esquemas que implementan la detección a ciegas. Además, este tipo de ataques ocurre comúnmente en varias aplicaciones prácticas. Por lo tanto, para combatir este problema, se han propuesto varios algoritmos en la literatura [10], [12], [18], [22-37], [46-47]. Como se revisó en el capítulo 2 de esta tesis, los algoritmos propuestos se pueden clasificar básicamente en seis categorías, las cuales son: los métodos basados en búsqueda exhaustiva, los que hacen uso de algún dominio invariante a distorsiones geométricas, los que utilizan una señal de re-sincronización, los que hacen uso de características relevantes de la imagen para llevar a cabo una re-sincronización, los que usan la técnica de normalización de imágenes y por último los que utilizan el histograma de la imagen como dominio invariante a las distorsiones geométricas.

Retomando la categoría que usa la técnica de normalización de imágenes introducida por [31], estos métodos están basados en un concepto en el cual, la versión normalizada de una imagen y sus versiones distorsionadas geoméricamente son exactamente iguales.

Usando este concepto, si la inserción y la detección de marca de agua se realizan en la versión normalizada de la imagen, teóricamente el problema de pérdida de sincronización entre ambos procesos no ocurre. En la práctica, debido a que el proceso de normalización contiene interpolación, la imagen marcada sufre una distorsión visual considerable.

Dong et al., propusieron dos algoritmos [33], uno de ellos está basado en la normalización de imágenes y detección de la marca de agua a ciegas; mientras que el otro algoritmo está basado en un grafo elástico para una técnica de marca de agua privada.

En el primer algoritmo de Dong et al. [33], para evitar una degradación de la calidad en la imagen marcada, la señal de marca de agua se normaliza en lugar de la imagen y se inserta a la imagen en el dominio espacial [33]. El algoritmo de Dong et al., mostró robustez de la marca de agua ante varias distorsiones geométricas, sin embargo para obtener una tasa de bits erróneos (del inglés *Bit Error Rate*) razonablemente baja en el proceso de detección, la energía de la señal de marca de agua se tiene que aumentar y como consecuencia de esto, la distorsión de la imagen marcada no se puede evitar. La tasa de bits erróneos se define como el resultado de dividir los bits recuperados erróneamente y el número total de bits que componen la marca de agua.

En este capítulo, se propone un algoritmo de marca de agua basado en la normalización de imágenes, en el cual, un patrón de marca de agua es normalizado usando los mismos factores geométricos obtenidos en la normalización de imagen. Para insertar la marca de agua con mayor energía, sin perjudicar la imperceptibilidad de la misma en el algoritmo propuesto, los bloques de tamaño 8x8 píxeles que contienen coeficientes DCT de la imagen normalizada, se clasifican dependiendo de la complejidad de texturas. Usando la complejidad de cada bloque, se determina la energía o fuerza de inserción de la marca de agua para este bloque.

El algoritmo propuesto es similar al algoritmo de Dong et al. [33] desde el punto de vista del uso de la normalización de imágenes, sin embargo el algoritmo propuesto difiere al de Dong et al. en los siguientes aspectos:

a) La energía de inserción de la marca de agua es adaptable, considerando la complejidad de texturas de cada bloque de la imagen.

b) El algoritmo propuesto fue evaluado con un mayor número de ataques además de los ataques geométricos.

c) El comportamiento del algoritmo propuesto es comparado con métodos de marca de agua basados en otras estrategias.

Este trabajo está organizado de la siguiente manera: en esta sección se realizó una introducción acerca de la técnica de marca de agua y sus antecedentes sobre algoritmos de marca de agua robustos a distorsiones geométricas. En la sección 3.2, la técnica de normalización de imágenes es descrita de forma detallada y el algoritmo propuesto es descrito en las secciones 3.3 y 3.4. Finalmente, en la sección 3.5, los resultados obtenidos por simulación computacional son mostrados.

## **3.2. Normalización de imágenes**

En el algoritmo propuesto, la imagen y el patrón de marca de agua son normalizados para construir un esquema de marca de agua robusto a distorsiones geométricas. En esta sección, se hace una descripción acerca de la técnica de normalización de imágenes, la cual se basa en la teoría de momentos invariantes propuesta en [31]. Aquí se describen detalladamente los procedimientos de cálculo de momentos invariantes y normalización de imágenes.

### 3.2.1 Momentos invariantes y procedimiento de normalización de imágenes

Los momentos geométricos  $m_{p,q}$  y los momentos centrales  $\mu_{p,q}$  de una imagen  $f(x, y)$  se definen en (3.1) y (3.2), respectivamente.

$$m_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q f(x, y) \quad , \quad (3.1)$$

$$\mu_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (x - \bar{x})^p (y - \bar{y})^q f(x, y) \quad , \quad (3.2)$$

donde  $p, q = 1, 2, \dots$ , y  $(\bar{x}, \bar{y})$  es la masa central de la imagen que se obtiene como:

$$\bar{x} = \frac{m_{10}}{m_{00}}, \bar{y} = \frac{m_{01}}{m_{00}} .$$

El procedimiento de normalización de una imagen  $f(x, y)$  consiste de las siguientes etapas:

1) Trasladar la imagen  $f(x, y)$  con los valores  $(d_x, d_y)$  para generar una nueva imagen  $f_1(x, y) = f(x_a, y_a)$ , cuyo centro es igual a la masa central de la imagen  $f(x, y)$ . Esta operación esta dada por (3.3) usando una Transformación Affine.

$$\begin{pmatrix} x_a \\ y_a \end{pmatrix} = A \cdot \begin{pmatrix} x \\ y \end{pmatrix} - d \quad , \quad (3.3)$$

donde:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, d = \begin{pmatrix} d_x \\ d_y \end{pmatrix} ,$$

cuyos elementos son:

$$d_x = \frac{m_{10}}{m_{00}}, d_y = \frac{m_{01}}{m_{00}} .$$

Este proceso normaliza una imagen respecto a la traslación.

2) Aplicar una transformación *shearing* en la dirección  $x$  a la imagen  $f_1(x, y)$ , usando:

$$A_x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} .$$

La imagen resultante se denota como  $f_2(x, y)$ , la cual está normalizada ante el efecto de deformación en la dirección  $x$ .

3) Aplicar una transformación *shearing* en la dirección  $y$  a la imagen  $f_2(x, y)$ , usando:

$$A_y = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} .$$

La imagen resultante se denota como  $f_3(x, y)$ , la cual está normalizada ante el efecto de deformación en la dirección  $y$ .

4) Cambiar el tamaño de la imagen  $f_3(x, y)$  en ambas direcciones, usando:

$$A_s = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} .$$

La imagen resultante se denota como  $f_4(x, y)$ , la cual esta normalizada ante el efecto de escalamiento en ambas direcciones. Finalmente la imagen  $f_4(x, y)$  es la imagen normalizada de la imagen original  $f(x, y)$ . Cabe mencionar que los procedimientos de normalización de imagen son totalmente invertibles, aplicando las matrices inversas de  $A_x, A_y, A_x$  y sumando el vector  $d$  a la imagen normalizada  $f_4(x, y)$ , se obtiene la imagen original  $f(x, y)$ . Sin embargo, para una implementación discreta de ambos procesos, el proceso de normalización y el proceso inverso requieren de una interpolación, la cual provoca una degradación en la calidad de la imagen.

Si la imagen  $g(x, y)$  es una imagen transformada de  $f(x, y)$ , aplicando una Transformación Affine General:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, d = 0 \quad ,$$

$g(x, y)$  está dada por  $g(x, y) = A \cdot f(x, y)$  y se obtienen las siguientes identidades:

$$m'_{p,q} = \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-i} a_{21}^j a_{22}^{q-j} m_{i+j, p+q-i-j} \quad , \quad (3.4)$$

$$\mu'_{p,q} = \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-i} a_{21}^j a_{22}^{q-j} \mu_{i+j, p+q-i-j} \quad . \quad (3.5)$$

Estas identidades se obtienen como se muestra a continuación:

Los momentos invariantes de la imagen  $g(x, y)$   $m'_{p,q}$  están dados por:

$$m'_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q g(x, y) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} A \cdot x^p y^q f(x, y) \quad . \quad (3.6)$$

Aplicando la transformación Affine general  $A$  en una coordenada  $(x, y)$ , se obtiene la coordenada transformada  $(x', y')$  :

$$\begin{aligned}x' &= a_{11}x + a_{12}y \\y' &= a_{21}x + a_{22}y\end{aligned}$$

Sustituyendo las coordenadas  $(x', y')$  en (3.6) se tiene:

$$m'_{pq} = \sum_{x=0}^{M-1N-1} \sum_{y=0}^{M-1N-1} (a_{11}x + a_{12}y)^p (a_{21}x + a_{22}y)^q f(x, y) \quad . \quad (3.7)$$

Aplicando el teorema binomial en (3.7):

$$(a_{11}x + a_{12}y)^p = \sum_{i=0}^p \binom{p}{i} a_{11}^i x^i a_{12}^{p-i} y^{p-i} = \sum_{i=0}^p \binom{p}{i} a_{11}^i a_{12}^{p-1} x^i y^{p-i} \quad , \quad (3.8)$$

$$(a_{21}x + a_{22}y)^q = \sum_{j=0}^q \binom{q}{j} a_{21}^j x^j a_{22}^{q-j} y^{q-j} = \sum_{j=0}^q \binom{q}{j} a_{21}^j a_{22}^{q-1} x^j y^{q-j} \quad . \quad (3.9)$$

Sustituyendo (3.8) y (3.9) en (3.7) se obtiene:

$$\begin{aligned}m'_{pq} &= \sum_{x=0}^{M-1N-1} \sum_{y=0}^{M-1N-1} \sum_{i=0}^p \binom{p}{i} a_{11}^i a_{12}^{p-1} x^i y^{p-i} \sum_{j=0}^q \binom{q}{j} a_{21}^j a_{22}^{q-1} x^j y^{q-j} f(x, y) \\&= \sum_{x=0}^{M-1N-1} \sum_{y=0}^{M-1N-1} \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-1} a_{21}^j a_{22}^{q-1} x^{i+j} y^{p+q-i-j} f(x, y) \\&= \sum_{x=0}^{M-1N-1} \sum_{y=0}^{M-1N-1} \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-1} a_{21}^j a_{22}^{q-1} x^{i+j} y^{p+q-i-j} f(x, y) \quad . \quad (3.10) \\&= \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-1} a_{21}^j a_{22}^{q-1} \sum_{x=0}^{M-1N-1} \sum_{y=0}^{M-1N-1} x^{i+j} y^{p+q-i-j} f(x, y)\end{aligned}$$

Usando la definición de la ecuación (3.1) se tiene:

$$m_{i+j, p+q-i-j} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^{i+j} y^{p+q-i-j} f(x, y) \quad . \quad (3.11)$$

Finalmente, sustituyendo (3.11) en (3.10) se obtiene:

$$m'_{p,q} = \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-i} a_{21}^j a_{22}^{q-j} m_{i+j, p+q-i-j} \quad . \quad (3.12)$$

De igual forma, se obtiene  $\mu'_{p,q}$ , quedando de la siguiente manera:

$$\mu'_{p,q} = \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-i} a_{21}^j a_{22}^{q-j} \mu_{i+j, p+q-i-j} \quad . \quad (3.13)$$

Usando esta relación entre los momentos invariantes de la imagen normalizada y la imagen original, se estiman los parámetros  $\alpha, \beta, \gamma, \delta$  de las matrices  $A_s, A_y, A_x$  de normalización. A continuación se describe con mayor detalle la determinación de los parámetros  $\alpha, \beta, \gamma$  y  $\delta$ :

1) Matriz de transformación shearing:

$$A_x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$$

A partir de la identidad 3.13 se tiene:

$$\mu_{30}^{(2)} = \mu_{30}^{(1)} + 3\beta\mu_{21}^{(1)} + 3\beta^2\mu_{12}^{(1)} + \beta^3\mu_{03}^{(1)} \quad , \quad (3.14)$$

donde  $\mu_{pq}^{(1)}$  son los momentos centrales de  $f_I(x,y)$ .

Haciendo  $\mu_{30}^{(2)}=0$ , se obtiene:

$$\mu_{30}^{(1)} + 3\beta\mu_{21}^{(1)} + 3\beta^2\mu_{12}^{(1)} + \beta^3\mu_{03}^{(1)} = 0 \quad . \quad (3.15)$$

A partir de (3.15), el parámetro  $\beta$  es calculado. Como se puede observar, en (3.15) se pueden obtener tres raíces en caso que  $\mu_{03}^{(1)} \neq 0$ , condición que generalmente se cumple en la mayor parte de las imágenes [33].

En particular, se pueden presentar los siguientes dos casos:

- 1) Una de las 3 raíces obtenidas es real y las otras dos son complejas.
- 2) Las 3 raíces son reales.

Cuando sucede el primer caso, simplemente se asigna a  $\beta$  la raíz real. En el segundo caso, se asigna a  $\beta$  la raíz que tenga un valor medio con respecto a las 3 raíces obtenidas. Por supuesto, bajo ciertas condiciones, el número de raíces en (3.15) puede variar. Por ejemplo, cuando todos los momentos involucrados en (3.15) son cero, esto provoca que se tenga un número infinito de soluciones.

Esto puede suceder cuando la imagen es simétrica de manera rotacional, como puede resultar un disco o un anillo. Para resolver esto, se proponen procedimientos de normalización detallados en [21] y [43].

2) Matriz de transformación shearing:

$$A_y = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$$

A partir de la identidad (3.13) se tiene:

$$\mu_{11}^{(3)} = \gamma\mu_{20}^{(2)} + \mu_{11}^{(2)} \quad . \quad (3.16)$$

Haciendo  $\mu_{11}^{(3)} = 0$ , se obtiene:

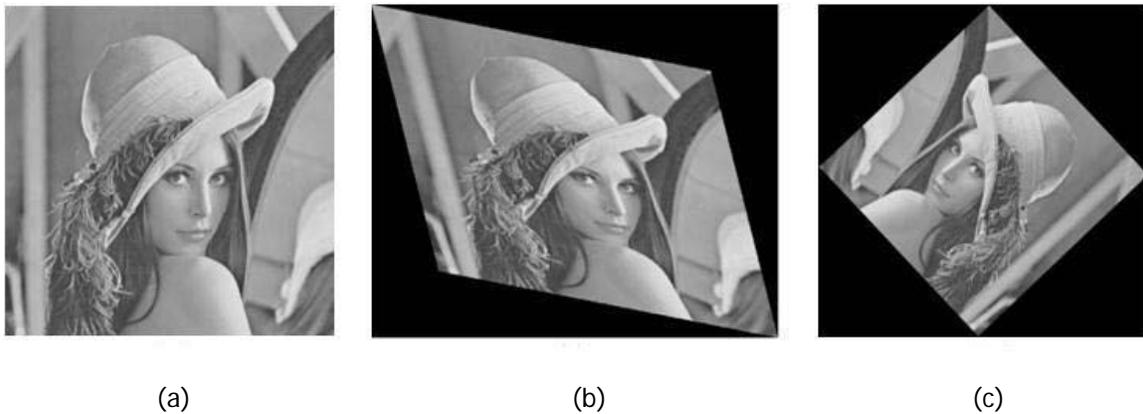
$$\gamma = -\frac{\mu_{11}^{(2)}}{\mu_{20}^{(2)}} \quad . \quad (3.17)$$

De este modo,  $\gamma$  genera una solución única.

3) Matriz de escalamiento:

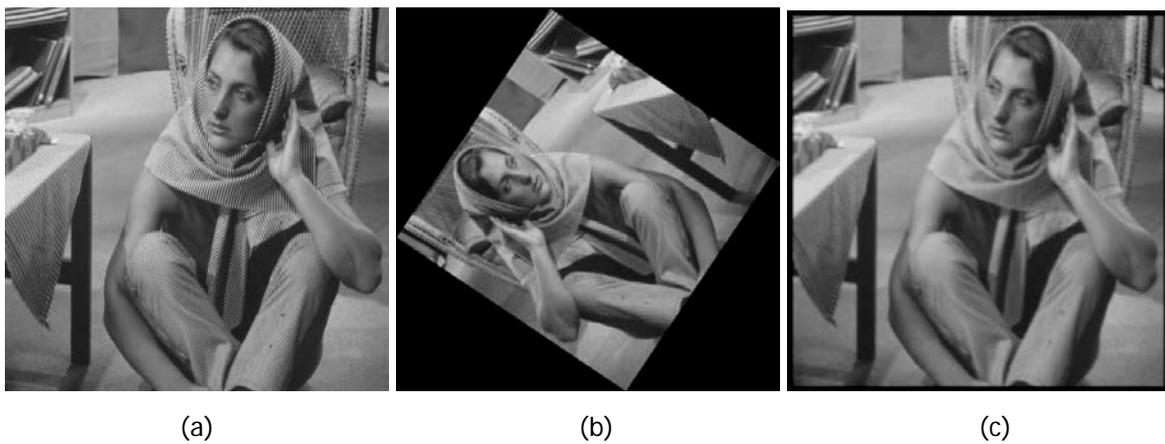
$$A_s = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \quad .$$

Las magnitudes de los parámetros de escalamiento  $\alpha$  y  $\delta$  se determinan por medio del cambio de escala de la imagen  $f_3(x,y)$  para establecer un tamaño estándar en direcciones horizontal y vertical. Sus signos son determinados a fin de que ambos momentos  $\mu_{50}^{(4)}$  y  $\mu_{05}^{(4)}$  sean positivos, aunque sus signos se pueden invertir aplicando un “volteo” o *flipping* de forma vertical y horizontal. En la figura 3.1 se muestra un ejemplo de normalización de imágenes, en el cual, (a) es la imagen original, (b) es la imagen (a) distorsionada geoméricamente y por último (c) es la imagen normalizada de ambas imágenes.



**Figura 3.1** Ejemplo del proceso de normalización de imagen. (a) Imagen original. (b) Imagen distorsionada y (c) imagen normalizada obtenida tanto de (a) como de (b).

Por otro lado, en la figura 3.2 se muestra como afecta el proceso inverso de normalización de imagen a la calidad de la imagen, (a) es la imagen original, (b) es la imagen normalizada y (c) es la imagen recuperada.



**Figura 3.2** Ejemplo del proceso inverso de normalización de imagen. (a) Imagen original. (b) Imagen normalizada y (c) imagen recuperada PSNR = 15.68 dB.

De los resultados que muestra la figura 3.2 y de la revisión bibliográfica realizada en el capítulo 2, se observa que en métodos basados en normalización de imágenes no es conveniente realizar la inserción de marca de agua en la versión normalizada obtenida de la imagen original, ya que el proceso inverso de normalización produce cambios visibles en la calidad de la imagen a proteger. Por ello, en este trabajo se propone una técnica de marca de agua que no afecta la calidad de la imagen, como se describe a continuación.

### **3.3. Proceso de inserción**

Aunque la imagen normalizada ofrece un dominio invariante a todas las distorsiones geométricas, la implementación discreta del proceso de normalización y su proceso inverso produce una degradación visual a la imagen, debido a los procesos de interpolación. Por lo tanto, en el algoritmo propuesto en vez de insertar la marca de agua en la imagen normalizada, el patrón de marca de agua es normalizado antes de su inserción, la normalización de la imagen original es usada solamente para determinar la energía de inserción adecuada, por lo que la inserción de marca de agua se lleva a cabo en el dominio espacial de la imagen sin normalizar. En esta sección se describe la creación del patrón de marca de agua y el proceso de inserción del mismo como sigue:

- 1) Aplicar el procedimiento de normalización de imágenes descrito en la sección anterior a la imagen original para generar una imagen normalizada.
  
- 2) Dividir la imagen normalizada en bloques de 8x8 píxeles y seleccionar los bloques con textura fuerte. Para estimar una complejidad de textura de cada bloque de la imagen normalizada, se usa la técnica propuesta en [44]. Primero, los coeficientes de DCT de cada bloque son cuantificados usando una matriz de cuantificación  $Q$  con un factor de calidad  $F_c = 50$ , que usa una codificación entrópica JPEG. La figura 3.3 muestra los coeficientes de la matriz de cuantificación  $Q$  con un  $F_c = 50$ .

$$\begin{aligned}
 Q = [ & 3 \ 5 \ 7 \ 9 \ 11 \ 13 \ 15 \ 17; \\
 & 5 \ 7 \ 9 \ 11 \ 13 \ 15 \ 17 \ 19; \\
 & 7 \ 9 \ 11 \ 13 \ 15 \ 17 \ 19 \ 21; \\
 & 9 \ 11 \ 13 \ 15 \ 17 \ 19 \ 21 \ 23; \\
 & 11 \ 13 \ 15 \ 17 \ 19 \ 21 \ 23 \ 25; \\
 & 13 \ 15 \ 17 \ 19 \ 21 \ 23 \ 25 \ 27; \\
 & 15 \ 17 \ 19 \ 21 \ 23 \ 25 \ 27 \ 29; \\
 & 17 \ 19 \ 21 \ 23 \ 25 \ 27 \ 29 \ 31;]
 \end{aligned}$$

**Figura 3.3** Matriz de cuantificación  $Q$ . Factor de calidad  $F_c = 50$ .

De acuerdo a [44], si el  $k$ -ésimo bloque  $F_k(u,v), 0 \leq u, v \leq 7$  satisface la condición de la ecuación (3.18), este bloque es clasificado como textura fuerte, en otro caso el bloque pertenece a una textura débil.

$$\text{si } F_k(0,0) > T_1 \text{ y } \text{numero}\{ \lfloor F_k(u,v)/Q(u,v) \rfloor \neq 0 \} > T_2 \quad (3.18)$$

donde la notación  $\lfloor \bullet \rfloor$  es una función de redondeo hacia 0 y la función  $\text{numero}\{\text{condición}\}$  obtiene el número de elementos que satisfacen la condición, y  $Q(u,v)$  es el valor de la matriz de cuantificación en la frecuencia espacial  $(u,v)$ .  $T_1$  y  $T_2$  son dos valores umbral predeterminados, el valor de coeficiente de frecuencia cero DC del  $k$ -ésimo bloque  $F_k(0,0)$  representa el promedio de luminancia del bloque y este se encuentra en un rango de  $[0, (2^l - 1)S]$  para un bloque de tamaño  $S \times S$  en nivel de escala de grises. Por ejemplo, si  $l=8$  bits y  $S=8$  (bloque de  $8 \times 8$ ), el rango de DC es  $[0, 2040]$ , de modo que, cuando el bloque es plano y negro en su totalidad, el valor de DC para  $F_k(0,0)$  es 0 y, cuando el bloque es plano y blanco en su totalidad, el valor de DC para  $F_k(0,0)$  es 2040. El valor umbral  $T_1$  usado para la simulación computacional es 230, en el cual la intensidad promedio del bloque es cercana a 255 en la escala de grises cuando  $l=5$ .

De acuerdo al sistema visual humano SVH, el detalle de esta intensidad se considera plano con uní-tono. Por otro lado, el rango de valores para  $\text{numero}\{[F_k(u,v)/Q(u,v)] \neq 0\}$  es  $[1,64]$ , debido a que el tamaño del bloque es  $8 \times 8$  haciendo un total de 64 coeficientes. Cuando el bloque contiene altas frecuencias, es decir, contiene detalles (por ejemplo una región con textura fuerte), los valores de alta frecuencia obtenidos después de aplicar una cuantificación con la matriz  $Q$  deben ser diferentes de cero, por lo tanto, si se desea obtener un bloque con textura fuerte, el número de altas frecuencias diferentes de cero debe ser mayor que un valor umbral  $T_2$ .

La matriz de cuantificación  $Q$  usada es la misma que se utiliza para la compresión JPEG con el factor de calidad 50. La combinación de ambas condiciones en la ecuación (3.18) permite obtener un bloque con textura fuerte y con detalles suficientemente claros para el SVH.

Tomando en cuenta los hechos antes mencionados, para determinar los umbrales  $T_1$  y  $T_2$  se realizaron pruebas asignando valores desde 230 hasta 245 en intervalos de 5 para el caso de  $T_1$ , para el caso de  $T_2$  se asignaron valores desde 10 hasta 14, como se muestra en la tabla 3.1.

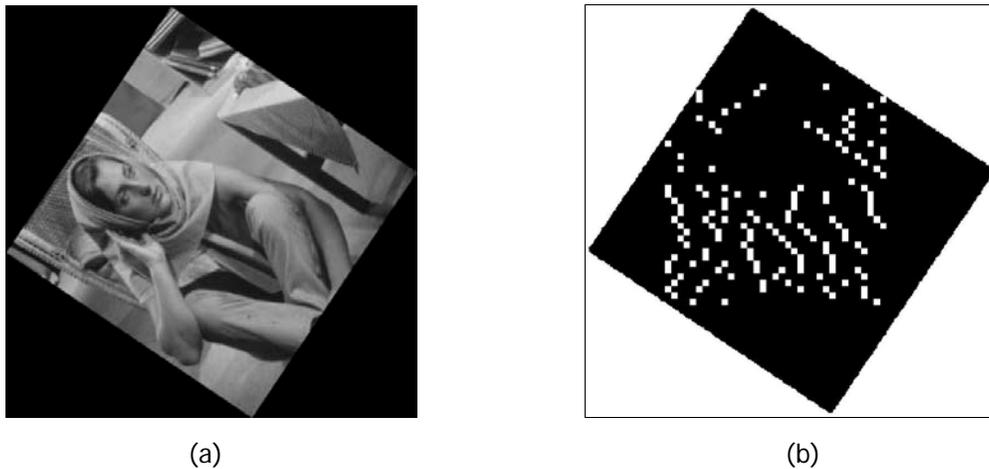
TABLA 3.1  
 NUMERO DE BLOQUES PROMEDIO CON TEXTURA FUERTE PARA  
 VALORES UMBRAL  $T_1$  Y  $T_2$ .

UMBRAL $T_2$	UMBRAL $T_1$			
	230	235	240	245
10	155	161	177	185
11	149	156	162	179
12	137	151	157	169
13	<b>130</b>	143	149	158
14	123	137	141	149

De la tabla 3.1 se puede observar que los valores óptimos para  $T_1$  y  $T_2$  en el esquema de marca de agua propuesto son 230 y 13 respectivamente, debido a que se considera que la marca de agua tenga un tamaño máximo de 64 bits, de modo que está puede ser insertada de forma redundante 16 veces insertando 8 bits de marca de agua en las posiciones correspondientes a los coeficientes de frecuencia media DCT en el bloque con textura fuerte, de esta forma, se necesita una cantidad total de 128 bloques con textura fuerte, que aproximadamente proporcionan los valores de umbral  $T_1$  y  $T_2$ .

Cabe señalar que aunque el resto de valores para  $T_1$  y  $T_2$  también proporcionan una cantidad suficiente de bloques con textura fuerte, se toma en cuenta el hecho de que la calidad de la imagen puede ser afectada.

Un ejemplo de clasificación de bloques se muestra en la figura 3.4, en la cual, los bloques blancos son bloques de textura fuerte y los bloques negros son texturas débiles.



**Figura 3.4** Ejemplo de clasificación de texturas. (a) Imagen original, (b) clasificación de texturas fuertes (bloques en color blanco).

3) Generar un patrón bi-dimensional pseudo-aleatorio  $R$ , cuyo tamaño es el mismo que la imagen original. Enmascarar un patrón binario  $M$  que funciona como molde al patrón pseudo-aleatorio  $R$  para generar el patrón  $MR$ .

4) Generar un vector de marca de agua binaria  $W = \{w_i | w_i = -1 \text{ o } 1, i = 1..n\}$ , cuyos elementos son pseudo-aleatorios y es generado por una llave secreta del propietario de la imagen. Después se multiplica por un factor de ganancia  $\alpha_l$  al vector de marca de agua, y se genera  $W' = \{\alpha_l w_i | w_i = -1 \text{ o } 1, i = 1..n\}$ .

5) Dividir el vector de marca de agua  $W'$ , generado por el paso 4 de este proceso, en  $N$  grupos de  $L$  elementos.  $L$  puede tener un valor desde 1 hasta 22, el cual es equivalente al número de coeficientes de frecuencia media en el bloque de DCT de 8x8 píxeles. Por ejemplo, si la longitud del vector de marca de agua  $W'$  es 500 y si el número de coeficientes  $L$  que se usan para la inserción de marca de agua es igual a 5, el número de grupos  $N$  entonces es 100 ( $N=500/5$ ).

6) Los elementos del patrón  $MR$  generado en el paso 3 de este proceso, que corresponden a los coeficientes en la frecuencia de banda media de los bloques de textura fuerte de la imagen normalizada, se reemplazan por los elementos de marca de agua  $W'$ . La Transformada Inversa de Coseno Discreta (IDCT) se aplica al patrón con la señal de marca de agua y se genera el patrón de marca de agua normalizado  $MR_w$ .

7) Aplicar el proceso inverso de normalización de imágenes al patrón de marca de agua  $MR_w$  para obtener un patrón bidimensional de marca de agua  $WP$ .

8) El patrón de marca de agua  $WP$  se inserta en la imagen original usando una inserción aditiva en el dominio espacial. La formula de la inserción esta dada en (3.19).

$$I_w = I_o + \alpha_2 WP \quad , \quad (3.19)$$

donde  $I_o$  e  $I_w$  son la imagen original e imagen marcada respectivamente y  $\alpha_2$  es la energía de inserción de la marca de agua. La figura 3.5 muestra el proceso de inserción de marca de agua descrito anteriormente. A grandes rasgos, en el proceso de inserción de marca de agua del algoritmo propuesto, se genera un patrón bi-dimensional normalizado usando los mismos factores geométricos de la normalización de la imagen original y para que éste patrón de marca de agua sea más robusto a los esquemas de procesamiento de señales, además de mantener su imperceptibilidad, se tomaron en cuenta las características de texturas de la imagen original para realizar una inserción adaptable. Cabe mencionar que la normalización del patrón de marca de agua en lugar de la misma imagen evita una distorsión en la imagen marcada.

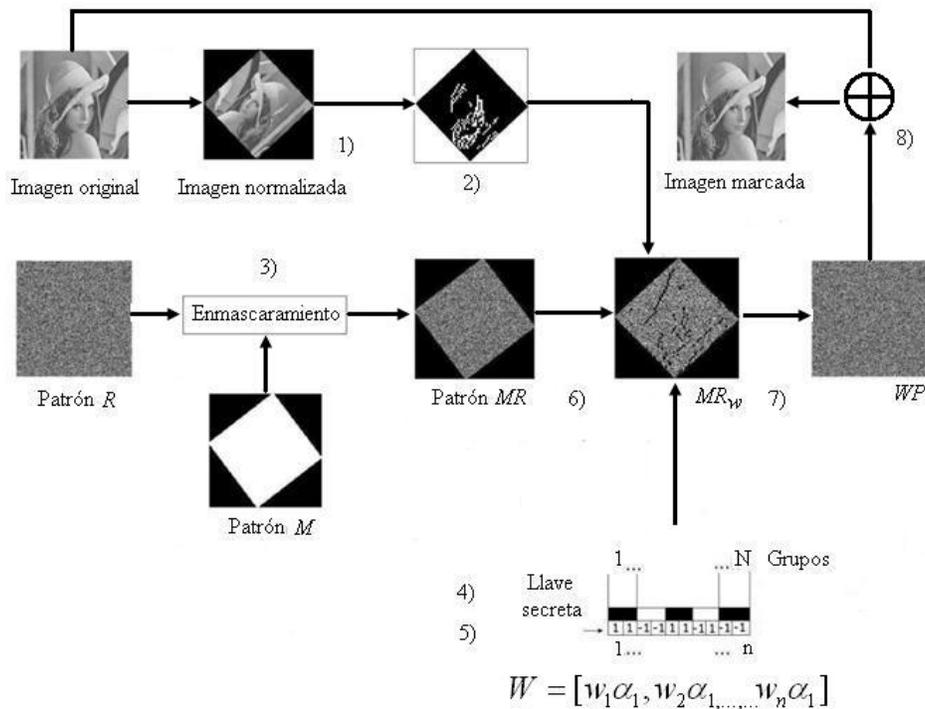


Figura 3.5 Diagrama del proceso de inserción de marca de agua.

### 3.4. Proceso de extracción

El proceso de extracción de marca de agua se describe como sigue:

- 1) Se aplica el proceso de normalización a la imagen marcada y se obtiene la versión normalizada de la imagen marcada.
- 2) Se aplica la DCT a los bloques de 8x8 píxeles de la imagen marcada normalizada, después se clasifican los bloques en bloques con textura fuerte y bloques con textura débil. Desde los bloques con textura fuerte, se extraen los coeficientes marcados localizados en el rango de frecuencia media.

Concatenando los vectores de coeficientes marcados extraídos desde todos los bloques con texturas fuertes, se genera un vector de coeficientes marcados  $CW = [cw_1, cw_2, \dots, cw_{N-1}, cw_N]$ .

- 3) Se extrae el vector de marca de agua, realizando la siguiente operación usando los elementos del vector  $CW$ .

$$\hat{W} = [\hat{w}_1, \hat{w}_2, \dots, \hat{w}_{N-1}, \hat{w}_N] \quad , \quad (3.20)$$

donde  $\hat{w}_k = \text{sign}(cw_k)$ ,  $\text{sign}$  es una función de signo.

La figura 3.6 muestra el proceso de extracción de marca de agua.

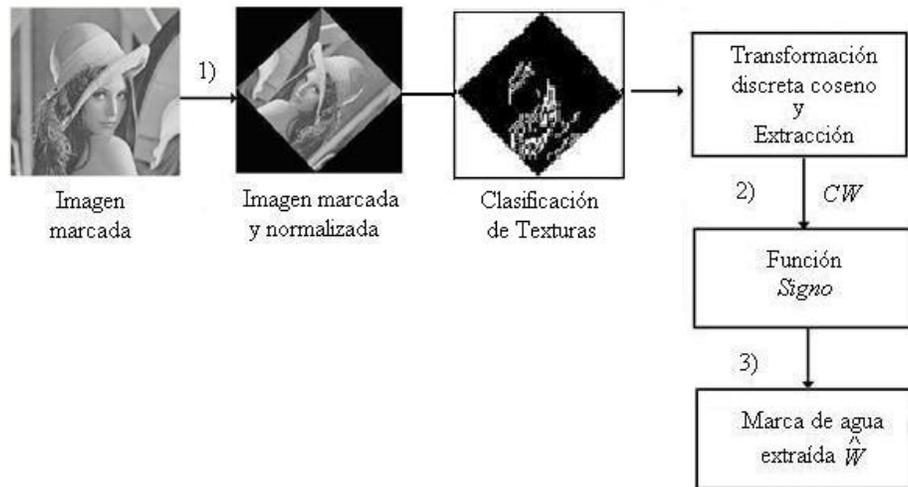


Figura 3.6 Diagrama del proceso de extracción de marca de agua.

### 3.5. Resultados experimentales

Para evaluar el esquema propuesto se llevaron a cabo simulaciones computacionales en el software Matlab 7 en las cuales se emplearon imágenes de 512 x 512 píxeles en escalas de grises con 8 bits de resolución: Lena, Peppers, Mandrill, Boat, Bridge, Goldhill, Barbara, Camera, Bird y Lake [45]. De acuerdo a la ecuación (3.18), se determinaron dos valores umbrales  $T_1$  y  $T_2$ , los cuales se emplearon para clasificar cada bloque de la imagen en dos clases: bloques con textura fuerte y bloques con textura débil. A estos umbrales se les asignó los valores 230 y 13, respectivamente. El esquema propuesto es evaluado desde el punto de vista de imperceptibilidad, robustez y no ambigüedad de la marca de agua extraída.

#### 3.5.1 Imperceptibilidad de la señal de la marca de agua

Un vector de marca de agua binario de 64 bits es insertado 16 veces redundantemente dentro de varias imágenes.

Para determinar los factores de energía de la marca de agua  $\alpha_1$  y  $\alpha_2$ , se realizó el proceso de inserción de marca de agua con las siguientes condiciones: el factor de energía  $\alpha_1$  es incrementado en intervalos de 2, desde el valor 2 hasta 10, por su parte, el factor de energía de la marca de agua  $\alpha_2$  es incrementado en intervalos de 0.02 desde el valor 0.01 a 0.09, para medir la relación entre la tasa de bits erróneos y la imperceptibilidad de la marca de agua. La tabla 3.2 muestra los resultados obtenidos. Con este fin, la Relación Señal a Ruido Pico (PSNR, por sus siglas en inglés) dada por (3.21), entre la imagen original y la imagen marcada fue calculada para cada valor de  $\alpha_1$  y  $\alpha_2$ .

$$PSNR(dB) = 10 \log_{10} \left( \frac{MN255^2}{\sum_{i=1}^M \sum_{j=1}^N (I_o(i, j) - I_w(i, j))^2} \right), \quad (3.21)$$

donde  $M \times N$  es el tamaño de la imagen,  $I_o, I_w$  son la imagen original y la imagen marcada, respectivamente, 255 denota el máximo valor que puede tomar un píxel en la imagen, ya que la resolución de las imágenes usadas es de 8 bits. Por su parte, la tasa de bits erróneos se define como el resultado de dividir los bits recuperados erróneamente y el número total de bits que componen la marca de agua.

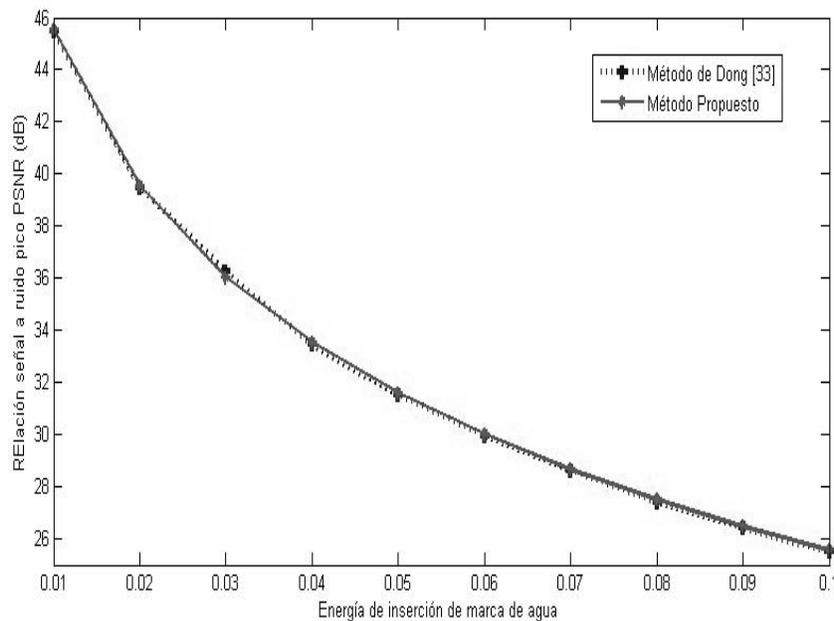
TABLA 3.2  
RELACIÓN PROMEDIO ENTRE LA TASA DE BITS ERRONEOS (BER) Y LA RELACIÓN SEÑAL A RUIDO PICO (PSNR).

$\alpha_2$	$\alpha_1$				
	2	4	6	8	10
0.01	47.23 / 0.18	46.92 / 0.17	45.84 / 0.16	44.56 / 0.14	42.09 / 0.13
0.03	46.81 / 0.13	45.01 / 0.12	<b>36.15 / 0.04</b>	34.05 / 0.05	33.17 / 0.04
0.05	45.57 / 0.12	44.14 / 0.11	31.87 / 0.04	30.93 / 0.04	29.24 / 0.03
0.07	42.26 / 0.12	39.11 / 0.10	29.58 / 0.03	27.84 / 0.02	26.50 / 0
0.09	39.07 / 0.11	38.05 / 0.09	26.07 / 0.02	25.98 / 0.02	24.04 / 0

$N_1/N_2$  en la tabla indican el PSNR promedio y BER promedio respectivamente, obtenidos de las imágenes marcadas.

Por otro lado, con el propósito de realizar un comparativo con el esquema propuesto por Dong et al., el factor de energía de la marca de agua  $\alpha_2$  es incrementado en intervalos de 0.01 desde el valor 0.01 a 0.1, para medir la relación entre este factor y la imperceptibilidad de la señal de marca de agua. El valor de  $\alpha_1$  usado en el proceso de generación de la secuencia de marca de agua propuesto en este trabajo fue el valor 6 en todos los casos. La figura 3.7 muestra la relación entre el valor de  $\alpha_2$  y el promedio de la PSNR obtenido en 10 imágenes aplicando nuestro esquema propuesto y el esquema propuesto por Dong et al.

Como se puede observar en la figura, la imperceptibilidad de marca de agua expresada por la PSNR con diferentes valores de  $\alpha_2$  en ambos esquemas es muy similar y también, ambos esquemas, cuando se usan los valores pequeños de  $\alpha_2 \leq 0.03$ , la PSNR es mayor que 36dB, lo cual garantiza la imperceptibilidad de la marca de agua.



**Figura 3.7** Relación entre la energía de marca de agua  $\alpha_2$  y la imperceptibilidad de la marca de agua en el esquema propuesto y el esquema de Dong. et al.

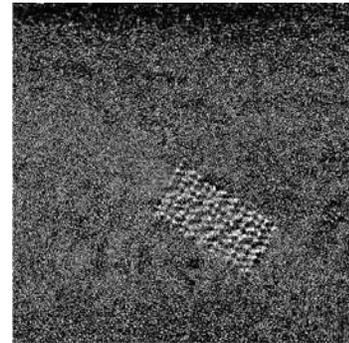
En la figura 3.8 se muestra un conjunto de 5 imágenes de prueba (Mandrill, Goldhill, Bridge, Lena y Barbara), con sus respectivas versiones marcadas. Los valores de Relación Señal a Ruido Pico obtenidos para cada imagen fueron: Mandrill (38.10 dB), Goldhill (37.05 dB), Bridge (36.48 dB), Lena (36.20 dB) y Barbara (36.03 dB).



(a)



(b)



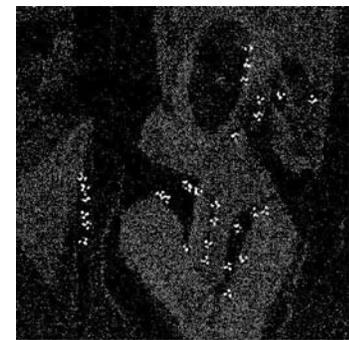
(c)



(d)



(e)



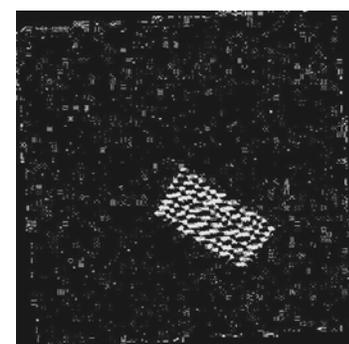
(f)



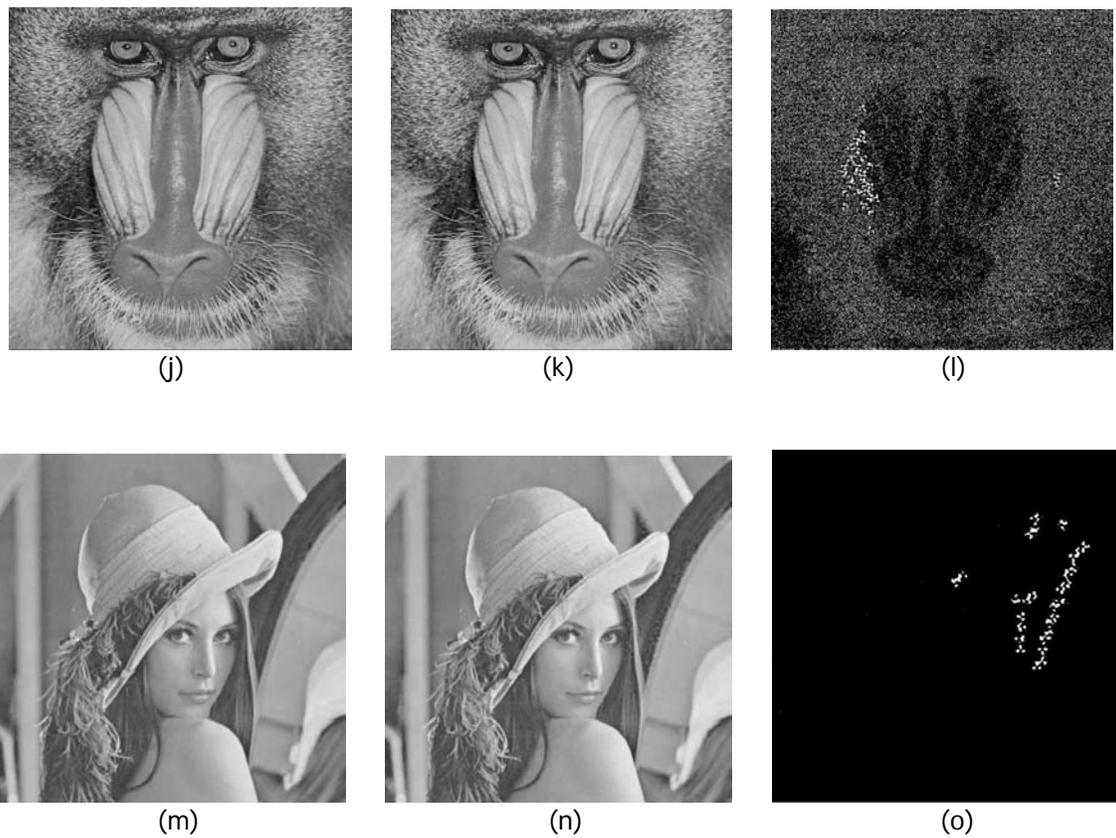
(g)



(h)



(i)



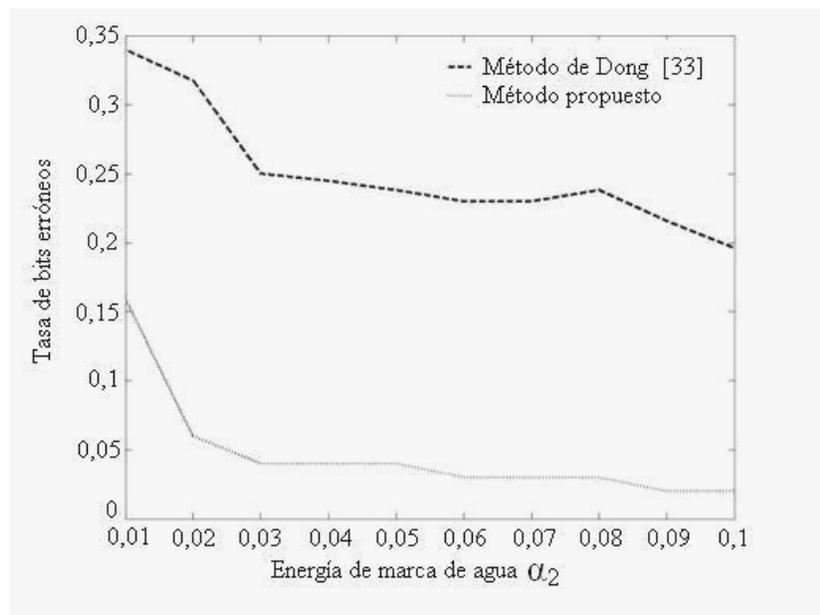
**Figura 3.8** Imágenes originales (a), (d), (g), (j) e (m). Versiones marcadas (b), (e), (h), (k), y (n), respectivamente. Imágenes de Error (c), (f), (i), (l) y (o).

### 3.5.2. Ambigüedad de marca de agua extraída

En el esquema de marca de agua, es muy importante que la señal de marca de agua extraída no sea ambigua, sobre todo si se trata de un mensaje constituido por texto en Código Estándar Estadounidense para el Intercambio de Información (ASCII) o la marca de agua es un logotipo.

Considerando esta situación, la tasa de bits erróneos (BER) de la secuencia binaria de marca de agua extraída respecto a la insertada fue calculada, variando el valor de  $\alpha_2$ .

La figura 3.9 muestra la relación entre  $\alpha_2$  y la BER de nuestro sistema propuesto y el propuesto por Dong et al. Como podemos observar en la figura 3.9, cuando los valores de  $\alpha_2$  son menores que 0.03, la BER de nuestro esquema es de 0.05, lo cual indica que la señal de marca de agua es suficientemente clara. Mientras que en el esquema de Dong et al., cuando el valor de  $\alpha_2 \leq 0.03$ , la BER es mayor que 0.25. Esto significa que aproximadamente un cuarto de bits de la secuencia de marca de agua extraída son erróneos, como consecuencia de esto, cuando la señal de marca de agua es un mensaje, el mensaje extraído en el esquema de Dong et al., no es legible.



**Figura 3.9** Relación entre la energía de marca de agua  $\alpha_2$  y la BER en el esquema propuesto y el de Dong et al.

### 3.5.3 Robustez de marca de agua

Para realizar una evaluación de robustez de la marca de agua en condiciones equiparables entre el esquema propuesto en esta tesis y el método de Dong et al. [33], se

hace uso de la herramienta estándar que aplica diversas distorsiones en las imágenes marcadas, Stirmark Benchmark 4.0 [13], [14], tomando en cuenta los ataques que son comunes para evaluar los esquemas de marca de agua orientados a combatir las distorsiones geométricas sin descuidar las operaciones de procesamiento de señales. Adicionalmente, se aplicaron algunas distorsiones que no vienen en la versión de Stirmark 4.0 y estas fueron aplicadas usando Matlab. La tabla 3.3 muestra la robustez de marca de agua en términos de la tasa de bits erróneos (BER) de la marca de agua extraída después de los correspondientes ataques aplicados. En todos los casos, los valores de  $\alpha_1$  y  $\alpha_2$  son 6 y 0.03 respectivamente para el método propuesto en este trabajo, en el caso del método de Dong. et al., el factor de energía de marca de agua utilizado es 0.03.

Para el caso de el esquema propuesto en esta tesis, la señal de marca de agua es suficientemente robusta a casi todos los tipos de distorsión geométrica así como a la mayoría de los procesamientos de señal comunes, tales como compresión de imágenes JPEG, contaminación por ruido y filtrado, ya que la BER de la señal de marca de agua extraída respecto a la original es menor que 0.11, excepto ante la compresión JPEG con un factor de calidad 25 (en este caso BER=0.14), el ataque de Stirmark RBA (*Random Bending Attack* por sus siglas en inglés), en este caso se obtuvo BER =0.59 y ante los ataques que involucran un recorte en la imagen, problema común en los métodos basados en normalización de imagen.

Por su parte, el algoritmo propuesto por Dong. et al.[33], muestra robustez ante la mayoría de las distorsiones aplicadas excepto para Stirmark RBA, ataques que implican recorte de la imagen y compresión JPEG con factor de calidad menor de 25, aunque, como se puede observar, la BER obtenida para todos los casos es mayor que 0.25, y como se comentó en el punto 3.5.2 de este capítulo, se tiene una pérdida de aproximadamente un cuarto de bits de la secuencia de marca de agua extraída. Respecto a las imágenes comprimidas usando el esquema de compresión JPEG con un factor de calidad menor a 25, estas imágenes se

distorsionan considerablemente por la alta tasa de compresión, por lo tanto en la mayoría de las ocasiones, la imagen pierde su valor comercial.

TABLA 3.3  
COMPARATIVO DE TASA DE BITS ERRONEOS PROMEDIO, MAXIMA Y MINIMA ENTRE EL METODO PROPUESTO Y EL DE DONG. ET AL.,[33]. INSERTANDO UNA MARCA DE AGUA DE 64 BITS Y USANDO UN FACTOR DE ENERGÍA DE MARCA DE AGUA= 0.03

ATAQUES	BER PROMEDIO METODO PROPUESTO	BER MAXIMO METODO PROPUESTO	BER MINIMO METODO PROPUESTO	BER PROMEDIO DONG ET AL.[33]	BER MAXIMO DONG ET AL.[33]	BER MINIMO DONG ET AL.[33]
Sin ataque	0.04	0.05	0.03	0.25	0.27	0.24
Ruido Gaussiano con media $m = 0$ , varianza $\sigma = 0.01$	0.09	0.11	0.07	0.27	0.30	0.27
Ruido impulsivo densidad de 0.09	0.06	0.08	0.03	0.28	0.29	0.26
Sharpening	0.06	0.07	0.05	0.26	0.29	0.24
Cambio de aspecto (1.2; 1.0)	0.06	0.09	0.04	0.28	0.29	0.27
Flipping horizontal y vertical	0.04	0.05	0.03	0.26	0.27	0.25
Shearing en dirección y con un factor de (0.7%).	0.06	0.08	0.05	0.26	0.29	0.25
Stirmark filtro de mediana 3x3	0.11	0.13	0.09	0.27	0.28	0.25
Stirmark compresión JPEG QF=50	0.06	0.09	0.05	0.25	0.28	0.25
Stirmark compresión JPEG QF=25	<i>0.14</i>	<i>0.16</i>	<i>0.13</i>	<i>0.30</i>	<i>0.31</i>	<i>0.28</i>
Stirmark rotación con ángulo de 80°	0.06	0.08	0.04	0.28	0.29	0.26
Stirmark escalamiento 1.5	0.08	0.09	0.07	0.26	0.28	0.24
Stirmark Transformación de Affine	0.08	0.09	0.06	0.27	0.28	0.25
Stirmark Remover Lineas RML = 50	0.10	0.11	0.08	0.31	0.32	0.27
Stirmark recorte	<i>0.62</i>	<i>0.65</i>	<i>0.60</i>	<i>0.55</i>	<i>0.58</i>	<i>0.51</i>
Stirmark rotación de 2° y recorte	<i>0.60</i>	<i>0.63</i>	<i>0.58</i>	<i>0.59</i>	<i>0.64</i>	<i>0.57</i>
Stirmark random bending attack (RBA)	<i>0.59</i>	<i>0.61</i>	<i>0.45</i>	<i>0.50</i>	<i>0.57</i>	<i>0.41</i>

Los datos en cursiva indican que el algoritmo no es robusto ante ese ataque.

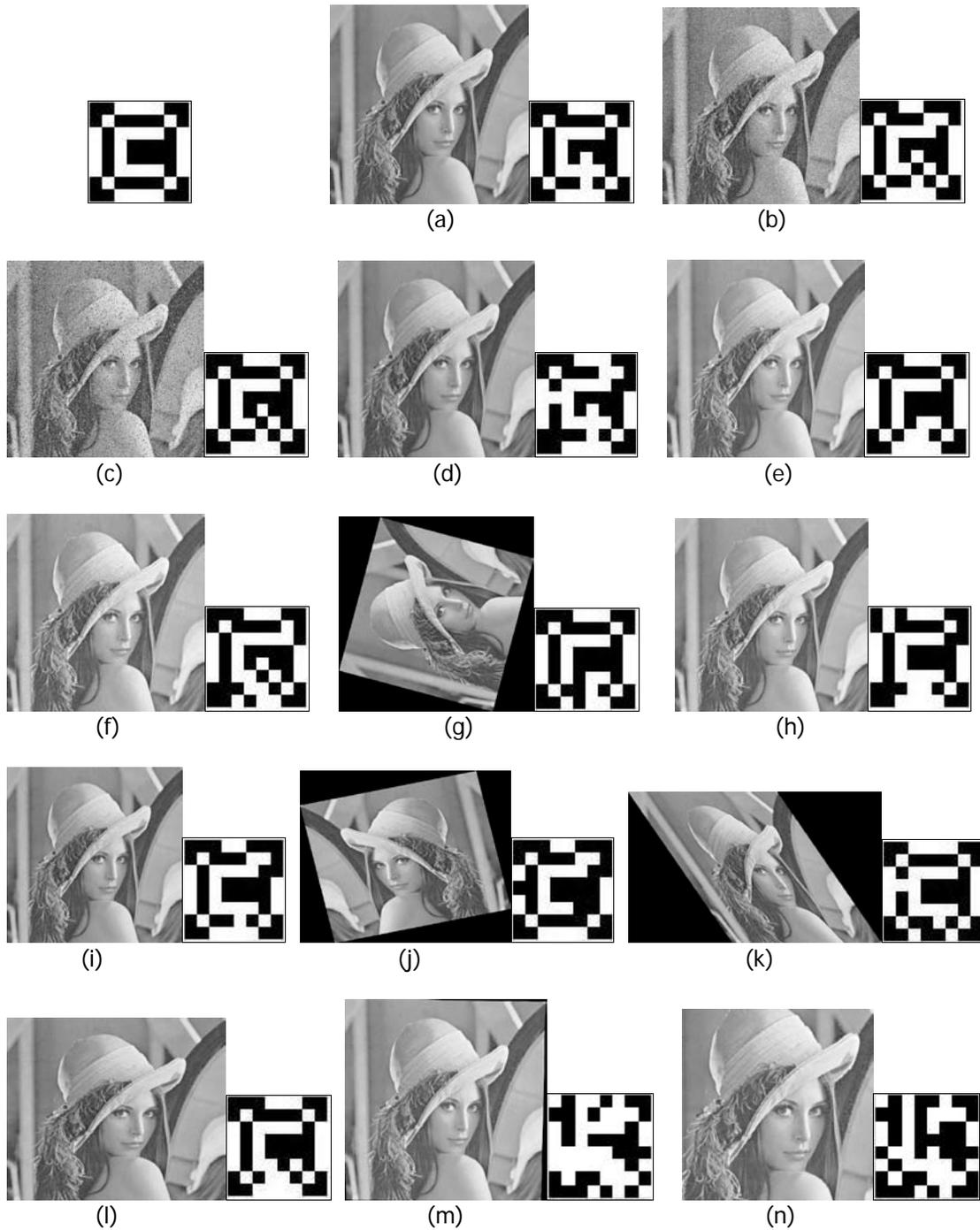
Por otro lado, se llevo a cabo la inserción de un logotipo binario (valores 1,-1) de 64 bits en la imagen Lena, que representa al símbolo del copyright ©, el cual es usado para indicar que una obra está sujeta al derecho de autor, usando los mismos valores para los parámetros  $\alpha_1$  y  $\alpha_2$ , aplicando las siguientes distorsiones:

- a) Sin ataque.
- b) Contaminación con ruido Gaussiano media  $M = 0$  y varianza  $\sigma = 0.01$ .
- c) Ruido impulsivo con densidad 0.08.
- d) Stirmark filtro mediano ventana  $3 \times 3$ .
- e) Stirmark compresión JPEG con factor de calidad  $QF = 50$ .
- f) Stirmark compresión JPEG con factor de calidad  $QF = 25$ .
- g) Rotación con  $80^\circ$  grados.
- h) StirMark remover líneas  $RML = 50$ .
- i) Stirmark escalamiento 1.5.
- j) Transformación Affine :  $\begin{pmatrix} -1.01 & 0.2 \\ 0.2 & 0.8 \end{pmatrix}$
- k) Shearing en dirección del eje y con un factor de (0,7%).
- l) Cambio de aspecto: (1.3, 1.0).
- m) Stirmark Random Bending Attack (RBA).
- n) Stirmark Cropping 75.

En la tabla 3.4 se muestra la correlación normalizada obtenida después de aplicar las distorsiones (a)-(n) y la figura 3.10 muestra el logotipo recuperado, junto con la imagen atacada. La correlación normalizada está dada por (3.22):

$$N_c = \frac{\sum_{i=1}^n W(i)W'(i)}{\sqrt{\sum_{i=1}^n W(i)^2} \sqrt{\sum_{i=1}^n W'(i)^2}} \quad (3.22)$$

Los resultados obtenidos, garantizan una legibilidad de marca de agua aceptable, excepto cuando se aplica a la imagen una compresión JPEG con factor de calidad  $\leq 25$ , Stirmark RBA y recorte con Stirmark.



**Figura 3.10** Logotipo original y versión marcada de imagen Lena con ataques (a)-(n), con su correspondiente logotipo recuperado.

TABLA 3.4  
CORRELACIÓN NORMALIZADA OBTENIDA DE LA IMAGEN LENA

	DISTORSIÓN	CN
(a)	Sin ataque	0.9844
(b)	Ruido Gaussiano	0.9219
(c)	Ruido impulsivo	0.9375
(d)	Stirmark filtro mediano 3x3	0.8906
(e)	Stirmark JPEG QF = 50	0.9375
(f)	Stirmark JPEG QF = 25	0.8438
(g)	Rotación	0.9219
(h)	Stirmark RML=50	0.9063
(i)	Stirmark escalamiento 1.5	0.9219
(j)	Stirmark Affine	0.9063
(k)	Shearing	0.9375
(l)	Cambio de aspecto	0.9375
(m)	Stirmark RBA	0.5156
(n)	Stirmark cropping 75	0.4688

Finalmente, el comportamiento del algoritmo propuesto es comparado con tres métodos basados en estrategias diferentes a la propuesta en este trabajo de tesis.

El primer método utilizado en la comparación es el propuesto por Ruanaidh y Pun en [12], el cual está basado en el uso de la FMT como dominio invariante para insertar y detectar la marca de agua. El segundo método en la comparación fue propuesto por Pereira y Pun en [26], el cual está basado en el uso de una plantilla que es utilizada como señal de re-sincronización de marca de agua en el proceso de detección. El tercer y último método es propuesto por Tang y Hang en [29]. Este método utiliza las características relevantes de la imagen para estimar factores geométricos que sirven para restaurar la imagen a su estado original en el proceso de detección.

Los parámetros utilizados para realizar la comparación del comportamiento del algoritmo son: tipo de detección y longitud de marca de agua utilizados en el método, y robustez ante los siguientes ataques: compresión JPEG, escalamiento, cambio de aspecto, rotación, deformación en planos paralelos (*shearing*), filtrado mediano y contaminación de imagen con ruido Gaussiano. En la tabla 3.5 se muestran los resultados del comparativo en cuestión de comportamiento. Un guión corto en la tabla indica que el parámetro de comparación no es reportado en el método.

En algunos métodos, los resultados reportados no expresan un rango en concreto de la distorsión aplicada a la imagen marcada, por tal motivo, los autores de cada método emplean la palabra “detectada”, para reportar que la marca de agua fue robusta ante dicho ataque.

TABLA 3.5  
COMPARACIÓN DE RENDIMIENTO CON MÉTODOS BASADOS EN DIFERENTES ESTRATEGIAS

PARAMETRO DE COMPARACIÓN	Ruanaidh y Pun [12] (Basado en Dominio Invariante)	Pereira y Pun.[26] (Basado en señal de re-sincronización)	Tang y Hang [29] (Basado en características relevantes)	Método Propuesto (Basado en normalización de imagen)
Compresión JPEG (QF)	75-100	75-100	40-100	25-100
Escalamiento	Detectada	0.75 - 2	-	0.4 – 2
Cambio de aspecto	-	Detectada	-	Detectada
Rotación	0°-360°	Detectada	1°-5°	0° - 360°
Deformación de planos paralelos	-	(X1%, Y1%)	(X1%, Y1%)	(X5%, Y5%)
Filtrado mediano	-	3x3	2x2	3x3
Ruido Gaussiano	-	-	Detectada	Detectada
Tipo de detección	Ciega	Necesaria imagen original	Ciega	Ciega
Longitud de marca de agua	104 bits	60 bits	16 bits	64 bits

Un guión en la tabla indica que el parámetro no es reportado en el método.

De la tabla 3.5, se puede apreciar que el método propuesto en este artículo presenta un mejor comportamiento con respecto a los métodos usados en el comparativo en cuanto a compresión JPEG, escalamiento, cambio de aspecto, rotación, shearing, filtrado de mediana, contaminación por ruido Gaussiano, teniendo una mayor tolerancia ante dichos ataques con respecto a los otros métodos.

## **Conclusiones**

En este capítulo se presento una técnica de marca de agua robusta a distorsiones geométricas y otros esquemas de procesamiento de señales. En el método de marca de agua propuesto, se hizo uso de una técnica de normalización de imágenes para obtener características invariantes de la imagen ante las distorsiones geométricas. Los procesos de inserción y detección de la marca de agua fueron realizados en el dominio de la Transformada Discreta del Coseno (DCT). Una clasificación de texturas basada en el dominio de la DCT fue usada para clasificar cada bloque de la imagen a fin de poder insertar una marca de agua fuerte, manteniendo al mismo tiempo la imperceptibilidad de la misma. La técnica propuesta es una técnica de marca de agua con detección a ciegas, en la cual, la imagen original no está disponible en el proceso de detección de la marca de agua. Los resultados experimentales muestran la imperceptibilidad de la marca de agua y su robustez ante las distorsiones geométricas, como son rotación, escalamiento, transformaciones Affine, y otros esquemas de procesamiento de señales, tales como compresión JPEG, contaminación de imagen por ruido Gaussiano e impulsivo.



# Capítulo 4

## Esquema Robusto de Marca de Agua Basado en Modificación de Histograma

### **4.1. Introducción**

En esquemas de marca de agua con detección a ciegas, la pérdida de sincronización entre los bloques de inserción y detección de marca de agua, provocan errores al momento de realizar la detección de la marca insertada en el material digital.

Manipulaciones geométricas, tales como rotación, escalamiento, traslación y cualquier transformación Affine, entre otros, son los principales factores que provocan este problema en el detector, sin embargo, este tipo de distorsiones son muy comunes en la práctica. En la literatura, diversos métodos han sido propuestos para combatir los ataques geométricos [10], [12], [18], [22-37], [46], [47], los cuales están clasificados básicamente en seis categorías, que fueron revisados en el capítulo 2 de esta tesis. Retomando la sexta categoría, la cual hace uso del histograma de la información de la imagen como dominio invariante de inserción de la marca de agua, esto debido a que el histograma es inherentemente invariante a los procesamientos geométricos, será la base para el esquema de marca de agua propuesto en este trabajo. El uso de histogramas de imagen como dominio de inserción de marca de agua ha sido previamente reportado en [34-37]. En [34], una especificación exacta del histograma es usada para insertar la marca de agua dentro de la imagen. En [35], se extiende la especificación de histograma propuesta en [34] para histogramas cromáticos y la secuencia de marca de agua es insertada en un plano cromático de la imagen a color.

Los autores del trabajo propuesto en [35] utilizan un histograma de color basado en una implementación reducida de Earth Mover's Distance (EMD), la cual es una medida matemática utilizada para calcular la distancia entre dos distribuciones dadas y es usada en [35] para optimizar la modificación de la imagen de acuerdo a un histograma dado. El trabajo presentado en [37] propone un método basado en propiedades de histograma que son usadas para medir numerosas características globales de todos los píxeles que componen la imagen, de modo que permita construir un espacio característico de tres dimensiones para insertar la marca de agua. Casi todos los trabajos citados previamente basados en modificación de histograma muestran robustez ante las distorsiones geométricas, sin embargo, no proporcionan suficiente robustez ante procesamiento de señales comunes y algunas combinaciones entre ataques geométricos- operaciones de procesamiento de señal.

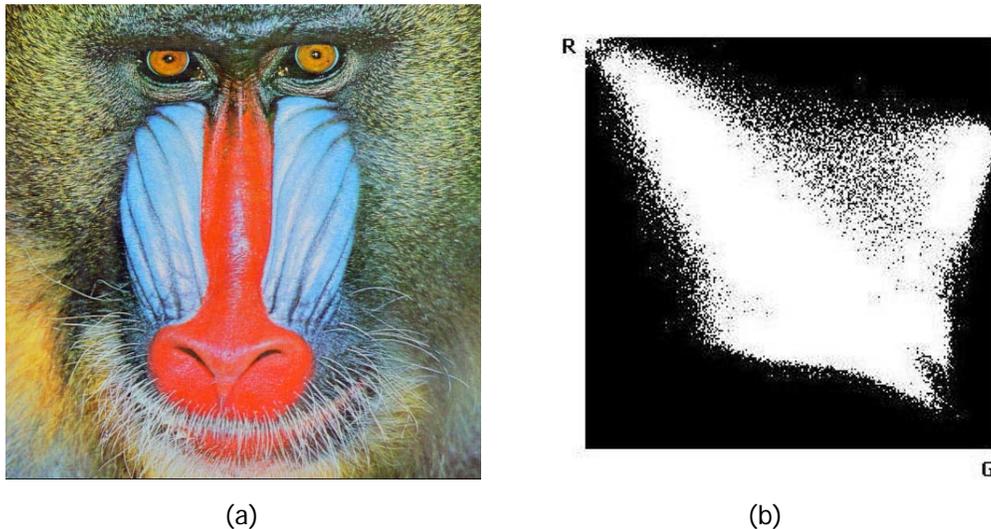
En este trabajo se presenta un algoritmo de marca de agua robusto ante distorsiones geométricas y diversas operaciones de procesamiento de señal. Está basado en dos modificaciones a histogramas en dos dimensiones. En la primera modificación, se obtiene un histograma de color en 2D, construido con las componentes de color rojo R y verde G, en el cual se selecciona una región adecuada y se modifica de acuerdo al patrón de marca de agua. Tal modificación al histograma R-G es llevada a cabo principalmente para combatir las distorsiones geométricas tales como rotación, escalamiento, recorte de imagen, entre otros. La robustez ante las transformaciones geométricas se obtiene debido a que el histograma de una imagen es considerado como un dominio invariante geoméricamente, si la marca de agua puede ser insertada dentro de este dominio, está puede sobrevivir a las distorsiones geométricas. En la segunda modificación se hace uso de histogramas en 2D construidos con la componente de color azul B y la componente marcada R filtrada. Estos histogramas son generados de acuerdo a una partición dinámica de las componentes B y R filtrada. Una vez obtenido cada histograma, es particionado en cuatro bloques y los valores de los bins que componen cada bloque son modificados de acuerdo al patrón de marca de agua. La modificación es llevada a cabo para combatir la compresión JPEG y otras operaciones de procesamiento de señal.

Los resultados experimentales muestran la robustez ante diversas distorsiones geométricas, procesamiento de señal y combinación de ambas distorsiones. También se lleva a cabo una comparación de rendimiento con trabajos previamente reportados, observándose un mejor rendimiento del método propuesto.

## 4.2. Proceso de inserción

En gráficos de computadora y fotografía digital, un histograma de color es una representación de la distribución de colores en una imagen, derivado de contar el número de píxeles de cada color.

Estas representaciones pueden ser presentadas en dos (2D) y tres 3(D) dimensiones. La figura 4.1 muestra un ejemplo de histograma de color R-G de dos dimensiones.



**Figura 4.1.** Ejemplo de un histograma de color en dos dimensiones. (a) Imagen original. (b) Histograma de color 2D obtenido de (a).

En este trabajo, se hace uso de dos diferentes histogramas 2D para insertar un patrón binario de marca de agua. El proceso de inserción comprende de dos estrategias para modificar las componentes de color R, G y B de la imagen.

### 4.2.1 Modificación de histograma 2D R-G.

En la figura 4.2 se muestra el proceso completo de inserción. En esta sección, se describe la modificación del histograma 2D compuesto por las componentes de color R-G.

1) Descomponer la imagen de color original  $I$  en tres componentes R, G y B. Utilizando las componentes R y G, obtener un histograma de color 2D R-G llamado  $H_{RG}$ .

2) Usando una llave de usuario secreta, generar la marca de agua  $W$ , la cual es un patrón binario pseudo-aleatorio de dos dimensiones 2D de tamaño  $L \times L$  donde  $0 \leq L=2^n-1 \leq 255$  con  $n=0, \dots, 8$  condicionado por las dimensiones del histograma  $H_{RG}$ . Un valor pequeño de  $L$  reduce la cantidad útil de marca de agua por lo tanto la robustez ante los ataques geométricos se ve severamente afectada. Por otro lado, si se elige un valor grande para  $L$ , la robustez ante las distorsiones geométricas se incrementa, pero la imperceptibilidad de la marca de agua puede verse afectada. Por lo tanto, es recomendable seleccionar un valor de  $L$  que proporcione robustez e imperceptibilidad al mismo tiempo.

3) Segmentar el histograma  $H_{RG}$  en bloques de tamaño  $L \times L$ .

4) Una vez que el histograma  $H_{RG}$  ha sido segmentado en bloques, es necesario seleccionar un bloque adecuado  $BH_{RG}$  para insertar la secuencia de marca de agua. La condición para considerar que un bloque es adecuado, es que casi todos los valores de los bins en el bloque deben ser diferentes de cero. Esta condición es requerida para asegurar que la modificación se realice de una manera correcta. El valor de un bin del bloque  $BH_{RG}(j,k)$  es modificado de acuerdo al bit de marca de agua  $W(j,k)$ , como se muestra en (3.1):

$$\begin{aligned} \text{if } W(j,k) = 0 \text{ entonces } BH_{RG}(j,k) &\leftarrow 0 \\ \text{if } W(j,k) = 1 \text{ entonces } BH_{RG}(j,k), j,k \in [1,L] &\leftarrow \text{valor diferente de cero} \end{aligned} \quad (3.1)$$

Diversas situaciones pueden surgir: Si  $W(j,k)=0$  y  $BH_{RG}(j,k)=0$  así como  $W(j,k)=1$  y  $BH_{RG}(j,k)\neq 0$ , en este caso no es necesario modificar el bin  $BH_{RG}(j,k)$ . Sin embargo, si estas condiciones no se cumplen,  $BH_{RG}(j,k)$  debe ser modificado. En la primera condición de la ecuación (1),  $BH_{RG}(j,k)$  debe ser forzado a cero, distribuyendo su valor lo más uniformemente posible entre sus cuatro vecinos. En la segunda condición,  $BH_{RG}(j,k)$  debe ser forzado a tener un valor diferente de cero, el cual puede ser obtenido substrayendo valores de bins de un vecino que tenga un valor grande y estos valores se asignan a  $BH_{RG}(j,k)$ . Este método de inserción asegura la imperceptibilidad de marca de agua, porque los valores modificados son asignados a los vecinos de  $BH_{RG}(j,k)$ , de modo que solo se observan ligeros cambios en los colores de la imagen, manteniendo inalterado el número total de bins con respecto a la cantidad original.

5) Una vez que el histograma  $H_{RG}$ , es modificado, todos los bins son restaurados y se obtienen las componentes marcadas  $R_w$  y  $G_w$ .

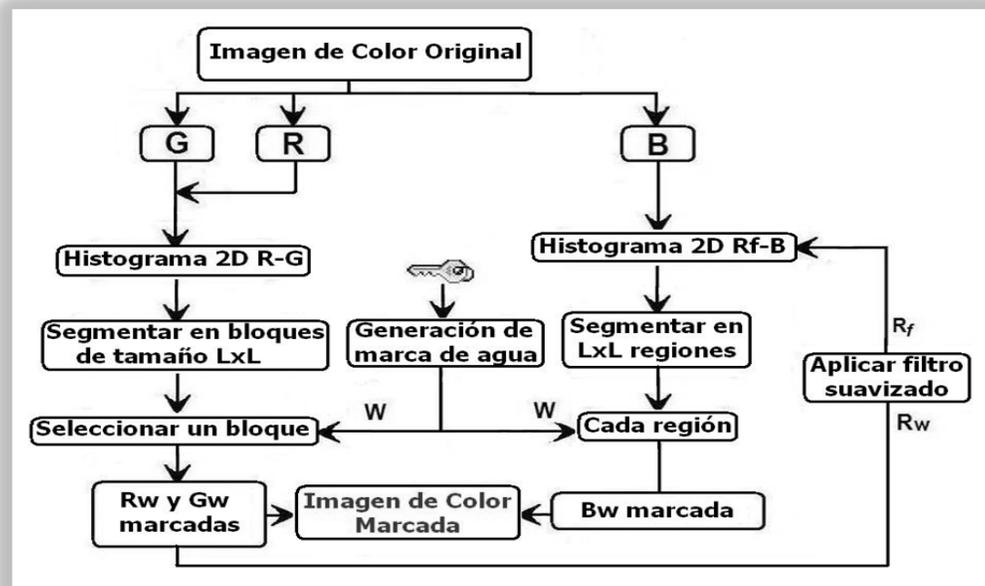


Figura 4.2. Proceso de inserción de marca de agua.

### 4.2.2 Modificación de histograma 2D B- $R_w$ filtrada.

Una vez que las componentes marcadas  $R_w$  y  $G_w$  son obtenidas, se continua con la modificación de la componente  $B$  como segunda estrategia, la cual está basada en un histograma 2D compuesto por las componentes  $B$  y  $R_w$  filtrada (2D B- $R_w$ ). Esta estrategia es descrita como sigue:

1) La compresión JPEG es considerada como un filtro pasa-bajos, porque elimina la mayoría de las componentes de alta frecuencia de una imagen. Algunos filtros adaptivos [48], [49], pueden ser diseñados para la reducción del efecto de bloque en la compresión JPEG. El filtro de suavizado presentado en (4.2) es usado y adoptado en esta estrategia para reducir eficazmente la variación de los coeficientes de  $R_w(x,y)$  en respuesta a la compresión JPEG con diferentes factores de calidad:

$$\begin{aligned}
 & \text{para todo } (x, y) \text{ teniendo } 0 \leq x \leq M - 1, 0 \leq y \leq N - 1 \\
 & \text{para todo } (\hat{x}, \hat{y}), \hat{x}^2 + \hat{y}^2 \leq r^2 \text{ teniendo } \begin{array}{l} 0 \leq x + \hat{x} \leq M - 1, \\ 0 \leq y + \hat{y} \leq N - 1 \end{array} \\
 R_{wf}(x, y) = \sum_x \sum_y \frac{R_w(x + \hat{x}, y + \hat{y})}{N_r}, \quad (4.2)
 \end{aligned}$$

donde  $r$  denota el radio de un círculo alrededor del punto central  $(x,y)$ , y  $N_r$  representa el número de píxeles dentro de este círculo. Después de que la ecuación (4.2) es aplicada, los coeficientes de  $R_{wf}$  son más estables bajo la compresión JPEG con diversos factores de calidad.

2) Dividir las componentes  $R_{wf}$  y  $B$  en  $p_i$  regiones. El número de regiones está dado por  $L^2$ , donde  $L$  indica la dimensión de la marca de agua, así, por ejemplo, si  $L = 16$ , entonces estas componentes son divididas en  $L^2 (=16 \times 16)$  regiones.

3) Para cada región  $p_i$ , se construye un histograma 2D  $h_i$  compuesto por las componentes  $Rw_f$  y  $B$ , y cada histograma  $h_i$  es particionado en cuatro bloques llamados  $BA$ ,  $BB$ ,  $BC$  y  $BD$  respectivamente.

4) El  $i$ -ésimo bit de marca de agua es insertado dentro del histograma  $h_i$  de la  $i$ -ésima región, modificando los valores de los bins de la componente  $B$ . Para insertar un patrón de marca de agua binario  $W(j,k)$ , la distribución de  $h_i$  es modificada. Por ejemplo, si  $W(j,k) = 1$ , algunos bins en  $BB$  y  $BC$  son movidos dentro de  $BA$  y  $BD$ ; en cambio si  $W(j,k) = 0$  algunos bins en  $BA$  y  $BD$  son movidos dentro de  $BB$  y  $BC$ , estas reglas de modificación están dadas por (4.3) y (4.4) respectivamente.

Los valores menor, medio y mayor de  $B$  en el histograma  $h_i$  son obtenidos y denotados por  $B_l$ ,  $B_m$  y  $B_h$  respectivamente, los cuales serán usados en el siguiente paso.

Si  $W(j,k) = 1$ :

$$\begin{aligned} N_{BA} &= N_{BA} + \alpha(N_{BB}) \\ N_{BD} &= N_{BD} + \alpha(N_{BC}) \end{aligned} \quad (4.3)$$

Si  $W(j,k) = 0$ :

$$\begin{aligned} N_{BB} &= N_{BB} + \alpha(N_{BA}) \\ N_{BC} &= N_{BC} + \alpha(N_{BD}) \end{aligned} \quad (4.4)$$

Donde  $N_{BA}$ ,  $N_{BB}$ ,  $N_{BC}$ ,  $N_{BD}$  representan el número total de bins de cada bloque,  $\alpha$  es un factor de ganancia ( $0 \leq \alpha \leq 1$ ), el cual indica la tasa del número de bins que pueden ser movidos entre los bloques, por lo que este factor controla la imperceptibilidad y la robustez de la marca de agua, y es más robusta cuando se incrementa el valor de  $\alpha$ , sin embargo, algunas regiones de la imagen marcada pueden ser distorsionadas. Para controlar la robustez ante la compresión JPEG, se calculan dos valores marginales  $B_l'$  y  $B_h'$ , como se muestra en la ecuación (4.5) [37],

$$\begin{aligned} B_l' &= B_m - \beta(B_m - B_l) \\ B_h' &= B_m + \beta(B_h - B_m) \end{aligned} \quad , \quad (4.5)$$

donde  $\beta$  es un factor que indica la resistencia a la compresión JPEG y su valor debe ser  $0 \leq \beta \leq 1$ . Si se utiliza un valor de  $\beta > 1$ , se pueden tener cambios visibles en la imagen. Este proceso cambia únicamente la distribución interior de  $h_i$ , pero la distribución entre histogramas  $h_i$  ( $i=1..L^2$ ) no se ve afectada. De modo que, la relación mutua entre histogramas  $h_{i1}$  y  $h_{i2}$  de  $i1$  y  $i2$  regiones se conserva. Después de insertar  $L^2$  bits de marca de agua, la distribución global de la componente  $B$  es modificada. Una adecuada selección de los factores  $\alpha$  y  $\beta$  garantizan una buena calidad de la imagen marcada. Este paso se ilustra en la figura 4.3.

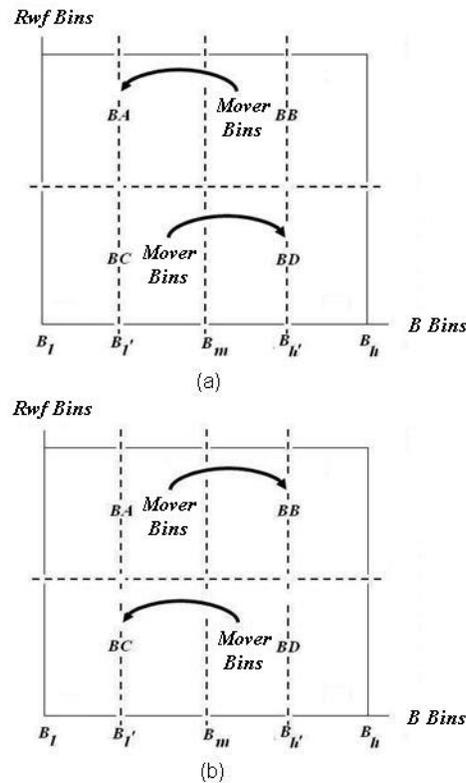


Figura 4.3. Modificación de histograma B- $R_w$  filtrada, por movimiento interno de bins .

5) Una vez que cada histograma  $h_i$  es modificado para insertar cada bit de marca de agua, la componente  $B$  es restaurada para obtener una componente marcada  $B_w$ . Finalmente, la imagen marcada  $I_w$  es construida utilizando las tres componentes marcadas  $R_w$ ,  $G_w$  y  $B_w$ .

### 4.3. Proceso de detección

El proceso de detección de marca de agua es descrito de la siguiente manera:

- 1) Obtener las componentes  $R_w$ ,  $G_w$ , y  $B_w$  de la imagen marcada  $I_w$ . Obtener un histograma 2D R-G llamado  $H_{RG}$  y segmentarlo en bloques de tamaño  $L \times L$ .
- 2) Extraer la región marcada  $H_{r_w}$  del histograma  $H_{RG}$ , en la cual fue insertada la marca de agua, y el patrón de marca de agua  $W_1$  es reconstruido de acuerdo a las siguientes condiciones: si  $H_{r_w}(j,k) > 0$  entonces  $W_1(j,k) = 1$ , en otro caso  $W_1(j,k) = 0$ .
- 3) Aplicar un filtrado de suavizado circular a la componente  $R_w$ , y obtener la componente filtrada  $R_{wf}$ . Segmentar las componentes  $R_{wf}$  y  $B_w$  en  $L^2$  regiones y construir con cada región obtenida de ambas componentes los  $L^2$  histogramas en 2D  $h_i$ ,  $i=1..L^2$ , donde  $L^2$  es la longitud de marca de agua.
- 4) Particionar cada histograma  $h_i$  en cuatro bloques llamados  $BA$ ,  $BB$ ,  $BC$  y  $BD$ , respectivamente.
- 5) Contar el número de bins en estos cuatro bloques y de acuerdo al número obtenido, el valor de cada bit de marca de agua es extraído. La condición para esta asignación es dada por la ecuación (4.6):

$$\begin{aligned} \text{si } N_{BA} + N_{BD} > N_{BB} + N_{BC} & \quad \text{entonces } W_2(j,k) = 1 \\ \text{otro caso } & \quad W_2(j,k) = 0 \end{aligned} \quad (4.6)$$

- 6) Una vez que los dos patrones de marca de agua  $W_1$  y  $W_2$  son extraídos, obtener la correlación cruzada  $c_1$  el patrón recuperado  $W_1$  y la marca de agua  $W$ .

7) Un valor umbral  $T$  debe ser definido para determinar si la marca de agua está presente o no en la imagen. Por lo tanto, si el número de bits extraídos correctamente excede el valor umbral  $T$ , la secuencia de marca de agua se considera extraída correctamente de la imagen marcada. La probabilidad de falsa alarma  $P_{fa}$  para  $n$  bits de marca de agua insertados está dada por (4.7) [29], y el valor  $T$  debe ser controlado de modo que  $P_{fa}$  sea menor que un valor predeterminado.

$$P_{fa} = \sum_{i=T}^n \left(\frac{1}{2}\right)^n \cdot \left(\frac{n!}{i!(n-i)!}\right) \quad , \quad (4.7)$$

donde  $n$  es el número total de bits de marca de agua. En la figura 4.4 se muestra el diagrama a bloques del proceso de detección de marca de agua.

8) Si el valor de correlación cruzada  $c_1$  es mayor que el valor umbral  $T$ ,  $c_1 > T$ , la marca de agua es detectada y termina el proceso de detección.

9) Si el valor de correlación cruzada  $c_1$  es menor que el valor umbral  $T$ ,  $c_1 < T$ , entonces obtener el valor de correlación cruzada  $c_2$  entre el patrón recuperado  $W_2$  y la marca de agua  $W$ .

10) Si el valor de correlación cruzada  $c_2$  es mayor que el valor umbral  $T$ ,  $c_2 > T$ , la marca de agua es detectada y termina el proceso de detección. En otro caso, la marca de agua no es detectada.

#### 4.4. Resultados experimentales

Para evaluar el rendimiento del método propuesto, las pruebas realizadas en esta sección son realizadas desde el punto de vista de imperceptibilidad y robustez de marca de agua. Se usaron un conjunto de 10 imágenes a color de tamaño 512 x 512, las cuales son: Lena, Peppers, Mandrill, Airplane, House, Tiffany, Lake, Tree, Car y Splash. El software Matlab 7 fue usado como herramienta de simulación computacional en este trabajo.

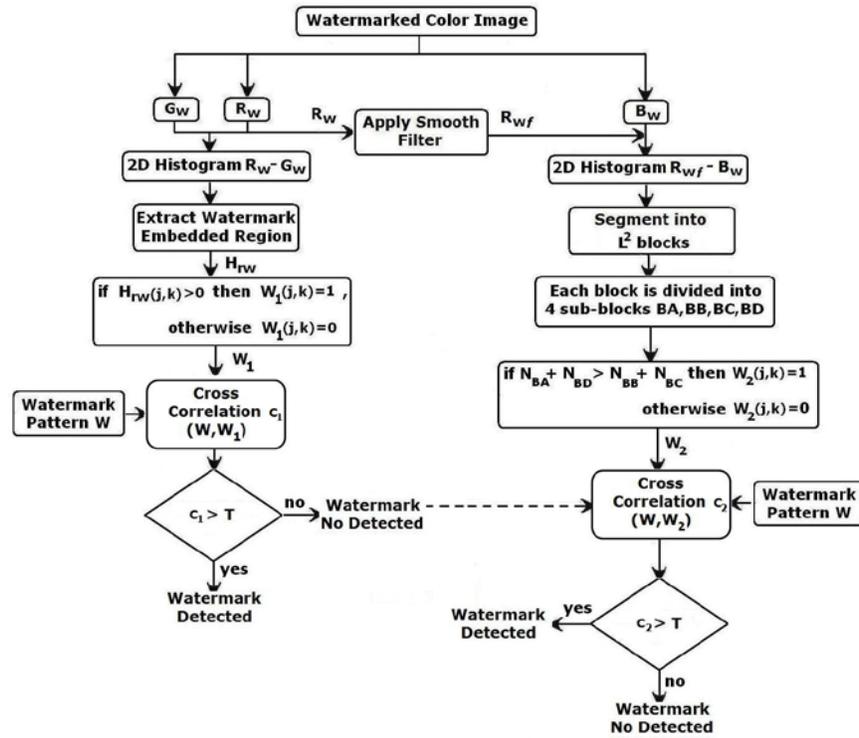


Figura 4.4. Proceso de detección de marca de agua.

#### 4.4.1 Determinación de parámetros

En primera instancia, se llevaron a cabo diversos experimentos para determinar los valores adecuados de los siguientes parámetros: factores de inserción de marca de agua ( $\alpha$ ,  $\beta$ ), dimensión de la marca de agua  $L$  y el radio usado por el filtro de suavizado circular  $r$ . La Tabla 4.1 muestra los valores promedio de la Relación Señal a Ruido Pico (PSNR) y los bits extraídos correctamente del conjunto de diez imágenes, esto con el objetivo de analizar los efectos que tienen los factores  $\alpha$  y  $\beta$  sobre la imperceptibilidad y robustez de marca de agua. En este experimento, las imágenes marcadas están comprimidas en un formato JPEG con un factor de calidad de 50 y rotadas  $7^\circ$ .

La dimensión de marca de agua y el radio usados para esta prueba son  $L=16$  y  $r=12$  respectivamente. El valor total promedio de PSNR obtenido de las componentes de color marcadas,  $R_w$ ,  $G_w$  y  $B_w$  está dado por (4.8):

$$PSNR_{Total} = 10 \log_{10} \frac{255^2}{(MSE_{R_w} + MSE_{G_w} + MSE_{B_w})/3}, \quad (4.8)$$

donde  $MSE_{R_w}$ ,  $MSE_{G_w}$  y  $MSE_{B_w}$  son el error cuadrático medio (MSE) de  $R_w$ ,  $G_w$  y  $B_w$ , respectivamente. Para evaluar los resultados, se utilizaron diversos valores de  $\alpha$  y  $\beta$ , como se muestra en la tabla 4.1, en la cual, se muestra que la robustez e imperceptibilidad de marca de agua son inversamente proporcionales una de otra. Debido a la dependencia de los factores  $\alpha$  y  $\beta$ , se deben estimar los valores adecuados para cada uno.

TABLA 4.1  
PSNR PROMEDIO DE LAS COMPONENTES DE COLOR Y NÚMERO DE  
BITS EXTRAÍDOS CORRECTAMENTE DE LAS IMÁGENES  
MARCADAS CON COMPRESION JPEG QF = 50 Y ROTACION DE 7°.  
 $L = 16$  y  $r = 12$ .

$\beta$	$\alpha$			
	0.2	0.4	0.6	0.8
0.1	40.05 / 152	39.52 / 159	38.94 / 168	35.65 / 181
0.3	38.63 / 155	37.56 / 165	36.75 / 179	34.81 / 187
0.5	37.92 / 161	36.78 / 173	<b>35.87 / 193</b>	32.42 / 194
0.7	37.04 / 169	35.15 / 182	33.58 / 198	31.04 / 197
0.9	36.98 / 170	34.09 / 189	32.07 / 201	30.88 / 202

$N_1/N_2$  en la tabla indican el PSNR promedio y el número de bits extraídos correctamente de las imágenes marcadas, respectivamente.

Como se muestra en la tabla 4.1, se puede concluir que los valores adecuados de  $\alpha$  y  $\beta$  para obtener una imperceptibilidad y robustez de marca de agua aceptable fueron 0.6 y 0.5, respectivamente.

Para seleccionar una adecuada carga útil de marca de agua  $L \times L$ , se realizaron diversas evaluaciones al respecto. La figura 4.5 muestra la PSNR promedio de un conjunto de 10 imágenes marcadas con un valor variable de dimensión de marca de agua  $L$  y con los siguientes valores de los parámetros  $r = 12$ ,  $Nr = 452$ ,  $\alpha = 0.6$  y  $\beta = 0.5$ . Un valor pequeño de  $L$  reduce la carga útil de marca de agua por lo tanto la robustez ante los ataques geométricos se ve severamente afectada. Por otro lado, si se elige un valor grande para  $L$ , la robustez ante las distorsiones geométricas se incrementa, pero la imperceptibilidad de la marca de agua puede verse afectada. Por lo tanto, es recomendable seleccionar un valor de  $L$  que proporcione robustez e imperceptibilidad al mismo tiempo. De la figura 4.5 podemos observar que el valor adecuado para  $L$  es 16.

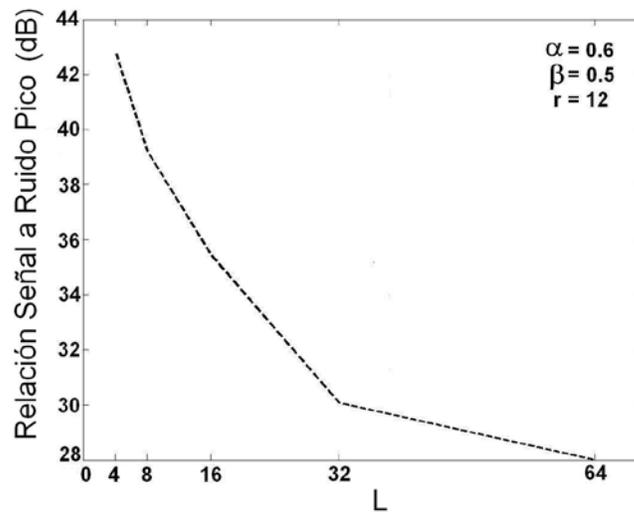
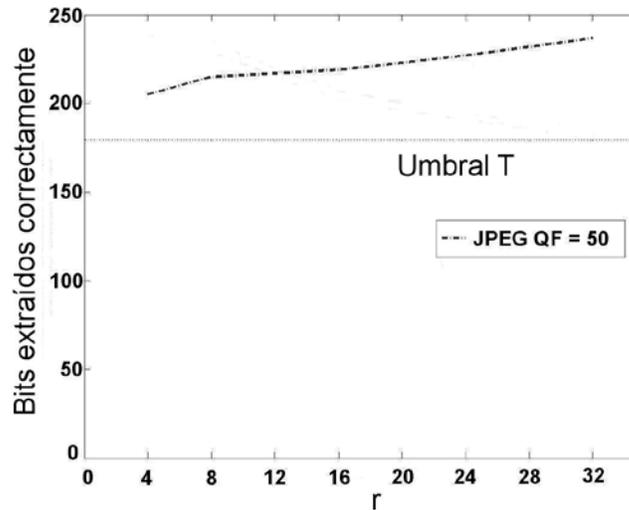


Figura 4.5. PSNR promedio con factor L variable.

El valor del radio  $r$  del filtro de suavizado circular influye en la robustez de marca de agua ante la compresión JPEG. Para seleccionar un valor adecuado de  $r$ , si se incrementa el valor de  $r$ , se pueden recuperar mayor cantidad de bits de manera correcta.

La figura 4.6 revela la relación entre el valor  $r$  y el número de bits extraídos correctamente, cuando la imagen marcada es comprimida por compresión JPEG con un factor de calidad de 50.

De la figura 4.6 se puede observar que al tener un valor grande para  $r$  se incrementa ligeramente el número de bits extraídos correctamente, sin embargo, la complejidad computacional es directamente proporcional al tamaño del radio  $r$ . Por lo tanto, el valor adecuado determinado para el radio utilizado por el filtro de suavizado circular es  $r=12$ .



**Figura 4.6.** Cantidad promedio de bits extraídos correctamente de un conjunto de imágenes con un valor de radio  $r$  variable.

Finalmente, los resultados experimentales muestran que los siguientes valores para los parámetros  $L = 16$  (longitud de marca de agua es  $L^2=256$ ),  $r = 12$ ,  $Nr = 452$ ,  $\alpha = 0.6$ ,  $\beta = 0.5$ , y  $T = 179$  con  $P_{fa} = 10^{-7}$ , son los más adecuados. Usando los parámetros estimados anteriormente,  $L$ ,  $r$ ,  $Nr$ ,  $\alpha$  y  $\beta$ , fueron usados para evaluar la imperceptibilidad de la marca de agua. La figura 4.7 muestra seis imágenes originales de prueba (a), (b), (c), (d), (e) y (f) junto con sus versiones marcadas (g), (h), (i), (j), (k) y (l) respectivamente. En cada caso se insertaron 256 bits de marca de agua. En esta figura se muestra que las imágenes marcadas no sufren mucha distorsión obteniéndose un PSNR de al menos 35 dB. Los valores de Relación Señal a Ruido Pico obtenidos para cada imagen fueron: (a)Airplane (38.65dB), (b)Peppers (36.73dB), (c)Car (36.51dB), (d)Mandrill (39.08dB), (e)Lena (35.98dB) y (f)Lake (37.12dB).



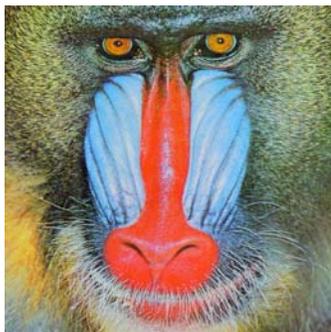
(a)



(b)



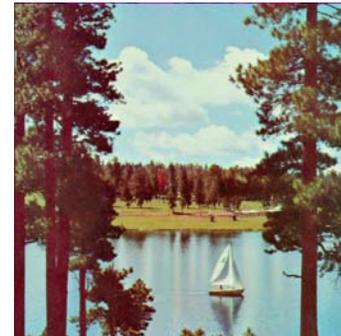
(c)



(d)



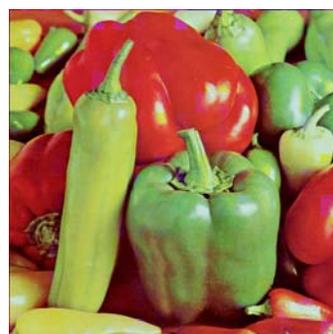
(e)



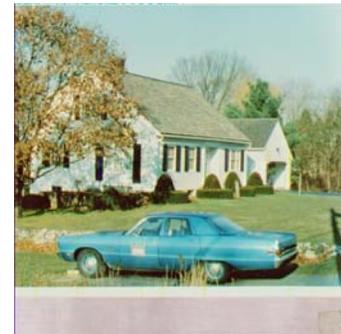
(f)



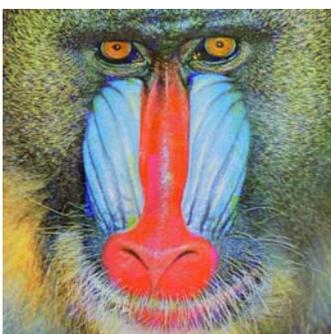
(g)



(h)



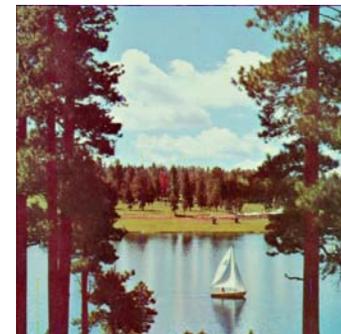
(i)



(j)



(k)



(l)

**Figura 4.7.** Imágenes de prueba originales (a-f) y sus versiones marcadas (g-l).

## 4.4.2 Imperceptibilidad de Marca de Agua

La imperceptibilidad o transparencia de la marca de agua en imágenes tiene como base el comportamiento del sistema visual humano. Una marca de agua es imperceptible, si la degradación que causa en los archivos donde se ha insertado es muy difícil de apreciar. En algunas aplicaciones se puede aceptar una pequeña degradación de los datos, a cambio de lograr mayor robustez o menor costo del sistema [2]. En esta sección, se muestran los resultados experimentales correspondientes a las pruebas de imperceptibilidad de marca de agua del algoritmo propuesto en este capítulo, el cual se basa en modificación de histograma.

### 4.4.2.1 Espacio de color CIELAB

Para medir el cambio de color<sup>1</sup> en la imagen original y la imagen marcada, se utilizo el espacio de color CIE 1976 ( $L^*a^*b^*$ ) [50][51], el cual proporciona una útil representación tridimensional de los estímulos perceptuales del color. En 1976, la Comisión Internacional de Iluminación CIE (*Commission Internationale d'Eclairage*), propuso el espacio de color CIELAB, también llamado espacio de color CIE 1976 (*CIE 1976 color space*) como una aproximación a un espacio de color uniforme. El espacio de color CIELAB es una transformación matemática del espacio XYZ en el cual se fija un blanco de referencia y cuyos valores de triestímulo son  $(x_n, y_n, z_n)$ . Ese blanco de referencia puede ser, por ejemplo una fuente luminosa, el iluminante al que se haya adaptado el observador, un difusor perfecto o el color neutro más reflectante o transmisor de un medio de reproducción. En el sistema CIELAB, los colores deben verse sobre un fondo que vaya de blanco a gris medio por un observador adaptado a un iluminante que no sea demasiado distinto a la luz natural del medio día. Los tres ejes del sistema CIELAB se indican con los nombres  $L^*$ ,  $a^*$  y  $b^*$ .

---

<sup>1</sup> Existen ecuaciones de diferencia de color tales como CMC, M&S, BFD, CIE94 y CIE2000, sin embargo, el objetivo de esta tesis no está enfocado al análisis de dichos métodos, para mayores detalles consultar las referencias [50] y [51].

Representan, respectivamente Luminosidad (*lightness*), tonalidad de rojo a verde (*redness-greenness*) y tonalidad de amarillo a azul (*yellowness-blueness*) (los dos últimos ejes están inspirados en la teoría de los colores oponentes). Si dos puntos en el espacio (que representan dos estímulos), son coincidentes, entonces la diferencia cromática entre ambos estímulos es igual a cero. Según se incrementa la distancia entre esos dos puntos: espacio original ( $L_o, a_o, b_o$ ) y espacio marcado ( $L_w, a_w, b_w$ ), es razonable suponer que va aumentando la percepción de que existe una diferencia cromática entre los estímulos que ambos puntos representan.

#### 4.4.2.2 Cambio de color en la imagen

Una forma de medir la diferencia cromática entre dos estímulos es, por tanto, medir la distancia euclidiana llamada Delta-E ( $\Delta E$ ), existente entre dos puntos en un espacio tridimensional. Esta distancia está dada por (4.9):

$$\Delta E = \sqrt{(\Delta L^*)^2 + (\Delta a^*)^2 + (\Delta b^*)^2} \quad , \quad (4.9)$$

donde,  $\Delta L^* = L_o - L_w$ ,  $\Delta a^*$  y  $\Delta b^*$  se definen similarmente. Por lo tanto, Delta-E ( $\Delta E$ ) es un único número que representa la "diferencia" entre dos colores correspondientes a dos puntos en un espacio tridimensional. La idea principal es que una delta  $\Delta E$  de 1.0 es la más pequeña diferencia de color que el ojo humano puede ver. De este modo, cualquier delta  $\Delta E$  menor que 1.0 se considera imperceptible, por el contrario, cualquier valor  $\Delta E$  mayor que 1.0 es considerado perceptible.

Sin embargo, algunas diferencias de color superiores a 1.0 son perfectamente aceptables, tal vez incluso imperceptibles [50]. Haciendo uso de este proceso, en la figura 4.8 se muestra la imagen de diferencia de color correspondiente entre la imagen original y la imagen marcada obtenida de tres imágenes prueba.

Por otro lado, para obtener una cantidad promedio de los píxeles que tuvieron un valor  $\Delta E$  mayor que 1.0, el cual es considerado perceptible, se hace uso de (4.10):

$$P_{perceptibles} = \frac{\text{Número de píxeles con } \Delta E > 1}{\text{Número total de píxeles}}, \quad (4.10)$$

La tabla 4.2 muestra el porcentaje de píxeles con una delta  $\Delta E > 1.0$  obtenidos de un conjunto de 6 imágenes marcadas con el método de Lin [37] y el esquema propuesto en esta tesis.

TABLA 4.2  
PORCENTAJE DE PÍXELES CON UNA DELTA  $\Delta E > 1.0$  EN LAS IMAGENES  
LENA, PEPPERS, TIFFANY, LAKE, AIRPLANE Y HOUSE

IMAGEN	METODO PROPUESTO POR LIN ET AL. [37]	METODO PROPUESTO EN ESTA TESIS
LENA	2.95 %	2.79 %
PEPPERS	3.75 %	3.95%
TIFFANY	2.31 %	1.91%
LAKE	2.15 %	2.56 %
AIRPLANE	2.35 %	2.10 %
HOUSE	4.24 %	3.82 %

De la tabla 4.2, se puede observar que en ambos esquemas el porcentaje de píxeles con un cambio de color perceptible, es decir, que tiene un valor de delta  $\Delta E > 1.0$  es bajo, considerando una escala de 0% a 100%, donde 0% es un cambio de color nulo en los píxeles de la imagen y 100% un cambio de color perceptible en todos los píxeles de la imagen.



**Figura 4.8.** Imágenes originales (a), (d) y (g). Versiones marcadas (b), (e) y (h). Imagen de diferencia de color (c), (f) y (i).

De la figura 4.8, en las imágenes de diferencia de color, se puede observar que las regiones de color blanco contienen un valor de  $\Delta E < 1$ , lo que indica que el cambio de color se considera imperceptible. Por otro lado, las regiones en color negro contienen un valor  $\Delta E > 1$ , lo cual indica que en ciertas regiones los cambios de color pueden resultar perceptibles al ojo humano. Sin embargo, como ya se comentó anteriormente, algunas diferencias de color superiores a 1.0 son perfectamente aceptables, tal vez incluso imperceptibles [50].

#### 4.4.2.3 Diferencia de Color Normalizada (NCD)

La Diferencia de Color Normalizada NCD (por sus siglas en inglés *Normalized Color Difference*) [52], [53], es una medida basada en el espacio de color CIELAB representada por un único número y se utiliza para medir el cambio de color entre dos imágenes, está dada por (4.11):

$$NCD = \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \left( \sqrt{\left( (\Delta L(i, j))^2 + (\Delta a(i, j))^2 + (\Delta b(i, j))^2 \right)} \right)}{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \left( \sqrt{\left( L(i, j)^2 + a(i, j)^2 + b(i, j)^2 \right)} \right)}, \quad (4.11)$$

donde  $\Delta L = L_o - L_w$ ,  $\Delta a$  y  $\Delta b$  se definen similarmente.

En la tabla 4.3 se muestra el NCD obtenido de 10 imágenes originales y sus respectivas versiones marcadas. Un valor de NCD igual a cero indica que la imagen original y la imagen de referencia son la misma, por lo tanto, la diferencia de colores es directamente proporcional al valor NCD, es decir, conforme el valor de NCD aumenta, la diferencia de colores es mayor entre ambas imágenes.

TABLA 4.3  
DIFERENCIA DE COLOR NORMALIZADA (NCD)

Imágenes	NCD
Lena	0.0844
Mandrill	0.0975
Tiffany	0.0344
Lake	0.0346
House	0.0826
Peppers	0.0685
Car	0.0756
Tree	0.0612
Airplane	0.0489
Splash	0.0356

De los resultados obtenidos de la tabla 4.3 se puede observar que se obtiene un valor de NCD aceptable [52], que representa una diferencia de colores pequeña para el conjunto de imágenes de color.

#### 4.4.2.4 Fidelidad de la Información Visual (VIF)

La Fidelidad de la Información Visual VIF (por sus siglas en inglés *Visual Information Fidelity*), es una medida de la calidad visual de una imagen basada en el dominio de la transformada wavelet que permite medir con mayor precisión la calidad de una imagen después de que esta ha sido procesada [54].

Está compuesto por tres modelos y un criterio derivado de estos modelos, los cuales se definen como: modelo fuente (*Source Model*), modelo de distorsión (*Distortion Model*), modelo del sistema visual humano HVS (*Human System Model*) y el criterio de fidelidad de la información visual IFC (*Visual Information Fidelity Criterion*). Todos los elementos anteriores componen la Fidelidad de la Información Visual VIF y el desarrollo de estos se describe con detalle en [54]. La VIF se define como (4.12):

$$VIF = \frac{\sum_{j \in \text{subbands}} I(\bar{C}^{N,j}; \bar{F}^{N,j} s^{N,j})}{\sum_{j \in \text{subbands}} I(\bar{C}^{N,j}; \bar{E}^{N,j} s^{N,j})}, \quad (4.12)$$

donde se suman las sub-bandas de interés,  $\bar{C}^{N,j}$  representa los  $N$  elementos del campo aleatorio [54] (*Random Field*) RF  $\bar{C}_j$  el cual describe los coeficientes de una sub-banda  $j$  y así sucesivamente.  $I(\bar{C}^{N,j}; \bar{F}^{N,j} s^{N,j})$ ,  $I(\bar{C}^{N,j}; \bar{E}^{N,j} s^{N,j})$  representan información de la imagen marcada y original respectivamente, ambos valores son obtenidos a partir de los tres modelos y del criterio mencionados con anterioridad. En la tabla 4.4 se muestra el valor de VIF y PSNR obtenidos de un conjunto de 10 imágenes.

TABLA 4.4  
FIDELIDAD DE LA INFORMACION VISUAL (VIF)

Imágenes	VIF	PSNR (dB)
Lena	0.864	36.03
Mandrill	0.875	35.96
Tiffany	0.920	36.42
Lake	0.972	36.28
House	0.970	35.95
Peppers	0.847	35.63
Car	0.773	35.12
Tree	0.854	35.67
Airplane	0.886	36.72
Splash	0.892	35.91

Los valores de la VIF reflejan distorsiones perceptuales más precisas que la PSNR. Como se puede observar en los resultados obtenidos en la tabla 4.4, el esquema propuesto proporciona una fidelidad aceptable en la imagen marcada, ya que la PSNR obtenida es mayor a 35dB y el valor de VIF obtenido es cercano a 1, donde un valor de VIF igual a 1 indica que la imagen procesada y la original son idénticas.

### **4.4.3 Robustez de marca de agua**

Para evaluar el rendimiento del método propuesto, se llevaron a cabo diversas comparaciones con otros métodos reportados anteriormente.

La primera comparación está enfocada hacia la robustez de marca de agua entre el método propuesto en este trabajo y el método propuesto por Lin [37], ya que el documento de Lin presenta robustez de marca de agua para diversos tipos de ataques geométricos y ataques combinados con procesamiento de señal común.

Una segunda evaluación también es llevada a cabo comparando la robustez del método propuesto en este trabajo y métodos reportados anteriormente los cuales están basados en diferentes estrategias y fueron mencionados en la introducción de este documento [23],[27],[29],[36],[37], [46].

Las tablas 4.5 y 4.6 muestran una comparación de rendimiento entre el método propuesto y el método de Lin [37] con 128 y 256 bits de marca de agua insertados, respectivamente. En ambas tablas, se muestra el número promedio de bits extraídos correctamente en imágenes marcadas y no marcadas.

Para realizar una evaluación de robustez de la marca de agua en condiciones equiparables entre el esquema propuesto en esta tesis y el método de Lin et al. [37], de igual forma que en el capítulo 3 de esta tesis, se hace uso de la herramienta estándar que aplica diversas distorsiones en las imágenes marcadas, Stirmark Benchmark 4.0 [13], [14], tomando en cuenta los ataques que son comunes para evaluar los esquemas de marca de agua orientados a combatir las distorsiones geométricas sin descuidar las operaciones de procesamiento de señales. Adicionalmente, se aplicaron algunas distorsiones que no vienen en la versión de Stirmark 4.0, además de distorsiones combinadas con compresión JPEG, las cuales fueron aplicadas usando Matlab 7.0.

TABLA 4.5  
 NUMERO PROMEDIO DE BITS EXTRAIDOS CORRECTAMENTE DE IMAGENES MARCADAS Y NO MARCADAS  
 ATACADAS POR DIVERSAS DISTORSIONES GEOMETRICAS Y DE PROCESAMIENTO DE SEÑAL CON 128 BITS  
 DE MARCA DE AGUA INSERTADOS. VALOR UMBRAL  $T = 89$

Ataque	Bits Correctos en [37] $p = 16, q = 2$ y $r = 4$ . 16 planos, 32 bandas y 128 bloques	Bits Correctos en Método Propuesto
Stirrmak remover filas y columnas RML 60	127 / 61	127 / 65
Stirrmak escalamiento fs=1.5	100 / 61	124 / 64
Stirrmak transformación Affine	112 / 60	120 / 61
Stirrmak Rotación por 45°	76 / 57	126 / 65
Stirrmak compresión JPEG QF = 50	120 / 62	115 / 64
Stirrmak compresión JPEG QF = 30	112 / 60	105 / 61
Stirrmak filtrado mediano 3 x 3	127 / 63	126 / 59
Stirrmak ConvFilter	60 / 55	58 / 61
Stirrmak Random Bending Attack	123 / 59	122 / 61
Recorte 30 %	77 / 55	122 / 63
Flipping horizontal y vertical.	124 / 67	127 / 66
Cambio de aspecto (1.0, 1.2), donde cada par de números indican el porcentaje de escalamiento en las direcciones $x$ e $y$ , respectivamente.	126 / 61	127 / 59
Shearing (5%, 5%), donde cada par de números indican el porcentaje de deformación en las direcciones $x$ e $y$ , respectivamente.	123 / 65	126 / 57
Ruido impulsivo, densidad= 0.01	122 / 59	125 / 62
Ruido Gaussiano, $M = 0, \sigma = 0.01$	120 / 54	122 / 66
Aplicar nitidez a la imagen 3 x 3	102 / 66	104 / 69
Ecuilización de histograma	65 / 61	59 / 64
JPEG_70 + Remover Filas y Columnas: 5 filas y 1 columnas.	110 / 63	114 / 66
JPEG_70 + Voltar imagen horizontal y vertical.	115 / 53	110 / 58
JPEG_70 + Transformación Affine con $A = [1, 0.01; 0.01, 1]$	101 / 62	116 / 59
JPEG_70 + Shearing (0, 0.9%), donde cada par de números indican el porcentaje de deformación en las direcciones $x$ e $y$ , respectivamente.	110 / 64	107 / 69
JPEG_70 + rotación 7°	95 / 58	110 / 67
JPEG_70 + escalamiento 1.1	111 / 59	115 / 68
JPEG_70 + recorte 10%	96 / 59	118 / 60
JPEG_70 + Nitidez 3 x 3	114 / 65	102 / 64
JPEG_70 + Filtrado mediano 3 x 3	105 / 56	103 / 58

$N_1/N_2$ :  $N_1$  indica el número de bits extraídos de forma correcta de una imagen marcada;  $N_2$  indica el número de bits extraídos de forma correcta de una imagen no marcada. Los datos con letra cursiva indican que el esquema no fue robusto ante ese ataque.

TABLA 4.6  
 NUMERO PROMEDIO DE BITS EXTRAIDOS CORRECTAMENTE DE IMAGENES MARCADAS Y NO MARCADAS  
 ATACADAS POR DIVERSAS DISTORSIONES GEOMETRICAS Y DE PROCESAMIENTO DE SEÑAL CON 256 BITS  
 DE MARCA DE AGUA INSERTADOS. VALOR UMBRAL  $T = 179$

Ataque	Bits Correctos en [37] $p = 32, q = 2$ y $r = 4$ . 32 planos, 64 bandas y 256 bloques	Bits Correctos en Método Propuesto
Stirmark remover filas y columnas RML 60	241 / 114	250 / 115
Stirmark escalamiento fs=1.5	198 / 112	231 / 116
Stirmark transformación Affine	200 / 117	242 / 112
Stirmark Rotación por 45°	<i>140 / 118</i>	249 / 114
Stirmark compresión JPEG QF = 50	210 / 117	206 / 119
Stirmark compresión JPEG QF = 30	200 / 115	195 / 117
Stirmark filtrado mediano 3 x 3	225 / 116	239 / 115
Stirmark ConvFilter	<i>130 / 129</i>	<i>128 / 123</i>
Stirmark Random Bending Attack	225 / 110	227 / 112
Recorte 30 %	<i>150 / 111</i>	232 / 118
Flipping horizontal y vertical.	239 / 116	251 / 117
Cambio de aspecto (1.0, 1.2), donde cada par de números indican el porcentaje de escalamiento en las direcciones $x$ e $y$ , respectivamente.	199 / 115	247 / 115
Shearing(5%, 5%), donde cada par de números indican el porcentaje de deformación en las direcciones $x$ e $y$ , respectivamente.	<i>170 / 112</i>	248 / 117
Ruido impulsivo, densidad= 0.01	220 / 114	238 / 118
Ruido Gaussiano, $M = 0, \sigma = 0.01$	229 / 119	237 / 115
Aplicar nitidez a la imagen 3 x 3	198 / 114	201 / 119
Ecualización de histograma	<i>115 / 112</i>	<i>117 / 114</i>
JPEG_70 + Remover Filas y Columnas: 5 filas y 1 columnas.	229 / 115	237 / 116
JPEG_70 + Voltrear imagen horizontal y vertical.	220 / 112	231 / 117
JPEG_70 + Transformación Affine con $A = [1, 0.01; 0.01, 1]$	190 / 114	235 / 120
JPEG_70 + shearing (0, 0.9%), donde cada par de números indican el porcentaje de deformación en las direcciones $x$ e $y$ , respectivamente.	190 / 115	221 / 119
JPEG_70 + rotación 7°	<i>171 / 112</i>	215 / 120
JPEG_70 + escalamiento 1.1	193 / 116	220 / 118
JPEG_70 + recorte 10%	<i>164 / 113</i>	212 / 118
JPEG_70 + Nitidez 3 x 3	189 / 117	199 / 114
JPEG_70 + Filtrado mediano 3 x 3	210 / 116	220 / 116

$N_1/N_2$ :  $N_1$  indica el número de bits extraídos de forma correcta de una imagen marcada;  $N_2$  indica el número de bits extraídos de forma correcta de una imagen no marcada. Los datos con letra cursiva indican que el esquema no fue robusto ante ese ataque.

Los resultados experimentales muestran que el método propuesto en este trabajo proporciona mejor robustez que el método propuesto por Lin ante ataques geométricos que involucren recorte y rotación de imagen. Esta vulnerabilidad se produce porque la estrategia usada en [37] implementa una partición dinámica de un espacio de características compuesto por todos los píxeles de la imagen, por lo tanto, la estrategia de Lin obtiene una adecuada detección de marca de agua, mientras la imagen marcada no sufra un ataque que involucre una considerable pérdida de información.

Cuando la imagen marcada es rotada con un ángulo mayor a  $15^\circ$ , se produce una mayor pérdida de información de la imagen, entonces, el detector no puede recuperar totalmente la marca de agua, porque la partición dinámica es llevada a cabo con píxeles que no contienen información de la imagen (regiones en color negro de la figura 4.9 (b)). Del mismo modo sucede cuando una imagen marcada es recortada. Por lo tanto, la pérdida de información de la imagen es directamente proporcional a la cantidad de recorte aplicado a la imagen marcada (regiones en color negro de la figura 4.9 (c)). La figura 4.9 (a) muestra una imagen marcada, (b) su versión rotada por  $45^\circ$  con auto recorte-escalamiento y (c) versión recortada.

Por otro lado, cuando la imagen marcada es distorsionada por otros procesamientos de señal tales como compresión JPEG, cambio de aspecto, filtrado mediano, entre otros, la marca de agua puede ser detectada con mayor efectividad, porque estas operaciones producen una distorsión en la imagen que no involucra pérdida de información de la imagen, por lo que, la marca de agua puede ser recuperada y detectada. Los resultados experimentales muestran que el método propuesto en esta tesis tiene una mayor robustez ante los ataques geométricos y de tipo procesamiento de señal, excepto ante distorsiones que cambian los colores de la imagen, tal es el caso del ataque StirMark ConvFilter, el cual, es un ataque que aclara y oscurece la imagen; por otro lado, la ecualización de histograma también es un ataque ante el cual el esquema propuesto en esta tesis no es robusto.

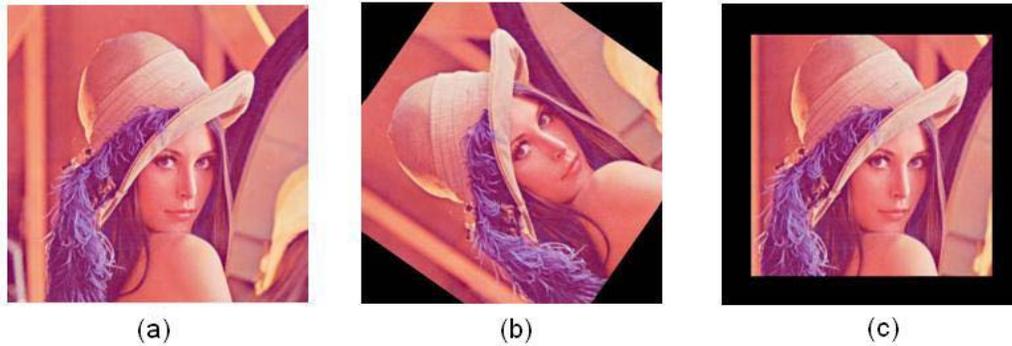


Figura 4.9. (a) Imagen marcada, (b) versión rotada por 45° con auto-recorte y escalamiento, (c) versión recortada.

En la tabla 4.7 se realiza una comparación de rendimiento entre el método propuesto y trabajos previos basados en otras estrategias, tales como el esquema basado en normalización de imagen propuesto por [46], el método basado en histograma de color propuesto por [36], el algoritmo de marca de agua orientado a histograma propuesto en [37], el esquema basado en valores característicos propuesto por [29], el esquema basado en un dominio invariante desarrollado por [23] y el método basado en el uso de plantilla propuesto por [27].

TABLA 4.7  
COMPARACION DE RENDIMIENTO

Comparación	Zheng <i>et al.</i> [23] (Basado en dominio invariante)	Kang <i>et al.</i> [27] (Basado en plantilla)	Tang y Hang [29] (Basado en características)	Roy <i>et al.</i> [36] (Basado en histograma)	C.H. Lin <i>et al.</i> [37] (Basado en histograma)	M. Cedillo <i>et al.</i> [46] (Basado en normalización de imagen)	Método propuesto (Basado en histograma)
Compresión JPEG (QF)	10-100	10-100	40-100	50-100	20-100	20-100	30-100
Escalamiento	0.6-1.3	detectada	-	1.2 – 1.4	0.75 – 1.5	0.4-2	0.2 – 1.8
Recorte	detectada	Hasta-65%	Hasta 10%	Hasta 60%	Hasta 15%	-	Hasta 55%
Cambio de aspecto	-	detectada	-	-	detectada	detectada	detectada
Rotación (con Auto-recorte y escalamiento)	0°-360°	detectada	1°-5°	0° - 40°	1° - 15°	detectada	0° - 360°
Deformación de planos paralelos	10 columnas o 10 filas	X5% Y5%	X1% Y1%	-	X5% Y5%	X5% Y5%	X5% Y5%
Filtrado mediano	Detectada	-	2x2	-	4x4	3x3	4x4
Ruido Gaussiano	Detectada necesaria o	-	detectada	detectada	-	detectada	detectada
Imagen original para detección	uso de búsqueda exhaustiva	Detección a ciegas	Detección a ciegas	Detección a ciegas	Detección a ciegas	Detección a ciegas	Detección a ciegas
Carga Útil de marca de agua	64 bits	60 bits	16 bits	256 bits	128 bits	64 bits	256 bits

Esta comparación incluye parámetros que permitan realizar una comparación equitativa en lo posible, así, se elige la compresión JPEG, escalamiento, recorte, cambio de aspecto, rotación, deformación de planos paralelos, contaminación por ruido Gaussiano y filtrado mediano. La tabla 4.7 muestra la comparación de rendimiento junto con el método de detección de marca de agua (a ciegas o no ciegas) y la longitud de marca de agua asociada con cada esquema. Los resultados muestran un mejor rendimiento del método propuesto en este trabajo comparado con el rendimiento mostrado por los otros métodos previamente reportados ante las distorsiones geométricas y procesamiento de señal. Siguiendo con la tabla 4.7, el algoritmo propuesto muestra una mejor robustez de la marca de agua ante una gran variedad de ataques, además, presenta robustez ante ataques combinados, como rotación con compresión JPEG, como se muestra en las tablas 4.5 y 4.6.

#### 4.4.4 Capacidad del Detector.

En el detector, el número de bits de marca de agua extraídos tienen una distribución binomial [29], la cual está dada por (4.13):

$$P = \sum_{i=T}^n (P_s)^i \cdot (1 - P_s)^{n-i} \cdot \left( \frac{n!}{i!(n-i)!} \right), \quad (4.13)$$

donde  $n$  es el número total de bits de marca de agua,  $i$  es el número de bits extraídos correctamente,  $T$  es el valor Umbral y  $P_s$  es la probabilidad de éxito.

Para una imagen no marcada, los bits extraídos pueden asumirse como una prueba de Bernoulli con probabilidad de éxito igual a 0.5, por lo tanto, la probabilidad de falsa alarma [29] con un valor Umbral  $T$  esta dada por (4.14):

$$P_{fa} = \sum_{i=T}^n \left(\frac{1}{2}\right)^n \cdot \left(\frac{n!}{i!(n-i)!}\right) \quad (4.14)$$

La probabilidad de detección de la marca de agua cuando la imagen realmente contiene una marca de agua de algún usuario, es calculada por (4.13) usando diferentes valores de probabilidad de éxito  $P_s$ . El valor de  $P_s$  depende del ataque que la imagen marcada ha recibido. La probabilidad de éxito  $P_s$  está determinada por (4.15).

$$P_s = \frac{\text{Total Number of Matching Bits}}{\text{Total Number of Watermark Data Bits}} \quad (4.15)$$

El número total de bits extraídos correctamente se obtiene aplicando un criterio similar al usado en [29], en el cual los bits correctos son extraídos después de que la imagen marcada es atacada con una distorsión combinada (ataque geométrico y procesamiento de señal). Por lo tanto, tres probabilidades de éxito  $P_s$  son calculadas cuando tres tipos de ataques combinados son aplicados a la imagen marcada, los cuales son clasificados como dificultad baja, moderada y alta, como se muestra en la tabla 4.8.

TABLA 4.8  
PROBABILIDADES DE ÉXITO PARA TRES TIPOS DE ATAQUES COMBINADOS

Ataque	Probabilidad de éxito $P_s$	Dificultad
JPEG 70 + Remove Cols-Rows	0.8671	Baja
JPEG 70 + rotation 15°with autocrop	0.7578	Moderada
JPEG 70 + sharpening 3x3	0.7188	Alta

Basados en las anteriores probabilidades de éxito y usando diferentes valores de Umbral (desde 175 hasta 190), las curvas de las características operativas del receptor (ROC) son graficadas como se muestra en la figura 4.10.

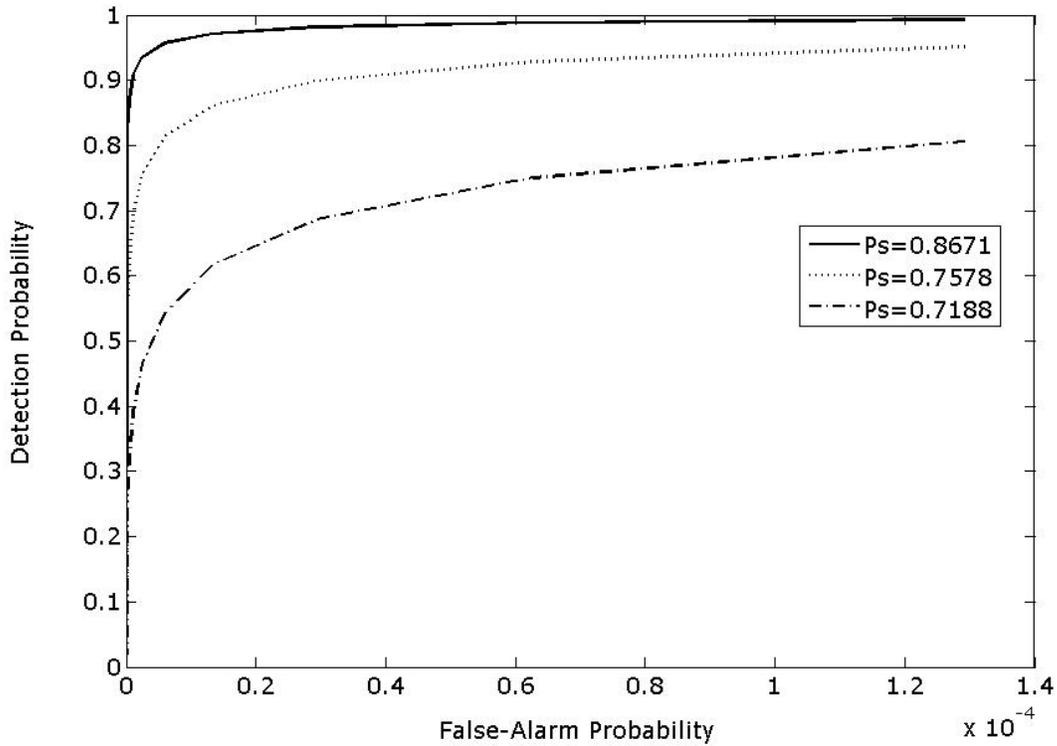


Figura 4.10. Gráfica de curvas ROC para tres probabilidades de éxito.

Como se puede observar en la figura 4.10, conforme la probabilidad de éxito disminuye, la probabilidad de detección también disminuye, debido al aumento en la complejidad del ataque combinado aplicado a la imagen marcada, lo cual afecta a la detección de la marca de agua.

## Conclusiones

En este capítulo se presento una técnica de marca de agua robusta a distorsiones geométricas y otros esquemas de procesamiento de señales. El método de marca de agua propuesto es aplicado en imágenes a color y está basado en dos modificaciones realizadas a histogramas de dos dimensiones (2D) obtenidos de la imagen.

En la primera modificación, una región del histograma en dos dimensiones compuesto por las componentes de color rojo y verde (R-G) obtenidas de la imagen, fue modificada de acuerdo al patrón de marca de agua. En la segunda modificación, un histograma en dos dimensiones compuesto por la componente de color azul (B) y la componente de color rojo filtrada ( $R_f$ ) fue particionado dinámicamente para insertar el patrón de marca de agua. Los resultados experimentales mostraron la robustez del método ante diversas distorsiones geométricas, operaciones comunes de procesamiento de señales y algunos ataques combinados. También se realizó una comparación con métodos reportados previamente que mostraron un mejor comportamiento del método propuesto.



## Capítulo 5

# Esquema Robusto de Marca de Agua Basado en Puntos Característicos y Normalización de Imagen

### 5.1 Introducción

Como se ha comentado en los capítulos 3 y 4, en esquemas de marca de agua pública, la pérdida de sincronización entre la etapa de inserción y detección provoca errores en la detección de la marca de agua. Distorsiones geométricas tales como la rotación, el escalamiento y transformaciones de tipo Affine, las cuales son muy comunes en la práctica, son los principales factores que provocan esta pérdida de sincronización.

En este capítulo, se presenta un esquema de marca de agua robusto a distorsiones geométricas y procesamientos de señal, basado en puntos característicos extraídos de la imagen. Inicialmente, la imagen original es normalizada y a partir de la versión normalizada, se extraen los puntos característicos de la misma. Posteriormente, se obtienen los puntos característicos más estables y son usados para generar diversas regiones circulares no traslapadas. Para mejorar la imperceptibilidad de la marca de agua, se hace uso de una clasificación de texturas de la imagen basada en el dominio de la Transformada Discreta del Coseno (DCT). Finalmente, la marca de agua es insertada dentro de las regiones clasificadas haciendo uso del dominio DCT. Por su parte, en la etapa de detección, la marca de agua puede ser obtenida sin la ayuda de la imagen original. Los resultados experimentales muestran la robustez del esquema ante distorsiones geométricas tales como rotación, escalamiento y diversas transformaciones Affine, así como procesamientos de señal común tales como la compresión de imagen JPEG y la contaminación por ruido.

## **5.2 Trabajos relacionados.**

Los esquemas de marca de agua que se basan en características de la imagen utilizan estas características sobresalientes para re-sincronizar la etapa de inserción y detección, sin necesidad de insertar alguna señal adicional dentro de la imagen. Los métodos de esta categoría son llamados comúnmente como esquemas de marca de agua de segunda generación. El concepto de segunda generación de marcado de agua fue reportado por primera vez en [56]. La idea principal es que la información de marca de agua sea asociada con características sobresalientes de la imagen las cuales son invariantes a distorsiones geométricas. En el trabajo reportado en [57], se presenta un método de marca de agua basado en puntos característicos de la imagen. Dichos puntos son extraídos para construir un mosaico que contiene regiones triangulares y así poder insertar la información de marca de agua en el dominio espacial. En la etapa de detección, el método extrae los puntos característicos a partir de la imagen marcada, la cual ha sido o no distorsionada. Usando estos puntos característicos, el mosaico con regiones triangulares es reconstruido y la marca de agua es detectada por una operación de correlación. Este esquema es robusto a pequeñas rotaciones y escalamiento. Sin embargo, la extracción de puntos característicos no es del todo estable en este método. Como resultado de este hecho, el conjunto de regiones triangulares obtenidas en las etapas de inserción y detección son diferentes. En [29], se propone otro esquema de marca de agua que usa puntos característicos, los cuales son extraídos por medio de una función llamada Mexican Hat wavelet. Posteriormente, se genera un conjunto de parches basados en los puntos característicos detectados. Una marca de agua de 16 bits de longitud es insertada dentro de bloques en el dominio de la Transformada Discreta de Fourier (DFT). En este método, la marca de agua es robusta ante ataques de rotación y recorte de imagen. Sin embargo, no presenta robustez al escalamiento de imagen. Además, la robustez ante la rotación está limitada a ángulos menores de  $5^\circ$ . En [58], se propone un algoritmo de marca de agua robusto a rotación, escalamiento y traslación (RTS). En este método, la marca de agua es insertada dentro de regiones locales de la imagen. Estas regiones son extraídas usando un detector de puntos característicos Harris.

Para dar robustez ante ataques de escalamiento, la imagen original es normalizada antes de la extracción de los puntos característicos. Localmente se eligen los puntos característicos más estables y son utilizados para generar diversas regiones circulares no traslapadas. Una vez obtenidas estas regiones circulares no traslapadas, se aplica una normalización ante rotación a estas regiones y los bits de marca de agua son insertados en el dominio DCT. Este esquema presenta robustez ante algunos procesamientos de señales como la compresión JPEG, distorsiones de tipo RST y algunos ataques combinados. Sin embargo, la robustez ante la rotación es obtenida únicamente para ángulos menores a  $30^\circ$  y no presenta robustez ante otro tipo de distorsiones geométricas como las transformaciones Affine. En este trabajo se presenta un esquema de marca de agua robusto a distorsiones geométricas y de tipo procesamiento de señal. Inicialmente la imagen original es normalizada y los puntos característicos son obtenidos de la versión normalizada de la imagen. Posteriormente, se obtienen los puntos característicos con mayor estabilidad y son usados para generar regiones circulares no traslapadas. Para proporcionar una mejor imperceptibilidad a la marca de agua, se realiza una clasificación de texturas en el dominio DCT. La marca de agua es insertada y detectada dentro de las regiones clasificadas en el dominio DCT. En la etapa de detección, la marca de agua es obtenida sin la ayuda de la imagen original. Los resultados experimentales muestran la robustez del método ante distorsiones geométricas tales como rotación, escalamiento y transformaciones de tipo Affine, así como ataques de tipo procesamiento de señal como compresión JPEG y contaminación por ruido. El presente trabajo es diferente al esquema propuesto en [58] en los siguientes puntos: a) En este trabajo se utiliza una clasificación de texturas en el dominio DCT, de modo que la clasificación de textura de cada bloque es usada para determinar adecuadamente la energía de inserción de la marca de agua y así mejorar la imperceptibilidad de la misma. b) A diferencia del esquema propuesto en [58], en el cual la normalización de escala y rotación es usada, en este trabajo se hace uso de un proceso de normalización de imagen global para obtener mayor robustez a una gran variedad de distorsiones geométricas así como transformaciones de tipo Affine.

### 5.3 Detector de esquinas de Harris.

El detector de esquinas de Harris [55] permite detectar los puntos característicos de una imagen original  $f(x,y)$  a partir de una matriz  $M$  de segundo momento, la cual está dada por la ecuación (5.1):

$$M = \begin{bmatrix} A & C \\ C & B \end{bmatrix} = \begin{bmatrix} \left( \frac{\partial f(x,y)}{\partial x} \right)^2 * \omega & \left( \frac{\partial f(x,y)}{\partial x} \right) \left( \frac{\partial f(x,y)}{\partial y} \right) * \omega \\ \left( \frac{\partial f(x,y)}{\partial x} \right) \left( \frac{\partial f(x,y)}{\partial y} \right) * \omega & \left( \frac{\partial f(x,y)}{\partial y} \right)^2 * \omega \end{bmatrix}, \quad (5.1)$$

donde  $\omega$  es una función Gaussiana y  $*$  denota convolución. El determinante y el trace de  $M$  son calculados por (5.2) y (5.3) respectivamente:

$$Det(M) = \lambda_1 \lambda_2 = AB - C^2, \quad (5.2)$$

$$Tr(M) = \lambda_1 + \lambda_2 = A + B = \left( \frac{\partial f(x,y)}{\partial x} \right)^2 * \omega + \left( \frac{\partial f(x,y)}{\partial y} \right)^2 * \omega, \quad (5.3)$$

Por tanto, la respuesta del detector es:

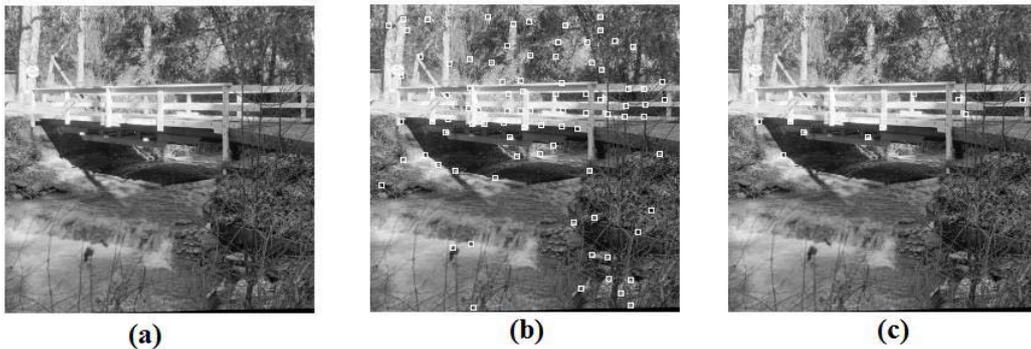
$$R_H = Det(M) - k Tr^2(M), \quad (5.4)$$

donde  $k$  es una constante dentro del rango 0.04 a 0.15 de acuerdo a [55].

Los puntos característicos de la imagen son detectados por una comparación entre  $R$  y un umbral predeterminado, como se muestra en (5.5):

$$R_H(i, j) > Th \ \& \ \max_{(i,j) \in \Omega} R_H(i, j), \quad (5.5)$$

De acuerdo a la ecuación (5.5), un punto es seleccionado en cada región  $\Omega$  en la cual  $RH$  es un valor máximo y excede un umbral predeterminado  $Th$ . Cuando el valor umbral es pequeño, el número de puntos característicos se incrementa, por otro lado, si el valor umbral se incrementa, el número de puntos característicos disminuye. La figura 5.1 muestra un ejemplo de extracción de puntos característicos de la imagen Bridge.



**Figura 5.1** (a) Imagen Original. (b) Puntos característicos obtenidos con un valor umbral 10. (c) Puntos característicos obtenidos con un valor umbral 100.

#### 5.4 Normalización de imágenes.

El proceso de normalización de imágenes usado en el esquema de marca de agua presentado en este capítulo es el mismo que se usó para el desarrollo del algoritmo de marca de agua presentado en el capítulo 3 de esta tesis. Por lo tanto, por tratarse del mismo procedimiento y con el propósito de evitar repetir información que es común entre ambos esquemas, el detalle del proceso de normalización de imágenes puede ser consultado en el capítulo 3 de esta tesis.

#### 5.5 Selección de puntos característicos invariantes.

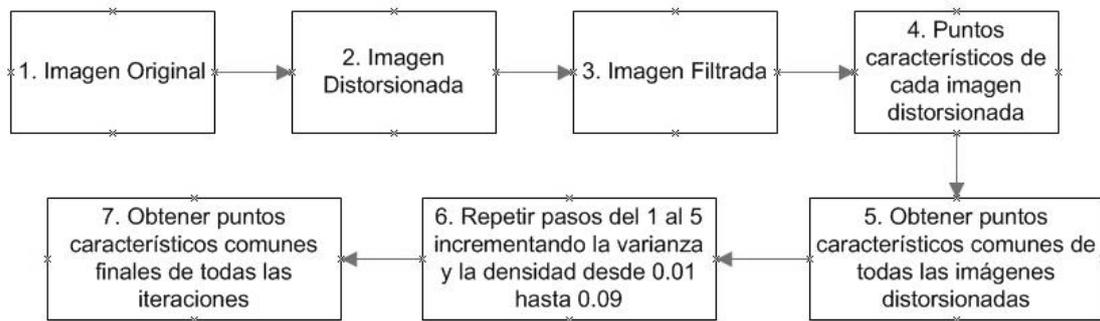
El algoritmo de marca de agua propuesto hace uso de regiones invariantes basadas en un detector de puntos característicos de Harris, en las cuales se lleva a cabo la inserción de la marca de agua. Sin embargo, los puntos característicos de Harris son sensibles principalmente al cambio de escalas, contaminación por ruido impulsivo y Gaussiano.

Para combatir esta problemática, se propone normalizar la imagen antes de la detección de los puntos característicos. De acuerdo al procedimiento de normalización de imágenes [31], [33], la imagen normalizada obtenida a partir de un proceso de transformación geométrica es invariante a distorsiones Affine y diversos ataques geométricos. El hecho de detectar los puntos característicos dentro de la versión normalizada de la imagen asegura la integridad de estos ante ataques de tipo geométrico. Esta estrategia resuelve la sensibilidad a los cambios de escala mencionados con anterioridad.

Por otro lado, para resolver la sensibilidad de los puntos característicos de Harris ante el ruido impulsivo y Gaussiano, la imagen es procesada como se describe a continuación:

- 1) Aplicar a la imagen original una transformación Affine, contaminarla con ruido Gaussiano con un valor de media  $M=0$ , varianza  $\sigma=0.01$ , y aplicar ruido impulsivo con una densidad  $d=0.01$ . Las imágenes resultantes son denotadas como  $f_{\text{affine}}(x,y)$ ,  $f_{\text{Gaussian}}(x,y)$  y  $f_{\text{impulsive}}(x,y)$  respectivamente.
- 2) Filtrar cada imagen con un filtro pasa-bajas, por ejemplo, un filtrado de mediana de ventana  $3 \times 3$ .
- 3) Obtener la imagen normalizada de  $f_{\text{affine}}(x,y)$ ,  $f_{\text{Gaussian}}(x,y)$  y  $f_{\text{impulsive}}(x,y)$ . Las imágenes resultantes son denotadas por  $f_{N\text{-affine}}(x,y)$ ,  $f_{N\text{-Gaussian}}(x,y)$  y  $f_{N\text{-impulsive}}(x,y)$ .
- 4) Obtener los puntos característicos de Harris de  $f_{N\text{-affine}}(x,y)$ ,  $f_{N\text{-Gaussian}}(x,y)$  y  $f_{N\text{-impulsive}}(x,y)$ . Los puntos característicos resultantes son denotados por  $FP_{\text{affine}}$ ,  $FP_{\text{Gaussian}}$  y  $FP_{\text{impulsive}}$  respectivamente.
- 5) Obtener los puntos característicos invariantes a partir de  $FP_{\text{affine}}$ ,  $FP_{\text{Gaussian}}$  y  $FP_{\text{impulsive}}$ .
- 6) Repetir los pasos 1 al 5 incrementando el valor de la varianza  $\sigma$  y la densidad  $d$  desde 0.01 hasta 0.09. La razón principal de seleccionar este intervalo es que el esquema debe ser robusto ante la contaminación por ruido y al mismo tiempo, la sensibilidad de los puntos característicos de Harris es resuelta. Si se utiliza un valor mayor a 0.09 de varianza  $\sigma$  ó de densidad  $d$  para contaminar una imagen ya sea con ruido Gaussiano ó impulsivo, la distorsión visual obtenida de la imagen contaminada es inaceptable.

7) Obtener los puntos característicos comunes que son invariantes, esto es, comparando los puntos característicos de  $FP_{affine}$ ,  $FP_{Gaussian}$  y  $FP_{impulsive}$  obtenidos en todas las iteraciones realizadas previamente. Finalmente, los puntos característicos comunes son considerados los más estables y robustos ante diversos ataques. Este procedimiento se ilustra en la figura 5.2.



**Figura 5.2** Extracción de puntos característicos de Harris invariantes.

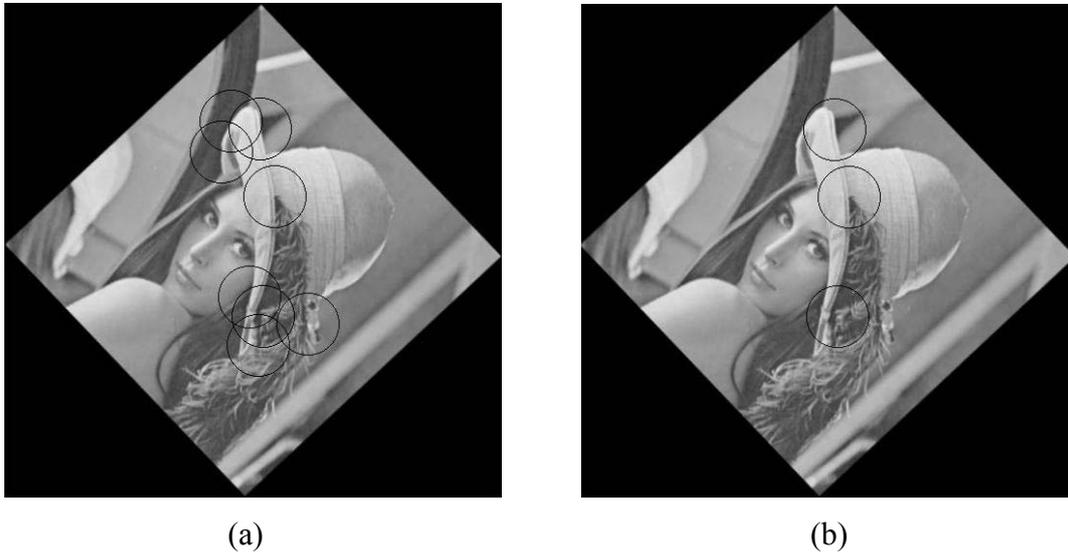
## 5.6 Proceso de Inserción.

El proceso de inserción de marca de agua se describe a continuación:

- 1) Aplicar el proceso de normalización de imágenes a la imagen original para obtener la versión normalizada.
- 2) Aplicar el proceso de extracción de puntos característicos de Harris invariantes mencionado en la sección anterior, para obtener los puntos más adecuados.
- 3) Una vez extraídos los puntos característicos, para cada punto característico, se genera una ventana circular de radio  $r$ . Esta ventana circular es denotada por  $S_l$ .
- 4) Para obtener las regiones circulares no traslapadas, algunos puntos característicos son descartados de acuerdo a la ecuación (5.6).

$$S_2 = \{(x, y) \mid (x, y), (s, t) \in S_1, U_{x,y} \cap U_{s,t} = null\} \quad , \quad (5.6)$$

donde  $U_{x,y}$  y  $U_{s,t}$  son ventanas circulares. La figura 5.3 muestra los puntos característicos finalmente seleccionados así como las regiones circulares no traslapadas.



**Figura 5.3** Regiones circulares obtenidas a partir de puntos característicos invariantes de Harris. (b) Regiones circulares no traslapadas.

- 5) Construir un parche de  $N \times N$  píxeles dentro de cada región circular no traslapada.
- 6) Dividir cada parche en bloques de  $8 \times 8$  píxeles y clasificar los bloques en texturas Fuertes y débiles. Para estimar la complejidad de textura, se usa la técnica propuesta por [44]. Primeramente, los coeficientes DCT de cada bloque son cuantificados usando el mismo método que el usado en el estándar de compresión JPEG. Si el  $k$ -ésimo bloque  $F_k(u,v), 0 \leq u, v \leq 7$ , satisface la siguiente condición (5.7), este bloque es clasificado como bloque de textura fuerte; en otro caso, el bloque es considerado como textura débil.

$$\text{if } F_k(0,0) > T_1 \text{ and } \text{number}\{\lfloor F_k(u,v)/Q(u,v) \rfloor \neq 0\} > T_2, \quad (5.7)$$

donde la notación  $\lfloor \cdot \rfloor$  es una función de redondeo, la función  $\text{number}\{\text{condición}\}$  obtiene el número de elementos que satisfacen la condición y  $Q(u,v)$  es el valor de cuantificación de la matriz en el dominio de la frecuencia  $(u,v)$ .  $T_1$  y  $T_2$  son dos valores umbrales predefinidos.

- 7) Crear una imagen mascara  $M$ , la cual es una imagen binaria, que contiene valores 1 dentro del área de la imagen normalizada y valores 0 fuera del área de la imagen normalizada, con los mismos factores de escalamiento y rotación usados para obtener la imagen normalizada. Este patrón es únicamente usado como soporte de la marca de agua.
- 8) Generar una marca de agua  $W=[w_1, w_2, \dots, w_n]$  usando una llave de usuario secreta, donde  $w_i = \{1, -1\}$ ,  $i=1..n$ .
- 9) Localizar cada parche dentro de la imagen mascara  $M$ .
- 10) Los coeficientes en el rango de frecuencias medias de cada bloque con textura fuerte y débil dentro del parche son remplazados con los elementos del patrón de marca de agua. Previamente, los elementos que son insertados dentro de las regiones con texturas fuertes son multiplicados por un factor de ganancia  $\alpha_1$ . Del mismo modo, los elementos que son insertados dentro de las texturas débiles, son multiplicados por un factor de ganancia  $\alpha_2$ . Posteriormente, aplicar la Transformada Discreta del Coseno Inversa (IDCT) a cada bloque marcado para obtener el patrón marcado  $M_w$ .
- 11) Aplicar el proceso de normalización inverso al patrón de marcado  $M_w$  para obtener el patrón de marca de agua  $W_p$  con las mismas dimensiones de la imagen original.
- 12)  $W_p$  es insertado dentro de la imagen original de forma aditiva con un factor de ganancia  $\alpha_3$ . Esto produce la imagen con marca de agua.

$$I_w = I_o + (W_p \cdot \alpha_3) \quad , \quad (5.8)$$

donde  $I_o$  y  $I_w$  son la imagen original y la imagen marcada respectivamente, y  $W_p$  es el patrón de marca de agua generado en el paso 11.

El procedimiento anterior es equivalente a insertar la marca de agua en el dominio DCT de la imagen normalizada. Los bloques con textura débil y fuerte permiten insertar adecuadamente la marca de agua sin provocar alguna distorsión visual a la imagen marcada.

## 5.7 Proceso de Detección.

El proceso de detección de marca de agua se describe a continuación:

- 1) Aplicar el procedimiento de normalización a la imagen marcada y obtener la versión normalizada.
- 2) Aplicar el proceso de extracción de puntos característicos invariantes de Harris a la imagen normalizada, el cual es el mismo que se utilizó en el proceso de inserción.
- 3) Similarmente al proceso de inserción, obtener los parches marcados, dividir cada parche en bloques de 8x8 píxeles y aplicar la DCT a cada bloque. Extraer los coeficientes  $C_W$  de cada bloque a partir del rango de frecuencias medias. La marca de agua extraída  $W'$  está formada por (5.9)

$$\begin{aligned} W' &= [w_1, w_2, \dots, w_{N-1}, w_N] \\ w_k &= \text{sign}(C_{Wk}) \end{aligned} \quad , \quad (5.9)$$

donde  $w_k$  es la secuencia de marca de agua extraída ( $L$  bits) de cada  $k$ -ésimo bloque y  $\text{sign}$  es una función signo. Finalmente, se hace uso de una correlación normalizada para evaluar la similitud de la marca de agua:

$$N_c = \frac{\sum_{i=1}^n W(i)W'(i)}{\sqrt{\sum_{i=1}^n W(i)^2} \sqrt{\sum_{i=1}^n W'(i)^2}} \quad , \quad (5.10)$$

donde  $n$  es la longitud de la marca de agua mientras que  $W$  y  $W'$  son la marca de agua original y extraída respectivamente.

La decisión es realizada considerando el valor máximo de la correlación normalizada  $N_c$  obtenido de todos los parches.

## 5.8 Resultados experimentales.

En la simulación computacional, se utilizaron imágenes en escala de grises con 8.-bits de resolución de tamaño 512 x 512, así como dos valores umbral  $T_1$ ,  $T_2$ , para clasificar los bloques en dos categorías: texturas fuertes y débiles, a los cuales se les asigno los valores 217 y 18, respectivamente. El método propuesto es evaluado desde el punto de vista de imperceptibilidad de marca de agua y robustez ante diversos tipos de distorsiones geométricas y de procesamiento de señal común. El software utilizado fue Matlab versión 7.0, y Stirmark Benchmark 4.0.

### 5.8.1 Imperceptibilidad de marca de agua

Una marca de agua binaria de 256-bits de longitud fue insertada de forma redundante 2 veces dentro del conjunto de imágenes. El factor de fuerza de inserción  $\alpha_3$  fue incrementado desde 0.01 hasta 0.1. El valor final de  $\alpha_3$  después de aplicar las pruebas de imperceptibilidad fue 0.03, usando simultáneamente valores 6 y 3.5 para los factores de fuerza de inserción  $\alpha_1$  (para texturas fuertes) y  $\alpha_2$  (para texturas débiles) respectivamente. En la figura 5.4 se muestra la imagen original y la imagen marcada de Lena, así como la imagen de diferencia entre ambas imágenes. La imagen de diferencia es magnificada para propósitos ilustrativos.



**Figura 5.4** (a) Imagen original de Lena. (b) Imagen marcada. (c) Diferencia entre (a) y (b).

En la figura 5.4 se puede observar que la marca de agua insertada en la imagen original de Lena no es visible a simple vista. Para realizar una comparación equitativa con los resultados reportados en [58], la tabla 5.1 muestra la relación señal a ruido pico (PSNR) de las imágenes de Lena, Peppers y House.

TABLA 5.1  
PSNR PROMEDIO DE IMÁGENES DE LENA, PEPPERS Y HOUSE

Imagen	Método propuesto por Lei-da et al. [58]	Método propuesto
Lena	37.4 dB	39.3 dB
Peppers	37.0 dB	38.7 dB
House	36.1 dB	38.1 dB

La tabla 5.1 muestra que la imperceptibilidad de marca de agua en términos de PSNR obtenida en el método propuesto tiene un mejor comportamiento con respecto al método de Lei-da et al. [58].

### 5.8.2 Robustez de marca de agua

Para evaluar la robustez de la marca de agua en el método propuesto, se aplicaron diversos ataques a las imágenes marcadas. La tabla 5.2 muestra un comparativo de robustez del método propuesto y los resultados reportados en el esquema de Lei-da et al. [58] en términos de correlación normalizada de la marca de agua extraída.

Un guión '-' en la tabla 5.2 indica que el resultado no fue reportado en el documento. De la tabla 5.2 se puede observar que el método propuesto por Lei-da et al. [58] presenta mejor comportamiento en algunos ataques con respecto al método propuesto en este capítulo, por ejemplo, cuando la imagen no ha sido atacada, contaminación por ruido Gaussiano, escalamiento y algunos ataques combinados compuestos por escalamiento y compresión JPEG.

Por otro lado, el método propuesto en esta tesis presenta un mejor rendimiento y robustez con respecto al documento de Lei-da et al. [58] ante una gran variedad de distorsiones, como son transformaciones de tipo Affine, contaminación por ruido impulsivo, deformación en planos paralelos (shearing), cambios de aspecto, voltear imagen (flipping) y cambio de contraste (sharpening), entre otros.

Aunque el valor de correlación normalizada obtenido en el método propuesto en este capítulo está por debajo de 1.0 aún cuando la imagen no ha sido atacada, la robustez y el comportamiento presentado es mejor con respecto al esquema de Lei-da et al. [58], porque el valor de correlación normalizada es mayor a 0.7 en todos los casos, cuando se establece un valor umbral  $Th = 0.7$ , por consecuencia, el método propuesto en este capítulo puede detectar la secuencia de marca de agua ante una gran variedad de ataques.

TABLA 5.2  
CORRELACION NORMALIZADA DE LA MARCA DE AGUA EXTRAIDA

Ataques	Lei-da et al. [58]	Método propuesto
Sin ataque	1.0	0.9733
Ruido Gaussiano $M=0, \sigma=0.01$	1.0	0.9012
Ruido impulsivo con densidad $d=0.09$	-	0.9145
Filtrado mediano 3x3	0.8310	0.8106
Compresión JPEG QF=50	0.9193	0.9375
Rotación 30°	0.8930	0.9219
Escalamiento 1.4	1.0	0.9317
Remover 5 filas y 17 columnas	0.9973	0.9063
Rotación 30° + JPEG QF=80	0.8750	0.7902
Escalamiento 1.5 + JPEG QF = 80	1.0	0.8030
Transformación Affine	-	0.9120
Shearing con factor (0.7%)	-	0.9265
Cambio de aspecto (1.2,1.0)	-	0.9516
Flipping Horizontal y Vertical	-	0.9428
Sharpening [0 -1 0; -1 5 -1; 0 -1 0]	-	0.8520

## Conclusiones

En este capítulo, se presento un método de marca de agua robusto a distorsiones geométricas y procesamientos de señal, basado en puntos característicos extraídos de la

imagen. Inicialmente, la imagen original es normalizada y a partir de la versión normalizada, se extraen los puntos característicos de la misma.

Posteriormente, se obtienen los puntos característicos más estables y son usados para generar diversas regiones circulares no traslapadas. Para mejorar la imperceptibilidad de la marca de agua, se hace uso de una clasificación de texturas de la imagen basada en el dominio de la Transformada Discreta del Coseno (DCT). Finalmente, la marca de agua es insertada dentro de las regiones clasificadas haciendo uso del dominio DCT. Por su parte, en la etapa de detección, la marca de agua puede ser obtenida sin la ayuda de la imagen original. Los resultados experimentales muestran la robustez del esquema ante distorsiones geométricas tales como rotación, escalamiento y diversas transformaciones Affine, así como procesamientos de señal común tales como la compresión de imagen JPEG y la contaminación por ruido.

El comportamiento del algoritmo propuesto en este capítulo fue comparado principalmente con el algoritmo propuesto por Lei-da et al. en [58] desde el punto de vista de imperceptibilidad y robustez de la marca de agua. Los resultados del comparativo muestran que el algoritmo propuesto en este capítulo tiene mayor robustez ante una gran variedad de distorsiones, entre las cuales se incluyeron transformaciones de tipo Affine, contaminación por ruido impulsivo, deformación en planos paralelos (shearing), cambios de aspecto, volteo de imagen (flipping) y cambios en contraste (sharpening), manteniendo una imperceptibilidad de marca de agua aceptable.

## Capítulo 6

# Conclusiones Generales y Trabajo a Futuro

### 6.1 Conclusiones Generales

Las marcas de agua digitales han sido propuestas como una solución eficiente para la protección de los derechos de copia y propiedad de los archivos de datos multimedia, posibilitando la identificación de la fuente, autor, propietario, distribuidor o consumidor autorizado, en el caso particular de esta tesis, de las imágenes digitales. Por tales motivos, el campo de las marcas de agua en imágenes digitales constituye un gran reto para la comunidad de investigadores interesados en el mismo.

En sus inicios, los esquemas de marca de agua aplicados a imágenes digitales consideraron ataques para comprobar la robustez de la marca de agua, como son el filtrado, contaminación por ruido y compresión JPEG, dichos esquemas suelen resultar robustos frente a la mayoría de los ataques descritos anteriormente.

Sin embargo, un problema de la robustez de las marcas de aguas son los ataques que dan lugar a una interpolación de la señal digital que representa la información. En el caso particular de imágenes digitales, estos ataques pueden realizarse mediante rotación, traslación de un número no entero de píxeles, cambios de escala y recortes de imagen. Una distorsión geométrica en una imagen marcada provoca que se elimine la sincronización con la cual la marca de agua fue insertada originalmente. Esta pérdida de sincronización ocasiona errores en la detección de la marca de agua cuando se aplica el proceso de detección correspondiente. Por lo tanto, los ataques geométricos se consideran ataques agresivos ante los cuales es muy difícil que una marca de agua logre sobrevivir.

Tomando en cuenta los hechos mencionados anteriormente, los ataques geométricos deben ser considerados de alta prioridad cuando se lleva a cabo el diseño de un algoritmo de marca de agua cuyo objetivo es proteger el derecho de autor.

En esta tesis se realizó el desarrollo de tres métodos de marca de agua aplicados en imágenes digitales que fueron diseñados para combatir diversas distorsiones geométricas entre las que se encuentran rotación, escalamiento y traslación (RST), transformaciones de tipo Affine, cambios de aspecto, entre otros, sin dejar de tomar en cuenta los ataques por procesamiento de señal como la compresión JPEG, el filtrado, la contaminación por ruido, entre otros. Es importante mencionar que los tres métodos también contemplan la combinación de distorsiones geométricas y de tipo procesamiento de señal. El software utilizado como herramienta de simulación computacional fue Matlab versión 7, y como herramienta estándar para aplicar distorsiones a las imágenes marcadas fue StirMark BenchMark en su versión 4.0.

El primero de los tres algoritmos propuestos hace uso de una técnica de normalización de imágenes para obtener características invariantes de la imagen ante las distorsiones geométricas. Una de las principales aportaciones en este primer trabajo fue el mejorar la imperceptibilidad de la marca de agua con respecto al trabajo reportado con anterioridad por [33], haciendo uso de una clasificación de texturas basada en el dominio de la DCT, la cual fue usada para clasificar cada bloque de la imagen a fin de poder insertar una marca de agua fuerte y mantener al mismo tiempo la imperceptibilidad de la misma. La técnica propuesta es una técnica de marca de agua con detección a ciegas. El método permite insertar información en forma de patrón pseudo-aleatorio y de pequeños logotipos binarios. Los resultados experimentales mostraron la imperceptibilidad de la marca de agua y su robustez ante diversas distorsiones geométricas, como son rotación, escalamiento, transformaciones Affine, y otros esquemas de procesamiento de señales, tales como compresión JPEG, contaminación de imagen por ruido Gaussiano e impulsivo. Finalmente, el comportamiento de este algoritmo fue comparado con tres métodos basados en estrategias diferentes para combatir los ataques geométricos, observándose un mejor rendimiento del método propuesto.

El segundo esquema tiene su base en dos modificaciones a histogramas de color en dos dimensiones obtenidos a partir del modelo de color RGB. Ambas modificaciones son complementarias para hacer frente a distorsiones geométricas, procesamientos de señal y combinaciones de ataques. Debido a que el histograma de una imagen es considerado como un dominio invariante geoméricamente, si la marca de agua puede ser insertada dentro de este dominio (histograma), está puede sobrevivir a las distorsiones geométricas. Tomando en cuenta que los trabajos basados en modificación de histograma reportados con anterioridad presentan algunas deficiencias ante ataques de tipo geométrico, la principal aportación de este trabajo fue el combatir dichas debilidades, principalmente a la rotación combinada con recorte y recortes grandes de imagen. Los resultados experimentales obtenidos mostraron la robustez ante diversas distorsiones geométricas, procesamiento de señal y combinación de ambas distorsiones. Finalmente, se llevo a cabo una comparación de rendimiento con trabajos previamente reportados, observándose un mejor rendimiento del método propuesto.

El tercer y último esquema está basado en el uso de puntos característicos y normalización de imágenes. Este trabajo pertenece a los métodos de marca de agua de segunda generación, ya que la idea principal es que la información de marca de agua sea asociada con características sobresalientes de la imagen las cuales son invariantes a distorsiones geométricas. Sin embargo, existen algunas deficiencias de los métodos basados en la extracción de puntos característicos, que están asociadas a la sensibilidad al cambio de escalas, contaminación por ruido impulsivo y Gaussiano. La principal aportación de este método es mitigar dicha sensibilidad y al mismo tiempo diseñar un método de marca de agua robusto a una gran variedad de ataques sin descuidar la imperceptibilidad de la marca. Los resultados experimentales muestran que el algoritmo propuesto en este trabajo presento una mayor robustez ante una gran variedad de distorsiones en comparación a los trabajos reportados con anterioridad, entre las cuales se incluyeron transformaciones de tipo Affine, contaminación por ruido impulsivo, deformación en planos paralelos (shearing), cambios de aspecto, volteo de imagen (flipping) y cambios en contraste (sharpening), entre otros, así como combinación de ataques, manteniendo una imperceptibilidad de marca de agua aceptable.

Los esquemas mostraron robustez ante una variedad de distorsiones geométricas y operaciones de procesamiento de señales, sin embargo, se presentaron ciertas debilidades que se plantean resolver en el trabajo a futuro de este capítulo.

## 6.2 Trabajo a Futuro

Los esquemas diseñados para implementar las estrategias propuestas en esta tesis utilizan tres técnicas diferentes, de este modo, una técnica de normalización de imágenes y clasificación de texturas fue usada en el primer método, el cual está orientado hacia imágenes en escala de grises, por su parte, el segundo esquema está basado en modificación de histograma de dos dimensiones y está orientado hacia imágenes de color y finalmente el tercer método se basa en el uso de puntos característicos y normalización de la imagen, orientado a imágenes en escala de grises.

Los resultados obtenidos en los tres esquemas fueron satisfactorios, sin embargo, es posible mejorar el desempeño de los esquemas en los siguientes aspectos como trabajo a futuro.

*Técnica robusta de marca de agua basada en normalización de imágenes:*

- Realizar la clasificación de texturas utilizando otra transformación en el dominio de la frecuencia, como puede ser la Transformada Wavelet Discreta o alguna otra transformación.
- Mejorar la robustez del método ante más distorsiones geométricas, principalmente el recorte de imagen y distorsiones geométricas aleatorias Stirmark RBA.

*Esquema robusto de marca de agua basado en modificación de histograma:*

- Mejorar la robustez del método ante ataques que implican un cambio significativo en los colores de la imagen y modifican la distribución del histograma de la imagen, tal es el caso de la ecualización del histograma.
- Mejorar la imperceptibilidad de la marca de agua tomando en cuenta no afectar la robustez de la misma ante distorsiones geométricas y procesamiento de señales comunes.
- El problema de inserción de múltiples marcas de agua afecta a la mayoría de técnicas de marca de agua que se han propuesto hasta la actualidad. El método propuesto en esta tesis garantiza únicamente la extracción de la marca de agua que es recién insertada en el material digital al momento de aplicar el método, por lo tanto, esta problemática tiene que ser resuelta en el futuro.

*Esquema de marca de agua basado en puntos característicos y normalización de imágenes:*

- Mejorar la robustez del método ante más distorsiones geométricas, principalmente el recorte de imagen y distorsiones geométricas aleatorias Stirmark RBA.
- Mejorar el procedimiento de obtención de puntos característicos invariantes a cambios de escala, contaminación por ruido impulsivo y Gaussiano.



---

---

## Referencias

- [1] G. C. Langelaar, I. Setyawan, R. L. Lagendijk. “*Watermarking Digital Image and Video Data*”, IEEE Signal Processing Magazine, Vol. 17. 2000. pp. 20-46.
- [2] I. J. Cox, M. L. Miller, J. A. Bloom. “*Digital Watermarking*”, San Francisco CA, Morgan Kaufmann Publishers, 2002.
- [3] J.J. Eggers, J.K. Su and B. Girod. “*Robustness of a Blind Image Watermarking Scheme*”, International Conference on Image Processing (ICIP 2000), Vancouver, Canada, September 2000.
- [4] M. Barni, F. Bartolini, R. Caldelli, A. Piva. “*Geometric-Invariant Robust Watermarking through Constellation Matching in the Frequency Domain*”, Proceedings of 7th IEEE International Conference on Image Processing ICIP 2000, Vancouver, Canada, , Vol. II, pp. 65 -68, September 10-13, 2000.
- [5] M. Kutter and F. Hartung, “*Introduction to Watermarking Techniques*”, cap. 5, pp. 97-120. Computer Security Series. Artech House, 1<sup>st</sup>. Ed, 2000.
- [6] S. Craver, A. Periig, and F. A. P. Petitcolas “*Robustness of copyright marking systems*”, cap. 7, pp. 149-174. Computer Security Series. Artech House, 1<sup>st</sup>. Ed, 2000.
- [7] F. Ergün, J. Kilian, and R. Kumar, “*A note on the limits of collusion resistant watermarks*”, in *EUROCRYPT*, pp. 140-149. 1999.
- [8] J. A. Bloom, I. J. Cox, T. Kalker, J. Linnartz, and M. L. Miller, “*Copy protection for dvd video*”, in Proceedings of the IEEE, Vol. 87. Jul. 1999.
- [9] I. Cox, J. Kilian, T. Leighton, y T. Shamoan, “*Secure spread spectrum Watermarking*” for multimedia. IEEE Transactions on Image Processing, 6(12):1673-1687, 1997.
- [10] V. Solachidis and I. Pitas, “*Circularly Symmetric Watermark Embedding in 2-D DFT Domain*”, IEEE Trans. Image Process, vol. 10 no. 11, pp 1741-1753 Nov. 2001.
- [11] P. Loo and N. G. Kingsbury “*Digital watermarking using complex wavelets*” (trimmed version). Inf. tech., Department of Engineering, Cambridge University, U.K, 1999.
- [12] J. Ó Ruanaidh and T. Pun, “*Rotation, scale and translation invariant digital image watermarking,*” in Proc. ICIP’97, vol. 1, , pp. 536–539, Atlanta, GA, Oct.1997.

- 
- [13] F. A. P. Petitcolas, R. J. Anderson, M. Kuhn. “Attacks on copyright marking systems”. II Int. Workshop on Information Hiding, pp. 218-238, 1998.
- [14] F. A. P. Petitcolas and R. J. Anderson, “Evaluation of copyright marking Systems”. in IEEE Multimedia Systems (ICMCS'99), págs. 574-579. Florencia, Italia, Jun. 1999.
- [15] S. Pereira, S. Voloshynovskiy, M. Madueno, S. Marchand-Maillet, and T. Pun, “Second generation benchmarking and application oriented evaluation”. in I. S. Moskowitz, ed., *Information Hiding*, Vol. 2137 Lecture Notes in Computer Science, pp. 340-353. Springer, 2001.
- [16] V. Links and R. Jordan, “Geometric Attacks on Image Watermarking Systems”, IEEE Multimedia, vol. 12, no. 3, pp. 68-78, 2005.
- [17] L. G. Brown, “A survey of image registration techniques”. Ed. ACM Computing Surveys, 24(4): 1992, pp.325-376.
- [18] A. Nikolaidis and I. Pitas, “Region-Based Image Watermarking”, IEEE Trans. on Image Processing, vol. 10, no. 11, pp. 1726-1739, 2005.
- [19] R. D. Brandt and F. Lin, “Representations that uniquely characterize image modulo transformation”, Pattern Recognition Letters, vol. 17, no. 8, pp. 1011-1015, 1996.
- [20] I. Rothe, H. Susse and K. Voss, “The Method of Normalization to determine invariants”, IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 18, no. 4, pp. 366-376, 1996.
- [21] D. Shen and H. S. Ip, “Generalized Affine Invariant Image Normalization”, IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 19, no. 5, pp. 431-440, 1997.
- [22] J. Ó Ruanaidh and T. Pun, “Rotation, Scale, and Translation Invariant Spread Spectrum Digital Image Watermarking”, Signal Processing, vol. 66, no. 3, pp. 303-317, 1998.
- [23] D. Zheng, J. Zhao and A. E. Saddik, “RST-Invariant Digital Image Watermarking Based on Log-Polar Mapping and Phase Correlation”, IEEE Trans on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 753-765, 2003.
- [24] C-Y. Lin, M. Wu, J. A. Bollm, I. Cox, M. Miller and Y. Lui, “Rotation, Scale and Translation Resilient Watermarking for Image”, IEEE Trans on Image Processing, vol. 10, no. 5, pp. 767-782, 2001.
- [25] S. Bravo Solorio, “Marca de Agua Robustas a Ataques Geométricas”, Tesis de Maestría en Ciencias en Ingeniería Eléctrica de Universidad Michoacana de San Nicolás de Hidalgo, 2005.
- [26] S. Pereira and T. Pun, “Robust Template Matching for Affine Resistant Image Watermarks”, IEEE Trans. on Image Processing, vol. 9, no. 6, pp. 1123-1129, 2000.

- 
- [27] X. Kang, J. Huang, Y. Q. Shi and Y. Lin, "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression", IEEE Trans. on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 776-785, 2003.
- [28] R. Caldelli, M. Barni, F. Bartoroni and A. Piva, "Geometric-Invariant Robust Watermarking Through Constellation Matching in the Frequency Domain", Proc. of IEEE Image Processing ICIP 2000, vol. 2, pp. 65-68, 2000.
- [29] C.W. Tang and H.M. Hang, "A Feature-Based Robust Digital Image Watermarking Scheme", IEEE Trans. on Signal Processing, vol. 15, no. 4, pp. 930-959, 2003.
- [30] E. Izquierdo, "Using Invariant Image Features for Synchronization in Spread Spectrum Image Watermarking", EURASIP Journal on Applied Signal Processing, vol. 4, pp. 410-417, 2002.
- [31] M. K. Hu. "Visual Pattern Recognition by Moment Invariants". IRE Trans. on Information Theory. Vol. 8. pp. 179-187. 1962.
- [32] M. Alghoniemy and A. H. Tewfik, "Geometric Invariance in Image Watermarking", IEEE Trans. on Image Processing, vol. 13, no. 2, pp. 145-153, 2004.
- [33] P. Dong, J. B. Brankov, N. P. Galatsanos, Y. Yang, F. Davoine. "Digital Watermarking robust to geometric distortions". IEEE Trans. on Image Processing. Vol. 14, pp. 2140-2150, 2005.
- [34] D. Coltuc and P. Bolon: "Robust watermarking by histogram specification", 6<sup>th</sup> IEEE Conf. on image Processing (ICIP' 99), Kobe, Japan, Vol. 2, 1999, pp. 236-239
- [35] G. Chareyron, B. Macq and A. Tremeau: "Watermarking of color images based on segmentation of the XYZ color space", CGIV Second Eur. Conf. on Color in Graphics, Imaging and Vision, Aachen, Germany, 2004 pp. 178-182
- [36] S. Roy and E.C. Chang: "Watermarking color histogram", in Proc. IEEE Int. Conf. on Image Processing, Singapore, 2004, pp. 2191-2194
- [37] C.H. Lin, D.Y. Chan, H. Su and Hsieh W.S.: "Histogram oriented watermarking algorithm: color image watermarking scheme robust against geometric attacks and signal processing", IEE Proc.-Vis. Image Signal Process., Vol. 153, No. 4, 2006, pp. 483-492
- [38] R. J. de Burgós, "Álgebra lineal". Ed. McGraw-Hill, 1997.
- [39] D. Delannay, J. Delaigle, B. M. Macq, and M. Barlaud "Compensation of geometrical deformations for watermark extraction in digital cinema Application", in Proc. SPIE Vol. 4314, p. 149-157, Security and Watermarking of Multimedia Contents III, Ping Wah Wong; Edward J. Delp; Eds., pp. 149-157. 2001.

- 
- [40] S. Belkasim and M. Kamel “*Fast computation of 2-D image moments using biaxial transform*”, Pattern Recognition Society, vol. 34, Issue 9, pp.1867-1877, September 2001.
- [41] S.X. Liao and M. Pawlak, “*On image Analysis by Moments*”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, issue 3, pp. 254-266, 1996.
- [42] R. González y R. E. Woods, “*Tratamiento Digital de Imágenes*”, Madrid, Ed. Addison-Wesley, 1996
- [43] D. Shen, H. S. Ip, K. K. T. Cheung, and E. K. Teoh, “*Symmetry detection by generalized complex (GC) moments: A close-form solution,*” IEEE Trans. Pattern Analysis. Mach. Intell., vol. 21, no. 5, pp. 466–476, 1999.
- [44] J. Huang, Y. Q. Shi. “*Adaptive image watermarking scheme based on visual masking*”. *IEEE Electronics Letter*. 1998. pp. 748-750.
- [45] Signal & Image Processing Institute. University of Southern California. Electrical Engineering Department. [URL:http://sipi.usc.edu/database/database.cgi?volume=misc](http://sipi.usc.edu/database/database.cgi?volume=misc)
- [46] M. Cedillo, M. Nakano and H.M. Perez: “*Robust watermarking to geometric distortion based on image normalization and texture classification*”, in Proc. IEEE Midwest Symposium CAS, Knoxville Tennessee, pp. 245-248, 2008.
- [47] M. Cedillo, M. Nakano and H.M. Perez: “*Robust watermarking based on histogram modification*”, in IEEE International Conference on Multimedia & Expo (ICME), Workshop on Multimedia Security and Content Protection, New York, USA, pp. 1748-1751, 2009.
- [48] Y.L. Lee, H.C. Kim and H.W. Park: “*Blocking effect reduction of JPEG images by signal adaptive filtering*”, IEEE Trans. Image Process., Vol. 7, No. 2, 1998, pp. 229-234
- [49] T.Q. Pham and L.J. Van Vliet,: “*Blocking artifacts removal by a hybrid filter method*”, ASCI 2005 Proc. of the eleventh annual conf. of the Advanced School for Computing and Imaging, ASCI Delft. Heijen, the Netherlands, 2005, pp. 372-377
- [50] G. Wyszecki and W.S. Stiles., “*Color Science: concepts and methods, quantitative data and formulae*”, Second Edition., Wiley, New York, 1982, 950 p. An exhaustive reference text for the expert, multitudes of tables.
- [51] < [http://www.colorwiki.com/wiki/Delta\\_E:\\_The\\_Color\\_Difference](http://www.colorwiki.com/wiki/Delta_E:_The_Color_Difference) >
- [52] H. Chang and H.H. Chen, “*Stochastic Color Interpolation for Digital Cameras,*” IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 8, pp. 964-973, Aug 2007.
- [53] K. N. Plataniotis, A. N. Venetsanopoulos, “*Color Image Processing and Applications*”, Springer Verlag, Berlin, 2000

- 
- [54] H.R. Sheikh and A.C. Bovik, "*Image information and visual quality*," IEEE Transactions on Image Processing, vol. 15, no. 2, pp. 430-444, Feb 2006.
- [55] Harris C, Stephens M., "*A combined corner and edge detector*," Proceedings of the Fourth Alvey Vision Conference, Manchester, UK, pp. 147-151, Aug 31-Sep 2, 1988.
- [56] Kutter M, Bhattacharjee S K, Ebrahimi T. "*Towards second generation watermarking schemes*". Proceedings of IEEE International Conference on Image Processing, Oct 24-28, 1999, Kobe, Japan. Piscataway, NJ, USA, IEEE, 1999, pp. 320-323
- [57] Bas P, Chassery J M, Macq B. "*Geometrically invariant watermarking using feature points*", IEEE Transactions on Image Processing, 2002, vol. 11, no. 9, pp. 1014-1028
- [58] Lei-da L., Bao-long G., Lei G., "*Rotation, scaling and translation invariant image watermarking using feature points*", in The Journal Of China Universities Of Post And Telecommunications, 2008, vol. 15, issue 2, pp.82-87
- [59] R.C. Gonzalez and R.E. Woods, "*Digital Image Processing*", Third Edition, Prentice Hall, pp. 839-841, 2008.

# Anexo A

## Lista de Publicaciones.

### REVISTAS INTERNACIONALES

- 1.- Manuel Cedillo Hernández, Mariko Nakano Miyatake, Héctor Pérez Meana: *“Técnica robusta de marca de agua basada en normalización de imágenes”* Revista Facultad de Ingeniería Universidad de Antioquia, Medellín Colombia, Sudamérica, No. 52, pp. 147-160, Marzo 2010. Revista Indizada ISI-JCR.
- 2.- Manuel Cedillo Hernández, Mariko Nakano Miyatake, Héctor Pérez Meana: *“Robust watermarking scheme based on histogram modification”* Actualmente en revision. Revista Facultad de Ingeniería Universidad de Antioquia, Medellín Colombia, Sudamérica. Revista Indizada ISI-JCR.

### MEMORIAS DE CONGRESOS INTERNACIONALES

- 1.- M. Cedillo, M. Nakano, H.M. Perez, K. Yamagushi and W. Na: *“Robust image watermarking using feature points and image normalization”*, in IEEE Electronics, Robotics and Automotive Mechanics Conference (CERMA 2010), Cuernavaca, Morelos, pp. 313-318, 2010.
- 2.- M. Cedillo, M. Nakano and H.M. Perez: *“Robust watermarking based on histogram modification”*, in IEEE International Conference on Multimedia & Expo (ICME), Workshop on Multimedia Security and Content Protection, New York, USA, pp. 1748-1751, 2009.
- 3.-M. Cedillo, M. Nakano and H.M. Perez: *“Robust watermarking to geometric distortion based on image normalization and texture classification”*, in Proc. IEEE Midwest Symposium CAS, Knoxville Tennessee, pp. 245-248, 2008.
- 4.- M. Cedillo Hernandez, M. Nakano Miyatake, H.M. Perez Meana: *“Geometric Distortions Resilient Watermarking Technique Based on 2D Color Histogram Modification”*, in 5th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2008), Mexico City, Mexico, 2008, pp. 286-291.

## Técnica robusta de marca de agua basada en normalización de imágenes

### A robust watermarking technique based on image normalization

*Manuel Cedillo Hernández\**, *Mariko Nakano Miyatake*, *Héctor Pérez Meana*

Sección de Posgrado e Investigación, Instituto Politécnico Nacional, Unidad Culhuacan Av. Santa Ana 1000 San Francisco Culhuacan, Coyoacán, México D.F., México

(Recibido el 29 de agosto de 2008. Aceptado el 23 de septiembre de 2009)

#### Resumen

En este artículo se presenta una técnica de marca de agua robusta a distorsiones geométricas y otros esquemas de procesamiento de señales. En el método de marca de agua propuesto, se hace uso de una técnica de normalización de imágenes para obtener características invariantes de la imagen ante las distorsiones geométricas. Los procesos de inserción y detección de la marca de agua se realizan en el dominio de la Transformada Discreta del Coseno (DCT). Una clasificación de texturas basada en el dominio de la DCT se usa para clasificar cada bloque de la imagen a fin de poder insertar una marca de agua fuerte, manteniendo al mismo tiempo la imperceptibilidad de la misma. La técnica propuesta es una técnica de marca de agua pública, en la cual, la imagen original no está disponible en el proceso de detección de la marca de agua. Los resultados experimentales muestran la imperceptibilidad de la marca de agua y su robustez ante las distorsiones geométricas, como son rotación, escalamiento, transformaciones *Affine*, y otros esquemas de procesamiento de señales, tales como compresión JPEG, contaminación de imagen por ruido Gaussiano e impulsivo.

----- *Palabras clave:* Marca de agua, normalización de imágenes, ataques geométricos, clasificación de texturas, transformada discreta del coseno

#### Abstract

This paper presents a robust watermarking method against geometric distortions and several other signal processing schemes. In the proposed watermarking method, image normalization is used to get geometric invariant

---

\* Autor de correspondencia: teléfono + 52 + 5 + 624 2000 ext 73256, fax: + 52 + 5 + 656 20 58, correo electrónico: mcedillohdz@hotmail.com (M. Cedillo)

features. The watermark embedding and detection process are carried out in the Discrete Cosine Transform (DCT) domain. A DCT based texture classification is used to classify each image block to embed a stronger as possible watermark, while maintaining watermark imperceptibility. The proposed watermarking scheme is a public watermarking, where the original image is not available for watermark detection. The experimental results show the watermark imperceptibility and robustness against geometric distortion such as rotation, scaling and various other Affine transformation, and common signal processing schemes, such as JPEG compression, Gaussian and impulsive noise contamination.

----- *Keywords:* Digital watermarking, image normalization, geometric attacks, texture classification, discrete cosine transform

### Introducción

El propietario de derechos de autor de información en forma digital necesita, para obtener una justa remuneración económica por la información que produce, de medios tecnológicos adecuados que permitan la autenticación de dicha información, así como el seguimiento de copias ilegalmente distribuidas. En plena era de la información, las posibilidades que brinda Internet como medio de comunicación ha permitido a los autores que tienen su información en forma digital utilizar Internet para promocionar, publicar y difundir sus obras. Cualquier usuario, desde cualquier lugar y de una manera muy fácil puede acceder a estas obras intelectuales en cuestión de segundos. La posibilidad de digitalización de cualquier tipo de información (imágenes, vídeo, audio, texto, etc.) junto con la existencia de Internet permite realizar copias perfectas de la información digitalizada. Los procesos criptográficos permiten proteger la adquisición legal de la información, pero una vez obtenida la información se pueden revender copias exactas. Por lo tanto, surge la necesidad de un sistema de seguimiento de copias para la protección de los derechos de autor, que también se utilice en el caso de adquisición legal para distribución fraudulenta (copias ilegales). Ante estos riesgos, legislar resulta insuficiente, y por ello se debe hacer uso de otros mecanismos que aseguren y protejan derechos fundamentales como es el derecho de propiedad intelectual. Las marcas de agua digitales han sido

propuestas como una solución eficiente para la protección de los derechos de copia y propiedad de los archivos de datos multimedia, posibilitando la identificación de la fuente, autor, propietario, distribuidor o consumidor autorizado, de imágenes digitales, grabaciones de audio o vídeo. La principal ventaja de los sistemas de marca de agua consiste en que la marca es inseparable del contenido del archivo. Sin embargo, existen algunas cuestiones que necesitan ser resueltas, antes de que estas técnicas puedan ser eficazmente aplicadas en los escenarios de la vida real. Durante los últimos 20 años se han desarrollado numerosos algoritmos para este fin [1]. Las técnicas de marca de agua para la protección de derechos de autor deben satisfacer varios requerimientos como son: imperceptibilidad de la marca de agua insertada dentro del material digital, robustez de la misma contra ataques y no ambigüedad de la señal de marca de agua cuando se extrae del material digital, etc. [1, 2]. Para imágenes digitales, la imperceptibilidad de la marca de agua es sinónimo de invisibilidad de la señal de marca en la imagen, es decir, la imagen no debe presentar distorsión visual a causa de la inserción de la marca de agua. La robustez de la marca de agua se refiere a que una vez que la marca de agua ha sido introducida en una imagen digital, está debe sobrevivir a una amplia diversidad de ataques que la distorsionarán, así como a la imagen en la que está se inserta. Según la causa y objetivo que los origina, éstos se pueden clasificar en ataques no intencionales e intencionales. Los ataques no

tencionales son aquellos a los cuales la marca de agua está sometida de manera casi inevitable, por ejemplo, la compresión JPEG, el ruido introducido por el canal de transmisión por el que se envía la imagen marcada, entre otros. Los ataques intencionales son manipulaciones que se realizan sobre la imagen marcada con el fin de eliminar la protección de derechos de autor. Aunque en la actualidad algunas técnicas de marca de agua presentan robustez frente a algunos de los ataques antes mencionados, se siguen teniendo problemas de robustez ante ataques que dan lugar a una interpolación de la señal digital que representa la información. En el caso de imágenes, estos ataques pueden realizarse mediante distorsiones geométricas tales como rotación, traslación de un número no entero de píxeles, escalamiento, entre otros. Por lo tanto, se requiere hacer mayor énfasis en combatir las distorsiones geométricas al momento de desarrollar una técnica de marca de agua. No ambigüedad de marca de agua en el proceso de detección significa que la marca de agua extraída o detectada debe ser lo suficientemente clara para poder mostrar la propiedad de autor. Para lograr que la marca de agua cumpla el requerimiento de imperceptibilidad, reducir la energía de la señal de marca de agua es una estrategia directa que se puede tomar, sin embargo, una señal débil es más fácil que se pierda después de cualquier modificación que sufra la imagen, de manera que cuando ésta sea detectada, podría resultar ambigua. Para poder extraer la marca de agua con mayor claridad, se podría incrementar el número de bits que constituyen la marca de agua, sin embargo con esto se perjudican los otros dos requerimientos mencionados anteriormente. Por lo tanto, estos requerimientos se consideran los tres vértices de un triángulo, donde cuando se trata de mejorar uno de los requerimientos, se perjudican forzosamente los otros dos. Desde el punto de vista del proceso de detección, las técnicas de marca de agua se pueden clasificar en técnicas de marca de agua pública y privada, respectivamente. En el caso de la técnica de marca de agua pública, la marca de agua se detecta sin usar la imagen original, mientras que en la técnica privada, la imagen original es usada

para detectar la señal de marca de agua. Obviamente, en la técnica de marca de agua privada, la señal de marca de agua puede ser más robusta y menos ambigua al momento de su detección, sin embargo, en muchas aplicaciones, la imagen original no está disponible en el proceso de detección [1,2]. Debido a que la técnica de marca de agua pública requiere una detección a ciegas, cuando la imagen marcada sufre algún ataque, se puede perder la sincronización de la marca de agua entre el proceso de inserción y el proceso de detección, lo que provocaría errores de detección. Distorsiones geométricas, tales como traslación, escalamiento, rotación y cualquier transformada Affine, son algunos de los principales factores causantes de la pérdida de sincronización en el esquema de marca de agua pública. Además, este tipo de ataques ocurre comúnmente en varias aplicaciones prácticas. Por lo tanto, para combatir este problema, se han propuesto varios algoritmos en la literatura [3-13]. Los algoritmos propuestos se pueden clasificar básicamente en cinco categorías, las cuales son: los métodos basados en búsqueda exhaustiva, los que hacen uso de algún dominio invariante a distorsiones geométricas, los que utilizan una señal de re-sincronización, los que hacen uso de características relevantes de la imagen para llevar a cabo una re-sincronización y los que usan la técnica de normalización de imágenes. El método de búsqueda exhaustiva, como su nombre lo indica, realiza una búsqueda a profundidad para encontrar los factores de distorsión geométrica, tales como factor de escalamiento, ángulo de rotación, relación de aspecto entre ancho y alto de la imagen, etc. Usando los factores geométricos estimados, la imagen marcada se restaura geoméricamente antes del proceso de detección. Aunque este método es óptimo para la estimación de factores geométricos, la complejidad computacional es considerablemente alta, lo que hace que este método sea impráctico [3]. En la segunda categoría, la señal de marca de agua se inserta en algún dominio invariante a las distorsiones geométricas, tales como el dominio de la Transformada Fourier-Mellin (FMT) [4] y el uso de histogramas [5, 6]. Teóricamente la FMT es invariante a la rotación,

el escalamiento y la traslación (RST), sin embargo, la implementación discreta del mapeo Log-Polar dentro de la FMT realiza una interpolación en los píxeles de la imagen, lo cual provoca una distorsión visual en la imagen marcada. Para imágenes de color, el histograma de la imagen es usado como dominio de inserción y detección de la marca de agua [5, 6]. En los algoritmos basados en el histograma, la marca de agua insertada es robusta a un gran número de distorsiones geométricas, sin embargo, esta no es robusta a esquemas de procesamientos de señales comunes, tales como compresión JPEG, filtraje y contaminación por ruido. En la tercera categoría, una señal llamada plantilla se inserta adicionalmente a la imagen junto con la señal de marca de agua [7, 8]. En el proceso de detección, se hace uso de la plantilla para estimar los factores geométricos y restaurar la imagen marcada con alguna distorsión geométrica a su estado original. La principal desventaja de este método es que la plantilla obviamente causa distorsión visual adicional a la imagen marcada y si ésta se llega a perder por alguna razón, no se puede detectar correctamente la señal de marca de agua. La cuarta categoría trata de resolver las desventajas que presentan los métodos de la tercera categoría, en la cual, se extraen las características relevantes de la imagen y son usadas para estimar los factores geométricos, restaurando así la imagen a su estado original en el proceso de detección [9, 10]. En estos métodos, no se inserta ninguna señal adicional a la imagen, lo cual no provoca distorsión visual a la imagen, además de que las características relevantes de una imagen son más difíciles de perder que la plantilla. La principal desventaja de este método es la alta complejidad para extraer las características relevantes útiles para satisfacer los requerimientos de marca de agua en ambos procesos, el proceso de inserción y el proceso de detección. La última categoría usa la técnica de normalización de imágenes introducido por [11]. Este método está basado en un concepto en el cual, la versión normalizada de una imagen y sus versiones distorsionadas geoméricamente son exactamente iguales. Usando este concepto, la inserción y la detección de marca de agua se reali-

zan en la versión normalizada de la imagen, teóricamente el problema de pérdida de sincronización entre ambos procesos no ocurre. En la práctica, debido a que el proceso de normalización contiene interpolación, la imagen marcada sufre una distorsión visual considerable. Dong et al., propusieron dos algoritmos [12], uno de ellos está basado en la normalización de imágenes y detección de la marca de agua a ciegas; mientras que el otro algoritmo está basado en un grafo elástico para una técnica de marca de agua privada. En el primer algoritmo de Dong et al. [12], para evitar una degradación de la calidad en la imagen marcada, la señal de marca de agua se normaliza en lugar de la imagen y se inserta a la imagen en el dominio espacial [12]. El algoritmo de Dong et al. mostró robustez de la marca de agua ante varias distorsiones geométricas, sin embargo para obtener una tasa de bits erróneos (BER) razonablemente baja en el proceso de detección, la energía de la señal de marca de agua se tiene que aumentar y como consecuencia de esto, la distorsión de la imagen marcada no se puede evitar.

En este artículo, se propone un algoritmo de marca de agua basado en la normalización de imágenes, en el cual, un patrón de marca de agua es normalizado usando los mismos factores geométricos obtenidos en la normalización de imagen. Para insertar la marca de agua con mayor energía, sin perjudicar la imperceptibilidad de la misma en el algoritmo propuesto, los bloques de tamaño 8x8 píxeles que contienen coeficientes DCT de la imagen normalizada, se clasifican dependiendo de la complejidad de texturas. Usando la complejidad de cada bloque, se determina la energía o fuerza de inserción de la marca de agua para este bloque. El algoritmo propuesto es similar al algoritmo de Dong et al. [12] desde el punto de vista del uso de la normalización de imágenes, sin embargo el algoritmo propuesto difiere al de Dong et al. en los siguientes aspectos: a) La energía de inserción de la marca de agua es adaptable, considerando la complejidad de texturas de cada bloque de la imagen, b) el algoritmo propuesto fue evaluado

con un mayor número de ataques además de los ataques geométricos, c) el comportamiento del algoritmo propuesto es comparado con métodos de marca de agua basados en otras estrategias. Este artículo esta organizado de la siguiente manera: en esta sección se realizó una introducción acerca de la técnica de marca de agua y sus antecedentes sobre algoritmos de marca de agua robustos a distorsiones geométricas. Seguidamente, se describe la técnica de normalización de imágenes y el algoritmo propuesto. A continuación se presentan los resultados obtenidos por simulación computacional y finalmente las conclusiones.

## Metodología

### Normalización de imágenes

En el algoritmo propuesto, la imagen y el patrón de marca de agua son normalizados para construir un esquema de marca de agua robusto a distorsiones geométricas. En esta sección, se hace una descripción acerca de la técnica de normalización de imágenes, la cual se basa en la teoría de momentos invariantes propuesta en [11]. Aquí se describen detalladamente los procedimientos de cálculo de momentos invariantes y normalización de imágenes.

### Momentos invariantes

Los momentos geométricos  $m_{p,q}$  y los momentos centrales  $\mu_{p,q}$  de una imagen  $f(x,y)$  se definen en (1) y (2), respectivamente.

$$m_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q f(x,y) \quad (1)$$

$$\mu_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (x - \bar{x})^p (y - \bar{y})^q f(x,y) \quad (2)$$

donde  $p, q = 1, 2, \dots$ , y  $(\bar{x}, \bar{y})$  es la masa central de la imagen que se obtiene como:

$$\bar{x} = \frac{m_{10}}{m_{00}}, \bar{y} = \frac{m_{01}}{m_{00}}$$

### Procedimiento de normalización de imágenes

El procedimiento de normalización de una imagen  $f(x,y)$  consiste de las siguientes etapas:

- 1) Trasladar la imagen  $f(x,y)$  con los valores  $f(d_x, d_y)$  para generar una nueva imagen  $f_1(x,y) = f(x_a, y_a)$ , cuyo centro es igual a la masa central de la imagen  $f(x,y)$ . Esta operación esta dada por (3) usando una Transformación Affine.

$$\begin{pmatrix} x_a \\ y_a \end{pmatrix} = A \cdot \begin{pmatrix} x \\ y \end{pmatrix} - d \quad (3)$$

Donde:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, d = \begin{pmatrix} d_x \\ d_y \end{pmatrix}$$

Cuyos elementos son:

$$d_x = \frac{m_{10}}{m_{00}}, d_y = \frac{m_{01}}{m_{00}}$$

Este proceso normaliza una imagen respecto a la traslación.

- 2) Aplicar una transformación de deformación en la dirección  $x$  a la imagen  $f_1(x,y)$ , usando:

$$A_x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$$

La imagen resultante se denota como  $f_2(x,y)$ , la cual está normalizada ante el efecto de deformación en la dirección  $x$ .

- 3) Aplicar una transformación de deformación en la dirección  $y$  a la imagen  $f_2(x,y)$ , usando:

$$A_y = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$$

La imagen resultante se denota como  $f_3(x,y)$ , la cual está normalizada ante el efecto de deformación en la dirección  $y$ .

- 4) Cambiar el tamaño de la imagen  $f_3(x,y)$  en ambas direcciones, usando:

$$A_s = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$$

La imagen resultante se denota como  $f_4(x,y)$ , la cual esta normalizada ante el efecto de escalamiento en ambas direcciones. Finalmente la imagen  $f_4(x,y)$  es la imagen normalizada de la imagen original  $f(x,y)$ . Cabe mencionar que los procedimientos de normalización de imagen son totalmente invertibles, aplicando las matrices inversas de  $A_s, A_y, A_x$  y sumando el vector  $d$  a la imagen normalizada  $f_4(x,y)$ , obtenemos la imagen original  $f(x,y)$ . Sin embargo, para una implementación discreta de ambos procesos, el proceso de normalización y el proceso inverso requieren de una interpolación, la cual provoca una degradación en la calidad de la imagen. La determinación de los parámetros  $\alpha, \beta, \gamma$  y  $\delta$  esta basada en la siguiente teoría [11]:

Si la imagen  $g(x,y)$  es una imagen transformada de  $f(x,y)$ , aplicando una transformación *Affine* general:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, d = 0$$

$g(x,y)$  está dada por  $g(x,y) = A \cdot f(x,y)$ . Los momentos invariantes de la imagen  $g(x,y)$   $m'_{p,q}$  están dados por:

$$\begin{aligned} m'_{pq} &= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q g(x,y) \\ &= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} A \cdot x^p y^q f(x,y) \end{aligned} \quad (4)$$

Aplicando la transformación *Affine* general  $A$  en una coordenada  $(x,y)$ , se obtiene la coordenada transformada  $(x',y')$ :

$$\begin{aligned} x' &= a_{11}x + a_{12}y \\ y' &= a_{21}x + a_{22}y \end{aligned}$$

Sustituyendo las coordenadas  $(x', y')$  en (4) se tiene:

$$\begin{aligned} m'_{pq} &= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (a_{11}x + a_{12}y)^p \\ &\quad (a_{21}x + a_{22}y)^q f(x,y) \end{aligned} \quad (5)$$

Aplicando el teorema binomial en (5):

$$\begin{aligned} (a_{11}x + a_{12}y)^p &= \sum_{i=0}^p \binom{p}{i} a_{11}^i x^i a_{12}^{p-i} y^{p-i} \\ &= \sum_{i=0}^p \binom{p}{i} a_{11}^i a_{12}^{p-1} x^i y^{p-i} \end{aligned} \quad (6)$$

$$\begin{aligned} (a_{21}x + a_{22}y)^q &= \sum_{j=0}^q \binom{q}{j} a_{21}^j x^j a_{22}^{q-j} y^{q-j} \\ &= \sum_{j=0}^q \binom{q}{j} a_{21}^j a_{22}^{q-1} x^j y^{q-j} \end{aligned} \quad (7)$$

Sustituyendo (6) y (7) en (5) se obtiene:

$$\begin{aligned} m'_{pq} &= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{i=0}^p \binom{p}{i} a_{11}^i a_{12}^{p-1} x^i y^{p-i} \sum_{j=0}^q \binom{q}{j} a_{21}^j a_{22}^{q-1} x^j y^{q-j} f(x,y) \\ &= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-1} a_{21}^j a_{22}^{q-1} x^{i+j} y^{p+q-i-j} f(x,y) \\ &= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-1} a_{21}^j a_{22}^{q-1} x^{i+j} y^{p+q-i-j} f(x,y) \end{aligned} \quad (8)$$

Usando la definición de la ecuación (1) se tiene:

$$m_{i+j, p+q-i-j} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^{i+j} y^{p+q-i-j} f(x,y) \quad (9)$$

Finalmente, sustituyendo (9) en (8) se obtiene:

$$\begin{aligned} m'_{p,q} &= \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} \\ &\quad a_{11}^i a_{12}^{p-i} a_{21}^j a_{22}^{q-j} m_{i+j, p+q-i-j} \end{aligned} \quad (10)$$

De igual forma, se obtiene  $\mu'_{p,q}$ , quedando de la siguiente manera:

$$\mu'_{p,q} = \sum_{i=0}^p \sum_{j=0}^q \binom{p}{i} \binom{q}{j} a_{11}^i a_{12}^{p-i} a_{21}^j a_{22}^{q-j} \mu_{i+j, p+q-i-j} \quad (11)$$

Usando esta relación entre los momentos invariantes de la imagen normalizada y la imagen original, se estiman los parámetros  $\alpha$ ,  $\beta$ ,  $\lambda$ ,  $\delta$  de las matrices  $A_s$ ,  $A_y$ ,  $A_x$  de normalización.

La figura 1 muestra un ejemplo de normalización de imágenes, en la cual, (c) es la imagen normalizada de ambas imágenes (a) original y (b) distorsionada geoméricamente.

### Proceso de inserción

Aunque la imagen normalizada ofrece un dominio invariante a todas las distorsiones geométricas, la implementación discreta del proceso de normalización y su proceso inverso produce una degradación visual a la imagen, debido a los procesos de interpolación. Por lo tanto, en el algoritmo propuesto en vez de insertar la marca de agua en la imagen normalizada, el patrón de marca de agua es normalizado antes de su inserción, la normalización de la imagen original es usada solamente para determinar la energía de inserción adecuada, por lo que la inserción de marca de agua se lleva a cabo en el dominio espacial de la imagen sin normalizar. En esta sección se describe la creación del patrón de marca de agua y el proceso de inserción del mismo como sigue:

- 1) Aplicar el procedimiento de normalización de imágenes descrito en la sección anterior a la imagen original para generar una imagen normalizada.
- 2) Dividir la imagen normalizada en bloques de 8x8 píxeles y seleccionar los bloques con textura fuerte. Para estimar una complejidad de textura de cada bloque de la imagen normalizada, se usa la técnica propuesta

en [13]. Primero, los coeficientes de DCT de cada bloque son cuantificados usando una matriz de cuantificación que usa una codificación de entropía de JPEG. Si el k-ésimo bloque  $F_k(u, v)$ ,  $0 \leq u, v \leq 7$  satisface la condición de la ecuación (12), este bloque es clasificado como textura fuerte, en otro caso el bloque pertenece a una textura débil.



(a)



(b)

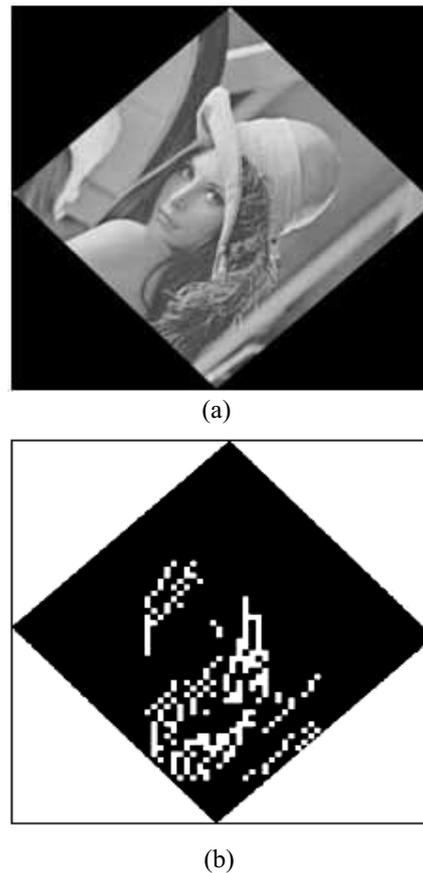


(c)

**Figura 1** (a) Imagen original (b) Versión distorsionada de la imagen (a), (c) Imagen normalizada obtenida de ambas imágenes (a) y (b)

$$\left\{ \left\lfloor \frac{F_k(0,0)}{Q(u,v)} \right\rfloor \neq 0 \right\} > T_2 \quad (12)$$

donde la notación  $\lfloor \bullet \rfloor$  es una función de redondeo hacia 0 y la función  $\text{numero}\{\text{condición}\}$  obtiene el número de elementos que satisfacen la condición, y  $Q(u, v)$  es el valor de la matriz de cuantificación en la frecuencia espacial  $(u, v)$ .  $T_1$  y  $T_2$  son dos valores umbral predeterminados, el valor de coeficiente de frecuencia cero DC del  $k$ -ésimo bloque  $F_k(0,0)$  representa el promedio de luminancia del bloque y este se encuentra en un rango de  $[0 \text{ a } (2^l-1)S]$  para un bloque de tamaño  $S \times S$  en nivel de escala de grises. Por ejemplo, si  $l=8$  bits y  $S=8$  (bloque de  $8 \times 8$ ), el rango de DC es  $[0 \text{ a } (2^8 - 1)S]$ , de modo que, cuando el bloque es plano y negro en su totalidad, el valor de DC para  $F_k(0,0)$  es 0 y, cuando el bloque es plano y blanco en su totalidad, el valor de DC para  $F_k(0,0)$  es 2040. Considerando  $l=5$ , la intensidad promedio del bloque es  $2^5 = 32$  de 255 en la escala de grises. De acuerdo al sistema visual humano SVH, el detalle de esta intensidad es imperceptible, por lo tanto, se propone un valor umbral  $T_1 = 230$ , el cual fue usado para la simulación computacional. Por otro lado, el rango de valores para  $\text{numero}\{\text{condición}\}$  es  $[1 \text{ a } 64]$ , debido a que el tamaño del bloque es  $8 \times 8$  haciendo un total de 64 coeficientes. Cuando el bloque contiene altas frecuencias, es decir, contiene detalles (por ejemplo una región con textura fuerte), los valores de alta frecuencia obtenidos después de aplicar una cuantificación con la matriz  $Q$  deben ser diferentes de cero, por lo tanto, si se desea obtener un bloque con textura fuerte, el número de altas frecuencias diferentes de cero debe ser mayor que un valor umbral  $T_2$ . La matriz de cuantificación  $Q$  usada es la misma que se utiliza para la compresión JPEG con el factor de calidad 50. La combinación de ambas condiciones en la ecuación (12) permite obtener un bloque con textura fuerte y con detalles suficientemente claros para el SVH. Un ejemplo de clasificación de bloques se muestra en la figura 2, en la cual, los bloques blancos son bloques de textura fuerte y los bloques negros son texturas débiles.



**Figura 2** Un ejemplo de clasificación de bloques por características de textura

- 3) Generar un patrón bi-dimensional pseudo-aleatorio  $R$ , cuyo tamaño es el mismo que la imagen original. Enmascarar un patrón binario  $M$  que funciona como molde al patrón pseudo-aleatorio  $R$  para generar el patrón  $MR$ .
- 4) Generar un vector de marca de agua binaria  $W = \{w_i | w_i = -1 \text{ o } 1, i = 1..n\}$ , cuyos elementos son pseudo-aleatorios y es generado por una llave secreta del propietario de la imagen. Después se multiplica por un factor de ganancia  $\alpha_i$  al vector de marca de agua, y se genera  $W' = \{\alpha_i w_i | w_i = -1 \text{ o } 1, i = 1..n\}$
- 5) Dividir el vector de marca de agua  $W'$ , generado por el paso 4 de este proceso, en  $N$  grupos de  $L$  elementos.  $L$  puede tener un valor desde 1 hasta 22, el cual es equivalente

- al número de coeficientes de frecuencia media en el bloque de DCT de 8x8 píxeles. Por ejemplo, si la longitud del vector de marca de agua  $W'$  es 500 y si el número de coeficientes  $L$  que se usan para la inserción de marca de agua es igual a 5, el número de grupos  $N$  entonces es 100 ( $N=500/5$ ).
- 6) Los elementos del patrón  $MR$  generado en el paso 3 de este proceso, que corresponden a los coeficientes en la frecuencia de banda media de los bloques de textura fuerte de la imagen normalizada, se reemplazan por los elementos de marca de agua  $W'$ . La Transformada Discreta del Coseno Inversa (IDCT) se aplica al patrón con la señal de marca de agua y se genera el patrón de marca de agua normalizado  $MR_w$ .
  - 7) Aplicar el proceso inverso de normalización de imágenes al patrón de marca de agua  $MR_w$  para obtener un patrón bidimensional de marca de agua  $WP$ .
  - 8) El patrón de marca de agua  $WP$  se inserta en la imagen original usando una inserción aditiva en el dominio espacial. La formula de la inserción esta dada en (13).
 
$$I_w = I_o + \alpha_2 WP \quad (13)$$
 donde  $I_o$  e  $I_w$  son la imagen original e imagen marcada respectivamente y  $\alpha_2$  es la energía de inserción de la marca de agua. A grandes rasgos, en el proceso de inserción de marca de agua del algoritmo propuesto, se genera un patrón bi-dimensional normalizado usando los mismos factores geométricos de la normalización de la imagen original y para que éste patrón de marca de agua sea más robusto a los esquemas de procesamiento de señales, además de mantener su imperceptibilidad, se tomaron en cuenta las características de texturas de la imagen original para realizar una inserción adaptable. Cabe mencionar que la normalización del patrón de marca de agua en lugar de la misma imagen evita una distorsión en la imagen marcada. La figura 3 muestra el proceso de inserción de marca de agua descrito anteriormente.

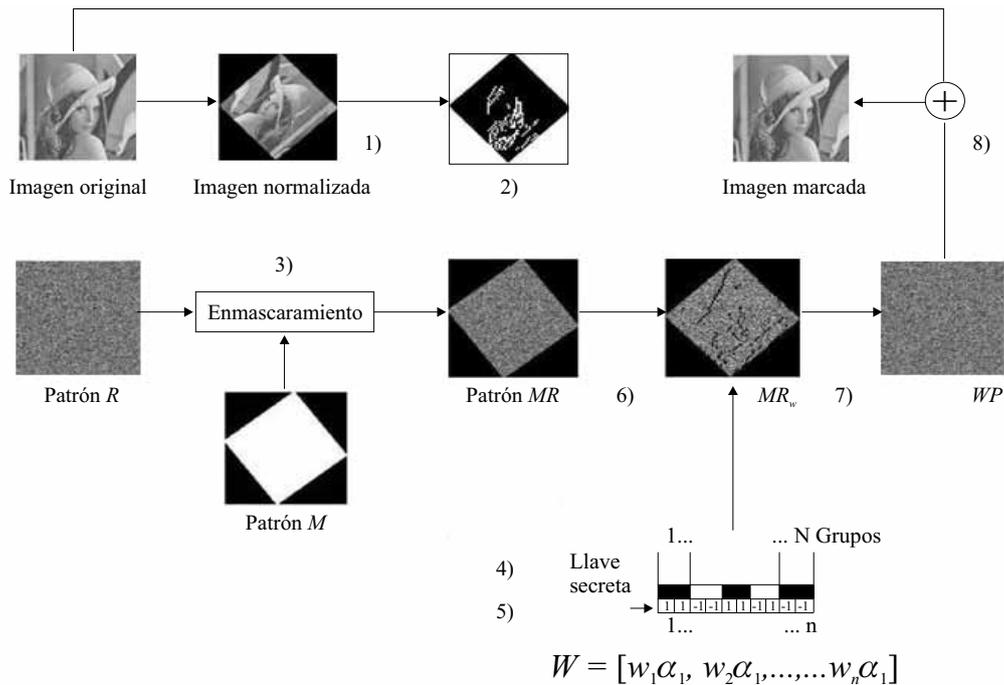


Figura 3 Proceso de inserción de marca de agua

### Proceso de detección

El proceso de detección de marca de agua se describe como sigue:

- 1) Se aplica el proceso de normalización a la imagen marcada y se obtiene la versión normalizada de la imagen marcada.
- 2) Se aplica la DCT a los bloques de 8x8 píxeles de la imagen marcada normalizada, después se clasifican los bloques en bloque con textura fuerte y bloques con textura débil. Desde los bloques con textura fuerte, se extraen los coeficientes marcados localizados en el rango de frecuencia media. Concatenando los vectores de coeficientes marcados extraídos desde todos los bloques con texturas fuertes, se genera un vector de coeficientes marcados  $CW = (cw_1, cw_2, \dots, cw_{N-1}, cw_N)$ .
- 3) Se extrae el vector de marca de agua, realizando la siguiente operación usando los elementos del vector  $CW$ .

$$\hat{W} = [\hat{w}_1, \hat{w}_2, \dots, \hat{w}_{N-1}, \hat{w}_N] \quad (14)$$

donde  $\hat{w}_k = \text{sign}(cw_k)$ ,  $\text{sign}$  es una función de signo.

La figura 4 muestra el proceso de extracción de marca de agua.

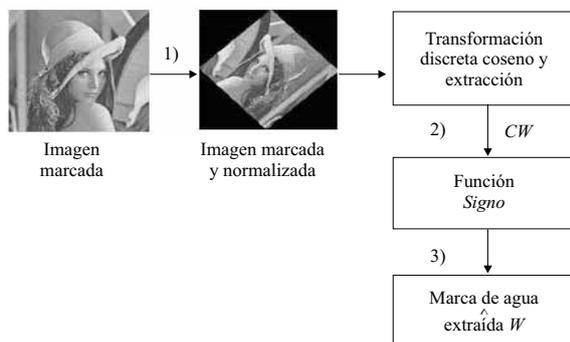


Figura 4 El proceso de extracción de marca de agua

### Resultados experimentales

Para evaluar el sistema se llevaron a cabo simulaciones computacionales en las cuales se

emplearon, imágenes de 512 x 512 píxeles en escalas de grises con 8 bits de resolución y dos valores umbrales  $T_1$  y  $T_2$ , los cuales se emplearon para clasificar cada bloque de la imagen en dos clases: bloques con textura fuerte y bloques con textura débil. A estos umbrales se les asignó los valores 230 y 13, respectivamente. El esquema propuesto es evaluado desde el punto de vista de imperceptibilidad, robustez y no ambigüedad de la marca de agua extraída.

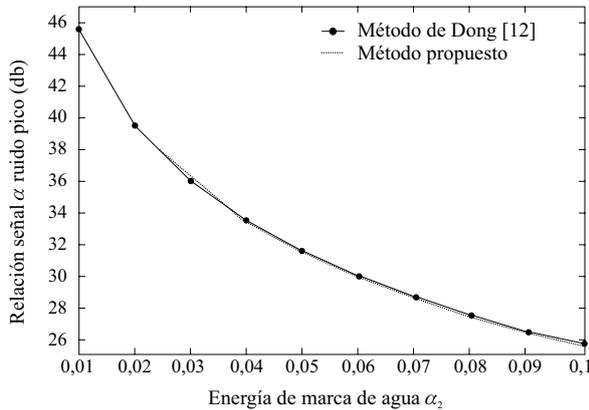
### Imperceptibilidad de la señal de marca de agua

Un vector de marca de agua binario de 64 bits es insertado 10 veces redundantemente dentro de varias imágenes. El factor de energía de la marca de agua  $\alpha_2$  es incrementado por 0,01 desde el valor 0,01 a 0,1, para medir la relación entre este factor y la imperceptibilidad de la señal de marca de agua. Con este fin, la Relación Señal a Ruido Pico (PSNR), dada por (15), entre la imagen original y la imagen marcada fue calculada para cada valor de  $\alpha_2$ .

$$PSNR(dB) = 10 \log_{10} \left( \frac{MN255^2}{\sum_{i=1}^M \sum_{j=1}^N (I_o(i, j) - I_w(i, j))^2} \right) \quad (15)$$

donde  $M \times N$  es el tamaño de la imagen,  $I_o$ ,  $I_w$  son la imagen original y la imagen marcada, respectivamente, 255 denota el máximo valor que puede tomar un píxel en la imagen, ya que la resolución de las imágenes usadas es de 8 bits. El valor de  $\alpha_1$  usado en el proceso de generación de la secuencia de marca de agua fue el valor 6 en todos los casos. La figura 5 muestra la relación entre el valor de  $\alpha_2$  y el promedio de la PSNR obtenido en 10 imágenes aplicando nuestro esquema propuesto y el esquema propuesto por Dong et al. Como podemos observar en la figura 5, la imperceptibilidad de marca de agua expresada por la PSNR con diferentes valores de  $\alpha_2$  en ambos esquemas es muy similar y en ambos

esquemas, cuando se usan los valores pequeños de  $\alpha_2 \leq 0,03$ , la PSNR es mayor que 36dB, lo cual garantiza la imperceptibilidad de la marca de agua.

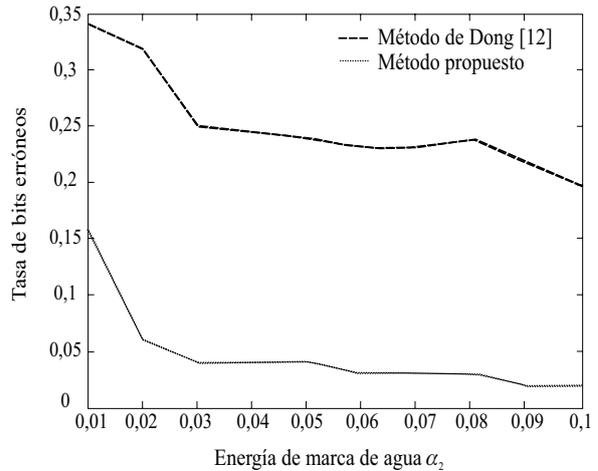


**Figura 5** Relación entre la energía de marca de agua  $\alpha_2$  y la imperceptibilidad de la marca de agua en el esquema propuesto y el esquema de Dong et al

**Ambigüedad de marca de agua extraída**

En el esquema de marca de agua, es muy importante que la señal de marca de agua extraída no sea ambigua, sobre todo si se trata de un mensaje constituido por texto en Código Estadounidense Estándar para el Intercambio de Información (ASCII) o la marca de agua es un logotipo. Considerando esta situación, la tasa de bits erróneos (BER) de la secuencia binaria de marca de agua extraída respecto a la insertada fue calculada, variando el valor de  $\alpha_2$ . La figura 6 muestra la relación entre  $\alpha_2$  y la BER de nuestro sistema propuesto y el propuesto por Dong et al. Como podemos observar en la figura 6, cuando los valores de  $\alpha_2$  son menores que 0,03, la BER de nuestro esquema es de 0,05, lo cual indica que la señal de marca de agua es suficientemente clara, así cuando la marca de agua es un mensaje de texto representado por código ASCII, el mensaje extraído es totalmente legible. Mientras que en el esquema de Dong et al., cuando el valor de  $\alpha_2 \leq 0,03$ , la BER es mayor que 0,25. Esto significa que aproximadamente un cuarto de bits

de la secuencia de marca de agua extraída son erróneos, como consecuencia de esto, cuando la señal de marca de agua es un mensaje, el mensaje extraído en el esquema de Dong et al., no es legible.



**Figura 6** Relación entre la energía de marca de agua  $\alpha_2$  y la BER en el esquema propuesto y el de Dong et al

La tabla 1 muestra una comparación de la BER entre el sistema propuesto y el sistema de Dong et al., usando imágenes bajo las mismas condiciones, tales como imperceptibilidad de la señal de marca de agua en términos de la PSNR (36 dB), número de bits de marca de agua (64 bits), lo más parecidas posible. Los valores de  $\alpha_1$  y  $\alpha_2$  usados en el esquema propuesto en este documento son 6 y 0,03, respectivamente.

**Tabla 1** Comparación de Ambigüedad de marca de agua extraída entre el método de Dong et al y el sistema propuesto en este artículo

<b>Método de Dong et al.[12]</b>	<b>Método propuesto</b>
BER = 0,25	BER = 0,04

De la tabla 1, podemos concluir que en nuestro esquema propuesto, la secuencia de la marca de agua extraída es menos ambigua, comparado con el de Dong et al.

### Robustez de marca de agua

Para evaluar la robustez de la marca de agua en el esquema propuesto, se aplicaron varios ataques a imágenes marcadas. La tabla 2 muestra la

robustez de marca de agua en términos de la tasa de bits erróneos (BER) de la marca de agua extraída después de los correspondientes ataques aplicados. En todos los casos, los valores de  $\alpha_1$  y  $\alpha_2$  son 6 y 0,03 respectivamente.

**Tabla 2** BER de la marca de agua extraída después de aplicar distintos ataques

<i>Ataques de marca de agua</i>	<i>BER</i>
Sin ataque.	0,04
Ruido Gaussiano con media $M = 0$ , varianza $\sigma = 0,01$	0,09
Ruido impulsivo con una densidad de 0,09	0,06
Filtro mediana con ventana de 3x3	0,11
Compresión JPEG con el factor de calidad QF=50	0,06
Compresión JPEG con el factor de calidad QF=25	0,14
Aplicar nitidez a la imagen con una matriz $\begin{bmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{bmatrix}$	0,06
Rotación con ángulo de 75°	0,06
Remover líneas RML=50.	0,09
Escalamiento con un factor de 1,4	0,08
Transformación de <i>Affine</i> con matriz $A = \begin{bmatrix} -1,01 & 0,2 \\ 0,2 & 0,8 \end{bmatrix}$	0,08
Deformación de planos paralelos en dirección $y$ con un factor de (0,7%), donde cada número representa el porcentaje de deformación en cada eje $(x,y)$ .	0,06
Invertir la imagen de forma horizontal y vertical	0,04
Cambio de aspecto con (1,2; 1,0), donde cada número representa el porcentaje de cambio de aspecto en cada eje $(x,y)$ .	0,06

De la tabla 2, podemos observar que la señal de marca de agua es suficientemente robusta a todos los tipos de distorsión geométrica así como a la mayoría de los procesamientos de señal comunes, tales como compresión de imágenes JPEG, contaminación por ruido y filtrado, ya que la BER de la señal de marca de agua extraída respecto a la original es menor que 0,11, excepto con la compresión JPEG con un factor de calidad 25 (en este caso BER=0,14). Este resultado garantiza una legibilidad de texto

extraído, cuando la señal de marca de agua es una secuencia de código ASCII que representa un texto. Cuando la marca de agua es una imagen de logotipo, la imagen de marca de agua extraída es totalmente clara. Respecto a las imágenes comprimidas usando el esquema de compresión JPEG con un factor de calidad menor a 25 estas imágenes se distorsionan considerablemente por la alta tasa de compresión, por lo tanto en la mayoría de las ocasiones, la imagen pierde su valor comercial.

Finalmente, el comportamiento del algoritmo propuesto es comparado con tres métodos basados en estrategias diferentes a la propuesta en este artículo. El primer método utilizado en la comparación es el propuesto por Ruanaidh y Pun en [4], el cual está basado en el uso de la FMT como dominio invariante para insertar y detectar la marca de agua. El segundo método en la comparación fue propuesto por Pereira y Pun en [7], el cual está basado en el uso de una plantilla que es utilizada como señal de re-sincronización de marca de agua en el proceso de detección. El tercer y último método es propuesto por Tang y Hang en [10]. Este método utiliza las características relevantes de la imagen para estimar factores geométricos que sirven para restaurar la imagen a

su estado original en el proceso de detección. Los parámetros utilizados para realizar la comparación del comportamiento del algoritmo son: tipo de detección y longitud de marca de agua utilizados en el método, y robustez ante los siguientes ataques: compresión JPEG, escalamiento, cambio de aspecto, rotación, deformación en planos paralelos, filtrado mediano y contaminación de imagen con ruido Gaussiano. En la tabla 3 se muestran los resultados del comparativo en cuestión de comportamiento. Un guión corto en la tabla indica que el parámetro de comparación no es reportado en el método. Los resultados muestran que el método propuesto en este artículo presenta un mejor comportamiento con respecto a los métodos usados en el comparativo.

**Tabla 3** Comparación de comportamiento con métodos basados en diferentes estrategias

<b>Parámetro de Comparación</b>	Ruanaidh y Pun [4] (Basado en Dominio Invariante)	Pereira y Pun. [7] (Basado en señal de re-sincronización)	Tang y Hang [10] (Basado en características relevantes)	Método Propuesto (Basado en normalización de imagen)
<b>Compresión JPEG (QF)</b>	75-100	75-100	40-100	20-100
<b>Escalamiento</b>	Detectada	0,75 - 2	-	0,4 – 2
<b>Cambio de aspecto</b>	-	Detectada	-	Detectada
<b>Rotación</b>	0°-360°	Detectada	1°-5°	0° - 360°
<b>Deformación de planos paralelos</b>	-	(X1%, Y1%)	(X1%, Y1%)	(X5%, Y5%)
<b>Filtrado mediano</b>	-	3x3	2x2	3x3
<b>Ruido Gaussiano</b>	-	-	Detectada	Detectada
<b>Tipo de detección</b>	Pública	Privada	Pública	Pública
<b>Longitud de marca de agua</b>	104 bits	60 bits	16 bits	64 bits

### Conclusiones

En este artículo se propuso un algoritmo de marca de agua robusto a distorsiones geométricas, tales como rotación, escalamiento, traslación

y transformación general *Affine*. En la etapa de inserción de la marca de agua, la técnica de normalización de imágenes es empleada para generar un patrón de marca de agua invariante a distorsiones geométricas, en lugar de realizar

una inserción en la imagen normalizada. Para poder proporcionar mayor robustez a la marca de agua, manteniendo la imperceptibilidad de la misma, se llevó a cabo una inserción adaptable de la marca en la imagen. Para realizar esta inserción adaptable, se estiman las características de las texturas de los bloques de la imagen usando los coeficientes de la DCT de la imagen. La extracción de la señal de marca de agua se llevó a cabo usando un esquema de normalización de imágenes y una transformación en el dominio DCT. Los resultados obtenidos por simulación computacional muestran la imperceptibilidad y no ambigüedad de la señal de marca de agua, además en el sistema propuesto, la marca de agua es suficientemente robusta contra las distorsiones geométricas y los esquemas de procesamiento de señales, tales como compresión JPEG y contaminación por ruido, entre otros. El funcionamiento del sistema propuesto fue comparado con otro esquema robusto a distorsiones geométricas el cual fue: el esquema de Dong et al., mostrándose una ventaja importante. Finalmente, el comportamiento del algoritmo propuesto es comparado con tres métodos basados en estrategias diferentes a la propuesta en este artículo. Los resultados muestran que el método propuesto en este artículo presenta un mejor comportamiento con respecto a los métodos usados en el comparativo.

### Agradecimientos

Los autores quieren agradecer al Consejo Nacional de Ciencia y Tecnología (CONACyT) de México y al Instituto Politécnico Nacional por el apoyo económico durante la elaboración de este trabajo.

### Referencias

1. I. J. Cox, M. L. Miller, J. A. Bloom. *Digital Watermarking*, San Francisco CA. Ed. Morgan Kaufmann. 2002. pp. 1-40
2. G. C. Langelaar, I. Setyawan, R. L. Lagendijk. "Watermarking Digital Image and Video Data". *IEEE Signal Processing Magazine*. Vol. 17. 2000. pp. 20-46.
3. M. Barni. "Effectiveness of exhaustive search and template matching against watermark desynchronization". *IEEE Trans. on Signal Processing Letter*. Vol. 12. 2005. pp. 158-161.
4. J. O. Ruanaidh, T. Pun. "Rotation, scale and translation invariant digital image watermarking". *Proc. ICIP'97*. Atlanta. Vol. 1. 1997. pp. 536-539.
5. S. Roy, E. Chang. "Watermarking Color Histograms". *Proc. ICIP'2004*. Vol. 1. 2004. pp. 2191-2194.
6. Z. Fan, Y. Zhao. "Image Watermarking Resisting to Geometrical Attacks Based on Histogram". *Proc. Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*. 2006. pp.79-82.
7. S. Pereira, T. Pun. "Robust template matching for affine resistant image watermarks". *IEEE Trans. on Image Processing*. Vol. 9. 2000. pp. 1123-1129.
8. J. L. Dugelay, S. Roche, C. Rey, G. Doërr. "Still-Image Watermarking Robust to Local Geometric Distortions". *IEEE Trans. on Image Processing*. Vol. 15. 2006. pp. 2831-2842.
9. E. Izquierdo. "Using Invariant Image Features for Synchronization". *Eurasip Journal on Applied Signal Processing*. Vol. 2. 2002. pp. 410-417.
10. C. Tang, H. M. hang. "A Feature-Based Robust Digital Image Watermarking Scheme". *IEEE Trans on Signal Processing*. Vol. 51. 2003. pp. 950-959.
11. M. K. Hu. "Visual Pattern Recognition by Moment Invariants". *IRE Trans. on Information Theory*. Vol. 8. 1962. pp. 179-187.
12. P. Dong, J. B. Brankov, N. P. Galatsanos, Y. Yang, F. Davoine. "Digital Watermarking robust to geometric distortions". *IEEE Trans. on Image Processing*. Vol. 14. 2005, pp. 2140-2150.
13. J. Huang, Y. Q. Shi. "Adaptive image watermarking scheme based on visual masking". *IEEE Electronics Letter*. Vol. 34. 1998. pp. 748-750.

# 2009 IEEE International Conference on Multimedia and Expo

June 28 - July 3, 2009 • New York, U.S.A.

**Organizing Committee**

**Technical Program Committee**

**Session Index**

**Author Index**

**Help**

©2009 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

IEEE Catalog No.: CFP09ICM-CDR ISBN: 978-1-4244-4291-1 ISSN: 1945-788X



# ICME 2009

## Session Index

---

### Multimedia Coding and Processing

[MCP-L1: Compression and Coding I](#)

[MCP-L2: Media Conversion and Transcoding](#)

[MCP-L3: Compression and Coding II](#)

[MCP-L4: Image Processing](#)

[MCP-L5: Compression and Coding III](#)

[MCP-L6: Multimedia Signal Processing](#)

[MCP-P1: Multimedia Coding and Processing](#)

### Multimedia Content Analysis

[MCA-L1: Content Analysis and Synthesis I](#)

[MCA-L2: Feature Extraction and Representation I](#)

[MCA-L3: Content Understanding and Knowledge Molding I](#)

[MCA-L4: Feature Extraction and Representation II](#)

[MCA-L5: Content Understanding and Knowledge Molding II](#)

[MCA-L6: Feature Extraction and Representation III](#)

[MCA-L7: Content Understanding and Knowledge Molding III](#)

[MCA-L8: Audio Analysis and Synthesis](#)

[MCA-L9: Audio / Video / Image Segmentation](#)

WS7-L3: Workshop on Media Information Analysis for Personal and Social Applications: Advances in Audio/Music Processing

WS7-L4: Workshop on Media Information Analysis for Personal and Social Applications: New Media Applications

WS8-L1: Workshop on Multimedia Aspects in Pervasive Healthcare

WS9-L1: Workshop on Multimedia Security and Content Protection

WS4-L1: Workshop on Multimedia Signal Processing and Novel Parallel Computing I

WS4-L2: Workshop on Multimedia Signal Processing and Novel Parallel Computing II

WS4-L3: Workshop on Multimedia Signal Processing and Novel Parallel Computing III

WS4-P1: Workshop on Multimedia Signal Processing and Novel Parallel Computing Posters

WS3-KN: Workshop on Emerging Multimedia Circuits and Systems Technologies: Keynote

WS3-L1: Workshop on Emerging Multimedia Circuits and Systems Technologies I

WS3-L2: Workshop on Emerging Multimedia Circuits and Systems Technologies II

WS3-L3: Workshop on Emerging Multimedia Circuits

States

**WS8-L1.5: CHARACTERIZING HUMAN SUBJECTS IN REAL-TIME AND THREE-DIMENSIONAL SPACES BY INTEGRATING THERMAL-INFRARED AND VISIBLE SPECTRUM CAMERAS**

Suk Kyu Lee, Kenton McHenry, Rob Kooper, Peter Bajcsy, University of Illinois at Urbana-Champaign, United States

**WS8-L1.6: DESIGN AND USE OF IMMERSIVE ENVIRONMENTS FOR REGAINING PROPRIOCEPTIVE ABILITIES**

Peter Bajcsy, Mike Frogley, Rob Kooper, Suk Kyu Lee, Rahul Malik, Kenton McHenry, Hyu Jung Na, Andrew Spencer, University of Illinois at Urbana-Champaign, United States

**WS8-L1.7: A FRAMEWORK TO DETECT AND CLASSIFY ACTIVITY TRANSITIONS IN LOW-POWER APPLICATIONS**

Jeffrey Boyd, Hari Sundaram, Arizona State University, United States

**WS8-L1.8: ASSOCIATION RULE MINING IN MULTIPLE, MULTIDIMENSIONAL TIME SERIES MEDICAL DATA**

G. N. Pradhan, Arizona State University, United States; B. Prabhakaran, University of Texas at Dallas, United States

**WS8-L1.9: A FRAMEWORK TO BRIDGE SOCIAL NETWORK AND BODY SENSOR NETWORK: AN E-HEALTH PERSPECTIVE**

Md. Abdur Rahman, Mohammed F. Alhamid, Abdulmotaleb El Saddik, MCRLab, Canada; Wail Gueaieb, MIRAM Laboratory, Canada

## WS9-L1: Workshop on Multimedia Security and Content Protection

**WS9-L1.1: EVALUATION OF JPEG2000 HASHING FOR EFFICIENT AUTHENTICATION**

Dominik Engel, Thomas Stütz, Andreas Uhl, University of Salzburg, Austria

**WS9-L1.2: DRM BASED ON RIGHTS CLAIM TAGS FOR LARGE-SCALE LIVE STREAMING**

Yuxuan Zhai, Minjuan Tang, Li Zhao, Tsinghua University, China

**WS9-L1.3: A NOVEL VIDEO COPY DETECTION METHOD BASED ON STATISTICAL ANALYSIS**

Hye-Jeong Cho, Yeo-Song Lee, Chae-Bong Sohn, Kwang-Sue Chung, Seoung-Jun Oh, Kwangwoon University, Republic of Korea

**WS9-L1.4: A NEW LOSSLESS DATA COMPRESSION METHOD**

Hyoungh Joong Kim, Korea University, Republic of Korea

**WS9-L1.5: STEGANALYSIS OF LSB BASED IMAGE STEGANOGRAPHY USING SPATIAL AND FREQUENCY DOMAIN FEATURES**

Hossein Malekmohamadi, Shahrokh Ghaemmaghami, Sharif University of Technology, Iran

**WS9-L1.6: ROBUST WATERMARKING BASED ON HISTOGRAM MODIFICATION**

Manuel Cedillo-Hernández, Mariko Nakano-Miyatake, Hector Perez-Meana, National Polytechnic Institute of Mexico, Mexico

**WS9-L1.7: COMPRESSED-DOMAIN TEMPORAL ADAPTATION-RESILIENT WATERMARKING FOR H.264 VIDEO AUTHENTICATION**

Sharmeen Shahabuddin, Razib Iqbal, Shervin Shirmohammadi, Jiying Zhao, University of Ottawa, Canada

**WS9-L1.8: OPTICAL WATERMARKING ROBUST TO OBJECT WITH LOW-REFLECTANCE**

Kazutake Uehira, Yasunori Ishikawa, Kazuhisa Yanaka, Kanagawa Institute of Technology, Japan

## WS4-L1: Workshop on Multimedia Signal Processing and Novel Parallel Computing I

**WS4-L1.1: MULTIMEDIA PROCESSING ON COMMODITY GRAPHICS HARDWARE**

Ruigang Yang, University of Kentucky, United States

**WS4-L1.2: SCALABLE HMM BASED INFERENCE ENGINE IN LARGE VOCABULARY CONTINUOUS SPEECH RECOGNITION**

Jike Chong, University of California, Berkeley, United States; Kisun You, Seoul National University, Republic of Korea; Youngmin Yi, Ekaterina Gonina, University of California, Berkeley, United States; Christopher Hughes, Intel Corporation, United States; Wonyong

# ROBUST WATERMARKING BASED ON HISTOGRAM MODIFICATION

*Manuel Cedillo Hernández, Mariko Nakano Miyatake, Héctor Pérez Meana*

Postgraduate and Research Section of ESIME Culhuacan  
National Polytechnic Institute. Mexico City. Mexico.  
hmpm@prodigy.net.mx

## ABSTRACT

In this paper, a robust watermarking method against geometric distortions and common signal processing is proposed. This method is based on two modifications in the 2D histograms. In the first modification, a selected region of 2D histogram composed by R-G color components is modified according to the watermark pattern. In the second modification, another 2D histogram composed by B component and image feature is dynamically partitioned to embed the watermark pattern. The experimental results show robustness against several geometric distortions, common signal processing attacks and some combination attacks. Also the comparison with the prior methods shows the better performance of the proposed method.

*Index Terms*— Copyright Protection, Digital Watermark, Geometric Attacks, RGB Color Model.

## 1. INTRODUCTION

In the public watermarking scheme, the synchronization loss, between the watermark embedding and the detection stages, causes watermark detection errors. Geometric distortions, such as rotation, scaling, translation and any Affine transformation, are the main causes of this problem, however this type of distortion is very common in practice; and then several approaches have been proposed in the literature to combat these attacks. One of these approaches uses the histogram information of the image, because the histogram is inherently invariant in geometrical processing. The use of image histograms, as watermark embedding domain, has been previously reported [1-4]. In [1], exact histogram specification is used to embed watermark into the images. In [2], the histogram-specification method proposed by [1] is extended to chromatic histograms and a watermark sequence is embedded in the chromatic plane of the color image. Authors of [3] proposed a watermarking method using a color histogram based on constrained Earth Mover Distance (EMD) to optimize the modification of the image, according to a target histogram. In [4], the authors proposed a method based on the histogram properties to measure the numerous global features of all pixels in a cover image and

to construct the three-dimensional feature space to embed the watermark. Almost all previous works based on histogram modification show watermark robustness to geometrical distortion; however they cannot provide sufficient robustness against common signal processing and some combinations of geometric attacks and common signal processing.

In this paper we propose a robust watermarking method against geometric distortions and several attacks of signal processing based on two modifications of bi-dimensional histograms. In the first modification, a 2D color histogram is composed by R and G color components, in which an adequate region is selected and modified according to binary watermark pattern. This R-G 2D histogram modification is carried out to principally combat geometric transformations, such as rotation, scaling, shearing, among others, because the image histogram is one of the geometric invariant domain, if the watermark can be embedded into this domain, it should survive to most geometric transformations. In the second modification, another 2D color histogram is composed by B color component and the image features. This histogram is dynamically partitioned in four blocks and bin values of each block are modified according to the watermark pattern. This modification is carried out to combat JPEG compression and other common signal processing attacks.

The experimental results show robustness against several geometric distortions, common signal processing attacks and combination attacks of geometric distortion and common signal processing. Also the comparison with the previously proposed methods shows better performance of the proposed method.

## 2. EMBEDDING PROCESS

In computer graphics and photography, a color histogram is a representation of the distribution of colors in an image, derived by counting the number of pixels of each color. These representations can be two-dimensional (2D) or three-dimensional (3D). In this paper, we use two different 2D color histograms to embed a binary watermark pattern. The embedding process comprises two strategies to modify the R, G and B color components.

## 2.1 Modification of 2D R-G histogram

1) Decompose the original Image  $I$  in three components  $R$ ,  $G$  and  $B$  from the RGB color model. Using  $R$  and  $G$  components, a 2D R-G color histogram  $H_{RG}$  is got. 2) Using user's secret key, generate a watermark  $W$ , which is a 2D pseudo-random binary pattern of size  $L \times L$ .  $L$  is conditioned by the  $H_{RG}$  dimensions, which is always  $256 \times 256$ , because the range of bin values is 1 to 256, thus,  $1 < L = 2^n < 256$ , where  $n = 1, \dots, 7$ . A small value for  $L$  reduces the watermark payload and then the robustness against geometric attacks is severely affected. On the other hand, choose a big value for  $L$ , the robustness against geometric attacks increases, but the watermark imperceptibility can be affected. Hence, it is recommended to select a value that provides watermark robustness and imperceptibility at same time. 3) Segment the histogram  $H_{RG}$  in blocks of size  $L \times L$ . 4) Once the histogram  $H_{RG}$  is segmented to blocks, it is necessary to select an adequate block  $BH_{RG}$  to embed watermark sequence. The condition for an adequate block is that all or almost all bin values in the block must be non-zero. This condition is required to ensure that the modification can be carried out in the correct manner. The bin value of  $BH_{RG}(j, k)$  is modified according to watermark bit  $W(j, k)$ , as shown by (1).

$$\begin{aligned} \text{if } W(j, k) = 0 \text{ then } BH_{RG}(j, k) &\leftarrow 0 \\ \text{if } W(j, k) = 1 \text{ then } BH_{RG}(j, k) &\leftarrow \text{non zero value} \end{aligned} \quad (1)$$

$j, k \in [1, L]$

To enforce  $BH_{RG}(j, k)$  to be zero, non-zero bin value of  $BH_{RG}(j, k)$  is distributed uniformly between its four neighbors. where  $j, k = 1, \dots, L$ . This embedding method ensures the watermark imperceptibility, because the modified values are assigned to the neighbor bins, so that there are slight changes in the colors of the image and the total number of bins is not altered with respect the original one. To enforce  $BH_{RG}(j, k)$  to be non-zero, non-zero neighbor's bin value is transferred. 5) Once the histogram  $H_{RG}$  is modified, all bin values are restored and watermarked components  $R_w$  and  $G_w$  are obtained.

## 2.2 Modification of 2D B-feature Histogram

After watermarked components  $R_w$  and  $G_w$  are constructed, we continued with the B component modification in second strategy, which is based on a 2D histogram composed by B component and features extracted from the image. To extract the features, the  $R_w$  component is used. This procedure is described as follows: 1) JPEG compression can be regarded as a low-pass filter. It eliminates major high-frequency components of an image. Some adaptive filters in [6] and [7] are designed to reduce effectively blocking artifacts of the JPEG image. The smoothing filter in (2) is

used and adopted in this strategy to reduce effectively the variability of the coefficients of  $R_w(x, y)$  in response to JPEG compression attacks with different quality factors,

$$\begin{aligned} \text{for all } x, y \text{ and } 0 \leq x \leq M-1, 0 \leq y \leq N-1 \\ \text{for all } \hat{x}, \hat{y}, \hat{x}^2 + \hat{y}^2 \leq r^2 \text{ and } 0 \leq x + \hat{x} \leq M-1, \\ 0 \leq y + \hat{y} \leq N-1 \\ R_f(x, y) = \sum_{\hat{x}} \sum_{\hat{y}} \frac{R_w(x + \hat{x}, y + \hat{y})}{N_r} \end{aligned} \quad (2)$$

where  $r$  denotes the radius of the set of pixels around  $(x, y)$ , and  $N_r$  represents the number of pixels within the circle. In this scheme,  $r$  is 12 and  $N_r$  is 452. After equation (2) is applied, the coefficients of  $R_f$  become more stable under JPEG attacks with various quality factors. 2) Divide the  $R_f$  and  $B$  components into  $p_i$  regions. The number of regions is given by  $L^2$ , where  $L$  indicates the watermark dimension, thus, i.e., if  $L = 16$ , then these components are divided in  $L^2$  ( $=16 \times 16$ ) regions. 3) For each  $p_i$  region, 2D histogram  $h_i$  is composed by  $R_f$  and  $B$  components, and each  $h_i$  is partitioned into four blocks called  $BA$ ,  $BB$ ,  $BC$  and  $BD$  respectively. The lowest, medium, highest values of  $B$  in  $h_i$  are got and denoted by  $B_l$ ,  $B_m$  and  $B_h$  respectively, which are used in the next step. 4) The  $i$ -th watermark bit is embedded into the histogram  $h_i$  of region  $p_i$ , modifying bin values of B components. Some bins are moved from one block to another, modifying the distribution of  $h_i$ , which indicates a specific watermark bit (0 or 1). For example, if  $W(j, k) = 1$ , some bins in  $BB$  and  $BC$  are moved into  $BA$  and  $BD$ , and if  $W(j, k) = 0$ , some pixels in  $BA$  and  $BD$  are moved into  $BB$  and  $BC$ , respectively. In this step, a gain factor  $\alpha$  ( $0 \leq \alpha \leq 1$ ) can be assigned, which controls watermark imperceptibility and robustness. This gain factor indicates the ratio between the number of bins that can be moved and total number of bins in  $h_i$ . The watermark signal is more robust when  $\alpha$  is increases, but some of the regions of the watermarked image may be distorted. Also two margin values are used to resist JPEG compression attack, then, we have two margin values  $B_l'$  and  $B_h'$ , as shown by (3) [4],

$$\begin{aligned} B_l' &= B_m - \beta(B_m - B_l) \\ B_h' &= B_m + \beta(B_h - B_m) \end{aligned} \quad (3)$$

where  $\beta$  is the variable that indicates the resistance to JPEG attack and its value must be  $0 \leq \beta \leq 1$ . If  $\beta > 1$  is used, the block artifact can be visible. This process changes only interior distribution of  $h_i$ , but global distribution of inter  $h_i$  ( $i = 1..L^2$ ) is not changed. Actually, mutual relationship between histogram  $h_{i1}$  and  $h_{i2}$  of two regions  $p_{i1}$  and  $p_{i2}$  is conserved. Consequently, the distribution of B component is modified, according to modification of each  $h_i$ . Because the modification of the B coefficients is controlled by the factors  $\alpha$  and  $\beta$ , watermark embedding dose not cause any degradation of the image quality. 4) Once each histogram  $h_i$

is modified to embed  $i$ th watermark sequence, the component  $B$  is restored to get the watermarked component  $B_w$ . Finally, the watermarked image  $I_w$  is constructed using three watermarked components  $R_w$ ,  $G_w$  and  $B_w$ .

### 3. DETECTION PROCESS

The watermark detection procedure is described as follows: 1) Obtain  $R_w$ ,  $G_w$ , and  $B_w$  components from the watermarked Image  $I_w$ . Calculate 2D R-G histogram  $H_{RG}$  and segment it into blocks of size  $L \times L$ . 2) Extract the region  $H_{r_w}$  from the  $H_{RG}$ . And reconstruct the watermark pattern  $W_1$  according to this conditions: if  $H_{r_w}(j,k) > 0$  then  $W_1(j,k) = 1$ , otherwise  $W_1(j,k) = 0$ . 3) Apply circular smooth filter to  $R_w$  component, and obtain filtered component  $R_{wf}$ . And segment the  $R_{wf}$  and  $B_w$  components into  $L^2$  regions  $p_i$ ,  $i=1 \dots L^2$ . Note that  $L^2$  is watermark length. 4) For each  $p_i$  region, 2D histogram  $h_i$  from  $R_{wf}$  and  $B_w$  components is constructed. 5) Partition each  $h_i$  into four blocks called  $BA$ ,  $BB$ ,  $BC$  and  $BD$ , respectively. 6) Count the number of bins in these four blocks, and according to the number,  $i$ -th watermark bit value is extracted. The condition for assignation is given by (4).

$$\text{if } N_{BA} + N_{BD} > N_{BB} + N_{BC} \quad \text{then } W_2(j,k) = 1 \\ \text{otherwise } W_2(j,k) = 0 \quad (4)$$

7) Once the two watermark patterns  $W_1$  and  $W_2$ , are extracted, the extracted final watermark patter  $\bar{W}$  is calculated by  $\bar{W} = (W_1 \vee W) \wedge (W_2 \vee W)$ , where  $W$  is original watermark sequence and notations  $\vee$ ,  $\wedge$  are bit-or and bit-and, respectively. 8) A threshold value  $T$  must be defined to determine if the watermark is present or not into the image. Hence, if the number of correct extracted bits exceeds  $T$ , the watermark sequence is extracted correctly from the image. The false alarm probability  $P_{fa}$  for  $n$  bits embedded watermark data is given by (5) [5], and the value  $T$  must be controlled in order that  $P_{fa}$  is smaller than a predetermined value.

$$P_{fa} = \sum_{i=T}^n \left(\frac{1}{2}\right)^n \cdot \left(\frac{n!}{i!(n-i)!}\right) \quad (5)$$

where  $n$  is the total number of watermark data bits.

### 4. EXPERIMENTAL RESULTS

In this section, we show the results after applying the embedding and detection procedures to a set of ten test images. In the experiments, we use color images of size  $512 \times 512$ . The parameters used to embed 256 bits watermark data are  $L = 16$ ,  $r = 12$ ,  $Nr = 452$ ,  $\alpha = 0.6$ ,  $\beta = 0.5$ , and  $T =$

179 with  $P_{fa} = 10^{-07}$ . Table 1 shows that the average number of correct bits extracted from a watermarked and un-watermarked test images, which are attacked by most common geometrical distortions, common signal processing, and combined attacks, respectively. The experimental results show the watermark robustness of the proposed method against these attacks. Also, a performance comparison between the proposed method and previous works, such as the color histogram method proposed by [3], the histogram oriented watermarking algorithm proposed by [4], the invariant domain scheme developed by [9], the template-based scheme proposed by [8], the feature-based scheme proposed by [5] and the image normalization based scheme proposed by [10]. This comparison includes JPEG compression, scaling, cropping, aspect ratio change, rotation, shearing, Gaussian noise, and median filtering. Table 2 shows the performance comparisons together with watermark detection methods (blind or original image is required) and the watermark data length associated with each scheme. These results show better performance of the proposed method compared with prior methods against most common geometric and signal processing attacks. In Fig 1, shows the original and watermarked version of Lena image after apply this watermarking scheme.

Table 1  
Number of average correct bits extracted from a watermarked image and un-watermarked image with 256 bits embedded.

Attack	Correct Bits
Compression JPEG QF = 30	205 / 117
Median filter 4x 4	239 / 115
Impulsive Noise, density = 0.01	238 / 118
Gaussian Noise, M = 0, $\sigma = 0.01$	237 / 115
Sharpening 3 x 3	201 / 119
Rotation by 55°	249 / 114
Cropping 40 %	235 / 118
Scale 0.75	233 / 116
Affine Transformation	242 / 112
Aspect ratio (1.0, 1.2)	247 / 115
JPEG 70 + Rotation 15 °	219 / 120
JPEG 70 + Cropping 10 %	212 / 118
JPEG 70 + median filter 3 x 3	220 / 116
JPEG 70 + Flipping horizontal and vertical.	231 / 117

$N_1/N_2$ :  $N_1$  and  $N_2$  indicate the number of correct bits extracted from a watermarked and an un-watermarked image, respectively



Fig. 1. Original (a) and watermarked version (b) of Lena image.

Table 2  
Performance Comparison

Comparison	Zheng <i>et al.</i> [9] (Invariant Domain Based)	Kang <i>et al.</i> [8] (Template Based)	Tang and Hang [5] (Feature Based)	Roy <i>et al.</i> [3] (Histogram Based)	C.H. Lin <i>et al.</i> [4] (Histogram Based)	M. Cedillo <i>et al.</i> [10] (image normalization based)	Proposed method (Histogram Based)
JPEG (QF)	10-100	10-100	40-100	50-100	20-100	20-100	30-100
Scaling	0.6-1.3	detected	-	1.2 – 1.4	0.75 – 1.5	0.4-2	0.2 – 1.8
Cropping	detected	Up-65%	Up to 10%	Up to 60%	Up to 15%	-	Up to 55%
Aspect Ratio	-	detected	-	-	detected	detected	detected
Rotation (with Auto-Crop and Scale)	0°-360°	detected	1°-5°	0° - 40°	1° - 15°	detected	0° - 360°
Shearing	10 columns or 10 rows	X5% Y5%	X1% Y1%	-	X5% Y5%	X5% Y5%	X5% Y5%
Median Filtering	detected	-	2x2	-	4x4	3x3	4x4
Gaussian Noise	detected	-	detected	detected	-	detected	detected
Original Image for detection	need or exhaustive search	blind	blind	blind	blind	blind	blind
Watermark length	64 bits	60 bits	16 bits	256 bits	128 bits	64 bits	256 bits

## 5. CONCLUSIONS

In this paper we proposed a robust watermarking method against geometric distortions and common signal processing attacks, which is based on two modifications of bi-dimensional histograms. In the first one, a 2D histogram is constructed by  $R$  and  $G$  components, in which an adequate region is selected and bin values within the region is modified according to binary watermark pattern. In second modification, another 2D histogram is constructed by  $B$  component and image features. This is dynamically partitioned to several blocks; each of them is used to embed the watermark sequence by modifying its distribution. The experimental results show a better performance compared with the prior methods against most common geometric and signal processing attacks, such as aspect ratio, rotation, cropping, scaling, median filtering and Gaussian noise.

## 6. REFERENCES

- [1] Coltuc, D., and Bolon, Ph.: "Robust watermarking by histogram specification". 6th IEEE Conf. on Image Processing (ICIP'99), Kobe, Japan, vol. 2, pp. 236–239, October 1999.
- [2] Chareyron, G., Macq, B., and Tremeau, A.: "Watermarking of color images based on segmentation of the XYZ color space". CGIV 2004 – Second Eur. Conf. on Color in Graphics, Imaging and Vision, Aachen, Germany, pp. 178-182. April 2004.
- [3] Roy, S., and Chang, E.C.: "Watermarking color histogram". Proc IEEE Int. Conf. on Image Processing, Singapore, 2004.
- [4] C.H. Lin, D.Y. Chan, H. Su and W.S. Hsieh, "Histogram Oriented watermarking Algorithm: colour image watermarking scheme robust against geometric attacks and signal processing". IEE Proc.-Vis. Image Signal Process., Vol. 153, No. 4, pp. 483-492, 2006.
- [5] C. Tang and H. M. Hang, "A Feature-Based Robust Digital Image Watermarking Scheme", IEEE Trans on Signal Processing, vol. 51, no. 4, 2003, pp. 950-959.
- [6] Lee, Y.L., Kim, H.C., and Park, H.W.: "Blocking effect reduction of JPEG images by signal adaptive filtering". IEEE Trans. Image Process., 7, (2), pp. 229-234, 1998.
- [7] Pham, T.Q., and van Vliet, L.J.: "Blocking artifacts removal by a hybrid filter method", ASCI 2005 Proc. Of the eleventh annual conf. of the Advanced School for Computing and Imaging, ASCI Delft. Heijden, the Netherlands, pp. 372-377, 8-10 June 2005.
- [8] Kang, X., Huang, J., Shi, Y. Q., and Lin, Y.: "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression", IEEE Trans. Circuits Syst. Video Technol., 13, (8), pp. 776-786, 2003.
- [9] Zheng, D., Zhao, J., and El Saddik, A.: "RST-invariant digital image watermarking based on log-polar mapping and phase correlation", IEEE Trans. Circuits Syst. Video Technol., 13, (8), pp. 753-765, 2003.
- [10] M. Cedillo, M. Nakano and H. Perez, "Robust watermarking to geometric distortion based on image normalization and texture classification", in Proc IEEE Midwest Symposium CAS 2008, Knoxville, Tennessee, pp. 245-248.

# 2008 IEEE International 51st Midwest Symposium on Circuits and Systems

August 10-13, 2008, Knoxville, Tennessee

[Welcome](#)

[Events](#)

[Committees](#)

[Copyright](#)

[Table of Contents](#)

[Author Index](#)

[Search](#)

[Help](#)



Photo credit: Tennessee Department of Tourist Development

©2008 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from IEEE.

CD-ROM support, contact The Printing House, Inc. at +1-608-873-4500. For more information, please see the "Copyright" page.



Circuits and  
System Society



Catalog Number: CFP08MID-USB  
ISBN: 978-1-4244-2167-1  
ISSN: 1548-3746

## **WELCOME to the 51<sup>st</sup> IEEE INTERNATIONAL MIDWEST SYMPOSIUM ON CIRCUITS AND SYSTEMS**

It is our pleasure to welcome you to Knoxville, Tennessee, the 2008 site of MWSCAS which is the longest-running symposium sponsored by the IEEE Circuits and Systems Society. Throughout its history, it has provided a forum for researchers and educators to share their enthusiasm and results in the Circuits and Systems area.

This year we received 362 submissions. We have chosen 248, from 28 countries, for 202 lecture and 44 poster presentations. We have also selected the 10 most outstanding student papers for special presentations in the Student Paper Contest. In addition, we have three keynote addresses to be presented by experts in their fields. Tours of the University of Tennessee and the Oak Ridge National Laboratory have been organized.

This year's Symposium focuses on the latest trends in circuits and systems research and the increasing impetus towards multi-disciplinary research, especially in electronics, biology and chemistry. The Symposium features sessions on trends in developing nanoscale devices and in new technologies for circuits and systems.

Along with the strong technical sessions, we hope you will enjoy the many cultural and recreational activities in the Knoxville and Great Smoky Mountain National Park area. In particular, we invite you to join us for the a special MWSCAS social event on Tuesday evening which will be held at the International Women's Basketball Hall of Fame. Participants will not only enjoy good food and music but will also be able to see the exhibits and even play a little basketball.



**Itamar Elhanany**  
**Co-General Chair**



**Don Bouldin**  
**Co-General Chair**



**Greg Peterson**  
**Technical Program Chair**

## Session: A3L-C Circuits for Digital Systems

<b>An Extended Library of Hardware Modules for Genetic Algorithms, with Applications to DNA Sequence Matching</b> .....	209
<i>Harish Ramaswamy, University of Cincinnati; Carla Purdy, University of Cincinnati</i>	
<b>Bus Encoding Schemes using Positive Correlated Switchings in Subbuses: A Comparison</b> .....	213
<i>Srinivasa Vemuru, Ohio Northern University; Ahmed Elkammar, City University of New York; Norman Scheinberg, City University of New York</i>	
<b>A SiGe BiCMOS Instrumentation Channel for Extreme Environment Applications</b> .....	217
<i>C. Ulaganathan, University of Tennessee; N. Nambiar, University of Tennessee; B. Prothro, University of Tennessee; R. Greenwell, University of Tennessee; S. Chen, University of Tennessee; B.J. Blalock, University of Tennessee; C.L. Britton Jr., University of Tennessee; M.N. Ericson, University of Tennessee; J.D. Cressler, Georgia Institute of Technology; H. Hoang, University of Arkansas; R. Broughton, University of Arkansas; K. Cornett, University of Arkansas; G. Fu, University of Arkansas; H.A. Mantooh, University of Arkansas; R.W. Berger, BAE Systems</i>	

## Session: A3L-D Architectures for Signal Processing

<b>An Efficient Architecture of RNS based Wallace Tree Multiplier for DSP Applications</b> .....	221
<i>Partha Pratim Kundu, West Bengal University of Technology; Oishila Bandyopadhyay, West Bengal University of Technology; Amitabha Sinha, West Bengal University of Technology</i>	
<b>An Advanced Recursive Algorithm for Low-Cost Implementation of Matrix Multipliers</b> .....	225
<i>Vijay Sundaram, National Institute of Technology, Tiruchirapalli</i>	
<b>Flexible Decoder Architectures for Irregular QC-LDPC Codes</b> .....	229
<i>Tzu-Chieh Kuo, University of California, Los Angeles; Alan N. Willson Jr., University of California, Los Angeles</i>	
<b>A Reusable Distributed Arithmetic Architecture for FIR Filtering</b> .....	233
<i>Haw-Jing Lo, Georgia Institute of Technology; Heejong Yoo, Georgia Institute of Technology; David V. Anderson, Georgia Institute of Technology</i>	

## Session: A3L-E Image Processing

<b>Parallel Structure System Employing PCA and VQ in the Transform Domain for Facial Recognition</b> .....	237
<i>Moataz M. Abdelwahab, University of Central Florida; Wasfy B. Mikhael, University of Central Florida</i>	
<b>Shape Adaptive Three Dimensional Cone Filter Bank</b> .....	241
<i>Santosh Singh, Siemens Information Systems Ltd.; Mehmet Celenk, Ohio University</i>	
<b>Robust Watermarking to Geometric Distortion based on Image Normalization and Texture Classification</b> .....	245
<i>Manuel Cedillo-Hernández, National Polytechnic Institute; Mariko Nakano-Miyatake, National Polytechnic Institute; Hector Perez-Meana, National Polytechnic Institute</i>	

# Robust Watermarking to Geometric Distortion Based on Image Normalization and Texture Classification

Manuel Cedillo-Hernández, Mariko Nakano-Miyatake, Hector Perez-Meana  
Postgraduate and Research Section of ESIME Culhuacan  
National Polytechnic Institute  
Mexico City, Mexico  
hmpm@prodigy.net.mx

**Abstract**—In this paper, we present a robust watermarking method against geometric distortions and several attacks of signal processing. In the proposed watermarking method, image normalization is used to get geometric invariant feature and watermark embedding and detection are carried out in the Discrete Cosine Transform (DCT) domain. Texture based image block classification in DCT domain is also used to get major watermark imperceptibility. The proposed watermarking scheme is a public watermarking, where the original image is not available in the watermark detection stage. The experimental results show the watermark imperceptibility and robustness against geometric distortion such as rotation, scaling and various other Affine Transformation, and common signal processing attacks, such as JPEG compression and noise contamination. Also the comparison with the prior methods shows better performance of the proposed method.

## I. INTRODUCTION

In the public watermarking scheme, the loss of the synchronization, between watermark embedding and detection stages, causes watermark detection error. Geometric distortions, such as rotation, scaling, translation and any Affine Transformation, are principal factors of this problem, however this type of distortion is common in practice. In the literature, several approaches have been proposed to combat the geometric attacks, which can be classified basically into five approaches. The first approach uses exhaustive search in the watermark detection stage, even if the effectiveness to estimate geometric factors is superior to other approaches [1], considerable high computational complexity makes this method impractical. In the second approach, watermark signal is embedded in a geometrically invariant domain, such as Fourier-Mellin transform (FMT) [2]. This approach is effective in theory, but difficult to implement, due to Log Polar Mapping and its inverse operation. In the third approach, together with watermark signal, template signal is embedded to use resynchronization [3]. A principal disadvantage of this approach is difficulty in keeping good quality of the watermarked image, because the template signal must be embedded additionally into the image. The fourth approach is a features based approach [4, 5], in which salient features of the image are used for resynchronization, this approach

doesn't embed additional signal into the image, however generally high computational complexity is required to extract salient feature in both (embedding and detection) stages. In the fifth approach, watermark signal is embedded into the normalized image generated by invariant moment factors introduced by [6]. Applying inverse normalization operation to normalized watermarked image, watermarked image is got. This approach is efficient theoretically, but discrete implementation causes quality degradation of the image, due to interpolation process. In [7], a multibits watermarking scheme based on image normalization is proposed, in which to avoid a quality degradation of the watermarked image, a watermark signal is normalized and embedded into the original version of the image. In this method, watermark is robust to almost geometric distortions, however to get acceptable lower Bit Error Rate (BER) of the extracted watermark sequence, watermark imperceptibility must be sacrificed.

In this paper, we propose a watermarking approach based on the image normalization, in which watermark embedding and detection are performed in the DCT domain. The proposed scheme is different from the scheme proposed by [7] in the following points: a) In the proposed scheme, image block is classified in DCT domain, using texture feature of each block, to determine adequate embedding energy for the watermark imperceptibility. b) Robustness of the proposed scheme is evaluated using more kinds of attacks, including impulsive and Gaussian noise.

## II. PROPOSED SCHEME

### A. Image Normalization

The normalization procedure of a image  $f(x,y)$  consists of the following steps:

1) Center the image  $f(x,y)$ , through the Affine Transformation as given by:

$$\begin{pmatrix} x_a \\ y_a \end{pmatrix} = A \cdot \begin{pmatrix} x \\ y \end{pmatrix} - d \quad (1)$$

where matrix  $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  and the vector  $d = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$  with

$$d_1 = \frac{m_{10}}{m_{00}}, d_2 = \frac{m_{01}}{m_{00}} \quad (2)$$

where  $m_{10}, m_{01}$  and  $m_{00}$ , are the moments of  $f(x,y)$ , and  $d_1, d_2$  are the central moments of  $f(x,y)$  [6]. This step eliminates the translation effect by assigning the center of the normalized image at the density center of the image. The resulting centered image is denoted as  $f_1(x,y)$ .

2) Apply a shearing transform to  $f_1(x,y)$  in the  $x$ -direction using the matrix  $A_x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ . The resulting image is denoted by  $f_2(x,y)$ . This step eliminates shearing effect in the  $x$ -direction.

3) Apply a shearing transform to  $f_2(x,y)$  in the  $y$ -direction using the matrix  $A_y = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$ . The resulting image is denoted by  $f_3(x,y)$ . This step eliminates shearing effect in the  $y$ -direction.

4) Scale  $f_3(x,y)$  in both  $x$  and  $y$  directions with the matrix  $A_s = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$  and the resulting image is denoted by  $f_4(x,y)$ .

This step eliminates the scaling effect by forcing the normalized image to a standard size.

The final image  $f_4(x,y)$  is the normalized image. It is important to denote that each step in the normalization procedure is invertible; this will allow us to convert the normalized image back to its original version.

The determination of transformation parameters  $\beta, \gamma, \alpha$  and  $\delta$ , associated with the transforms  $A_x, A_y$ , and  $A_s$  are shown in detail in the paper presented by [7]. In the figure 1, an example of the original image, the image suffered an Affine distortion and the normalized version of both images are shown.

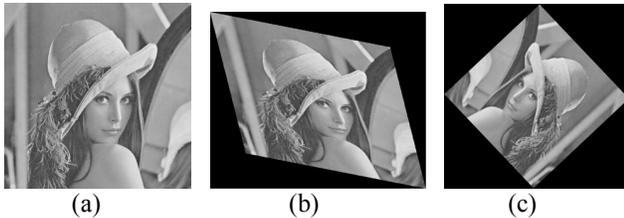


Figure 1. (a) Original image Lena. (b) Lena image (a) with affine distortion. (c) Normalized version from (a) and (b).

### B. Embedding Process

The watermark generation and embedding process are described as follows:

1) Apply the normalization procedure to the original image to get the normalized image.

2) Divide the normalized image in blocks of 8x8 pixels and select the blocks with strong texture. To estimate the texture complexity, we use the technique proposed by [8]. Firstly DCT coefficients of each block are quantized using the same method as that used in JPEG. If the  $k$ -th block  $F_k(u,v), 0 \leq u,v \leq 7$  satisfies the following condition, this block is classified as strong texture block; otherwise the block is weak texture.

$$\text{if } F_k(0,0) > T_1 \text{ and } \text{number}\{\lfloor F_k(u,v)/Q(u,v) \rfloor \neq 0\} > T_2$$

Where, the notation  $\lfloor \bullet \rfloor$  is integer floor function, the function  $\text{number}\{\text{condition}\}$  gets number of elements satisfied the *condition* and  $Q(u,v)$  is the value of quantification matrix at spatial frequency  $(u,v)$ .  $T_1$  and  $T_2$  are two predefined thresholds. An example of classification of blocks is shown by fig.2, (a) shows normalized image and (b) shows block classification, where white blocks are strong texture blocks.

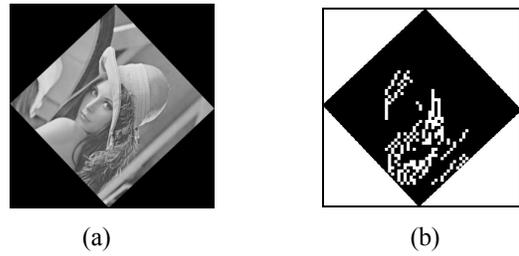


Figure 2. An example of classification of blocks by texture characteristics. (a) Normalized image (b) blocks classification.

3) Generate the 2-D pseudo-random pattern  $R$  of the same size of original image with any key, because this pattern is only used as the support of the watermark vector.

4) Generate a watermark vector  $W = [w_1, w_2, \dots, w_n]$  using a user's secret key, where  $w_i = \{1, -1\}, i=1..n$ .

5) Create a mask image  $M$ , which is a binary image, taking 1s within normalized image area and 0s elsewhere, to generate masked pseudo-random pattern  $MR$  with same scale and rotation factors as that of the normalized image.

6) Watermark vector  $W$  is multiplied by a gain factor  $\alpha_1$ .

7) Divide the watermark vector  $W$  into  $N$  groups of  $L$  elements, where  $L$  must be one number from 1 to 22 (number of coefficients that compose the middle frequency range in DCT domain), thus, for example, if  $L = 5$  and size of  $W$  is 500, the number of groups  $N = 500 / 5 = 100$ .

8) The coefficients in middle frequency range of each strong texture block are replaced with  $L$  elements of each group of watermark sequence. Then apply the IDCT to each watermarked block to get watermarked pattern  $MR_W$ .

9) Apply the inverse normalization to the watermarked pattern  $MR_W$  to get watermarked pattern  $WP$  with same size as the cover image.

10)  $WP$  is embedded into the original image additively with a gain factor  $\alpha_2$ . This produces the watermark image.

$$I_w = I_o + (WP \cdot \alpha_2) \quad (3)$$

where  $I_o$  and  $I_w$  are original and watermarked image, and  $WP$  is watermark pattern generated by step 9.

The whole procedure is equivalent to embedding the watermark into the DCT domain of the normalized image. The blocks with strong texture allow embedding strong watermark without causing any visual distortion to watermarked image. The figure 3 shows the watermark generation and embedding procedures.

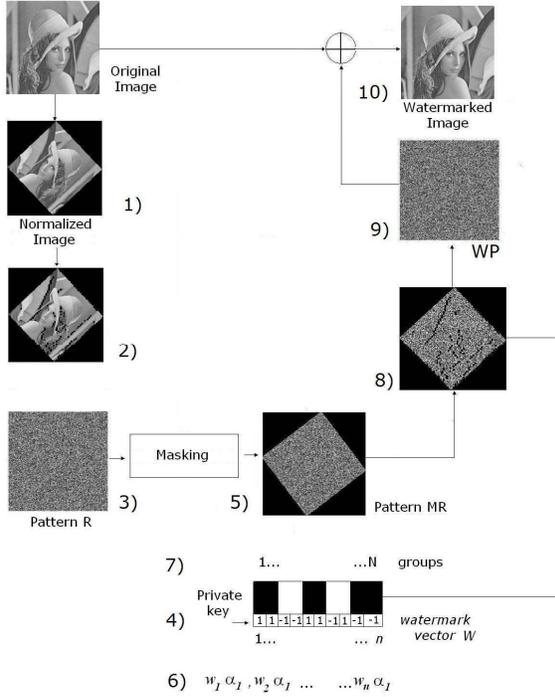


Figure 3. Watermark Generation and embedding procedure.

### C. Watermark Extraction

The process of the watermark detection is:

1) Apply the normalization procedure to watermarked image to get the normalized watermarked image.

2) Apply the DCT to each block of the normalized watermarked image, the middle range of the DCT coefficients  $CW$  of strong texture block are extracted. Extract the watermark vector  $\hat{W}$  is formed by (4)

$$\hat{W} = [w_1, w_2, \dots, w_{N-1}, w_N] \quad (4)$$

$$w_k = \text{sign}(CW_k)$$

where  $w_k$  is extracted watermark sequence (L bits) from k-th strong texture block and  $\text{sign}$  is a sign function.

## III. EXPERIMENTAL RESULTS

In the computer simulations, 8 bits grayscale images of size 512x512 were used, and two threshold values  $T_1, T_2$ , to classify blocks into two categories: strong texture and weak texture, are set 230 and 15, respectively. The proposed scheme is evaluated from the watermark imperceptibility and robustness points of view.

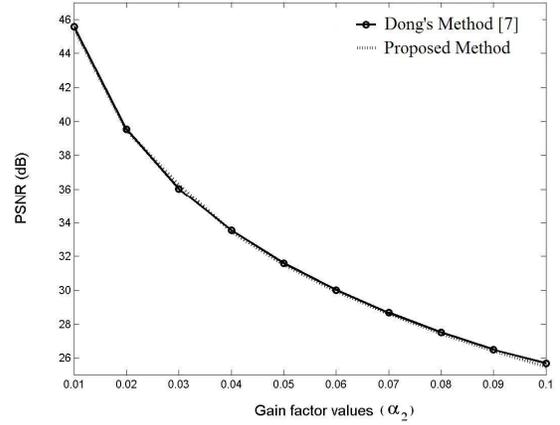


Figure 4. Peak Signal to Noise Ratio (PSNR) of both methods.

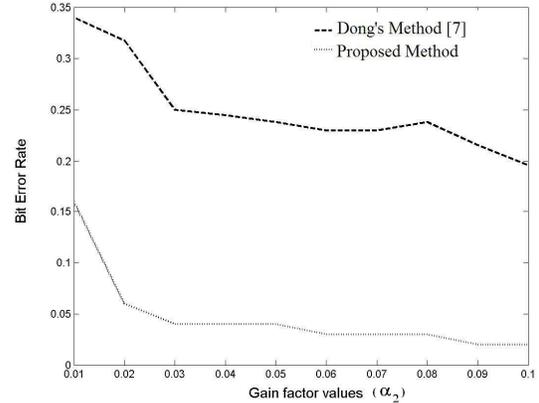


Figure 5. BER of both methods without any attack.

### A. Watermark Imperceptibility

A 50-bit binary watermark vector was embedded redundantly 10 times into the images. The gain factors  $\alpha_2$  are increased from 0.01 to 0.1. The bit-error-rate (BER) of the extracted watermark bit sequence (respect to the embedded one and the peak signal to noise ratio (PSNR) between the original image and the watermarked one were then computed over the test images. Fig. 4 and 5 shown the PSNR and BER calculated using Dong's method [7] and our proposed method respectively, watermark generation gain factor  $\alpha_1$  is set to 6 in all cases. From fig. 4, watermark imperceptibility is very similar between both methods when same embedding gain factor  $\alpha_2$  is used. However, fig. 5 shows that the BER of extracted watermark sequence using our proposed method is smaller than 0.05 when gain factor  $\alpha_2$  is bigger than 0.03, while Dong's method shows much higher BER than our

proposed method. When watermark signal has some meaningful data, such as message and logotype, the proposed system can extract the watermark in totally legible manner, while extracted watermark by Dong's method will be illegible because more than 20% of bits are changed in all evaluated range of  $\alpha_2$ .

### B. Watermark Robustness

To evaluate watermark robustness in the proposed scheme, several attacks are applied to the watermarked images. Table I shows watermark robustness in the terms of BER of extracted watermark.

TABLE I. BER OF EXTRACTED WATERMARK AFTER ATTACKS

Attacks	BER
Without Attack	0.04
Gaussian Noise with mean=0, variance $\sigma=0.01$	0.09
Impulsive Noise with density 0.09	0.06
Median Filter with window's size 3x3	0.11
JPEG Compression with quality factor QF=50	0.06
JPEG Compression with quality factor QF=25	0.14
Rotation with 75° degrees	0.06
Remove lines with StirMark RML=50.	0.09
Scaling with scaling factor=1.4	0.08
Affine Transformation with matrix $A = \begin{bmatrix} -1.01 & 0.2 \\ 0.2 & 0.8 \end{bmatrix}$	0.08
Shearing with factor (0,7%)	0.06
Aspect ratio change (1.2,1.0)	0.06

From table I we can observe that the embedded watermark signal is sufficiently robust to geometrical distortions and common signal processing.

TABLE II. BER OF EXTRACTED WATERMARK IN DONG'S, DUGELAY'S AND PROPOSED METHODS WITH 64 BITS OF INFORMATION

Dong's Method [7]	Dugelay's Method [9]	Proposed Method
BER = 0.25	BER = 0.05	BER = 0.04

Table II shows a comparison of BER of the extracted watermark sequence, between the proposed method, Dong's method [7] and Dugelay's method [9]. In all method, 64 bits watermark sequence is embedded under the similar conditions: same image, similar PSNR of watermarked image, without attack. From table II, we can observe that the proposed method is slightly better than the Dugelay's method [9], but much better than the Dong's method [7].

## IV. CONCLUSIONS

In this paper we proposed a robust watermarking algorithm to geometrical distortion such as rotation, scaling, translation and general Affine Transformation. In the watermark embedding and detection stage, image normalization process is employed to generate an invariant watermark pattern to the geometric distortion. Also the proposed algorithm classifies DCT blocks, using texture feature, into the strong texture blocks and weak texture blocks, and watermark signal is embedded into only strong texture blocks. Using this image adaptive embedding method, a stronger watermark signal can be embedded in an imperceptible manner. The simulation results show watermark imperceptibility and robustness to various geometrical attacks and common signal processing such as JPEG compression, filtering operation and noise contamination, etc. The performance of the proposed algorithm is compared with basically Dong's algorithm [7] from watermark imperceptibility and robustness point of view. Comparison results show that the proposed algorithm can extract the watermark bit sequence with very low bit error rates, while keeping sufficiently high imperceptibility of the watermark signal.

### ACKNOWLEDGMENT

The authors thank The National Science and Technology Council (CONACyT) of Mexico and to the National Polytechnic Institute of Mexico for the financial supports during realization of this research.

### REFERENCES

- [1] M. Barni, "Effectiveness of exhaustive search and template matching against watermark desynchronization", IEEE Trans. on Signal Processing Letter, vol. 12, no. 2, 2005, pp. 158-161.
- [2] J. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking", in Proc. ICIP' 97, Atlanta, vol. 1, 1997, pp. 536-539.
- [3] S. Pereira, and T. Pun, "Robust template matching for affine resistant image watermarks", IEEE Trans. on Image Processing, vol. 9, no. 6, 2000, pp. 1123-1129.
- [4] E. Izquierdo, "Using Invariant Image Features for Synchronization", Eurasip Journal on Applied Signal Processing, vol. 2, 2002, pp. 410-417.
- [5] C. Tang and H. M. hang, "A Feature-Based Robust Digital Image Watermarking Scheme", IEEE Trans on Signal Processing, vol. 51, no. 4, 2003, pp. 950-959.
- [6] M. K. Hu, "Visual Pattern Recognition by Moment Invariants", IRE Trans. on Information Theory, vol. 8, 1962, pp. 179-187.
- [7] P. Dong, J. B. Brankov, N. P. Galatsanos, Y. Yang and F. Davoine, "Digital Watermarking robust to geometric distortions.", IEEE Trans. on Image Processing, vol. 14, no. 12, 2005, pp. 2140-2150.
- [8] J. Huang and Y. Q. Shi, "Adaptive image watermarking scheme based on visual masking", IEEE Electronics Letter, 1998, pp. 748-750.
- [9] J.L. Dugelay, S. Roche, C. Rey and G. Doërr, "Still-Image Watermarking Robust to Local Geometric Distortions", IEEE Trans. on Image Processing, vol. 15, no. 9, 2006, pp. 2831-2842.



Access this document

Full Text: PDF (903 KB)

Download this citation

Choose Citation

Download ASCII Text



Learn More

Rights and Permissions

Learn More

## Robust watermarking to geometric distortion based on image normalization and texture classification

Cedillo, M.H. Nakano, M.M. Perez, H.M.

Postgrad. & Res. Sect. of ESIME Culhuacan, Nat. Polytech. Inst., Mexico City;

This paper appears in: [Circuits and Systems, 2008. MWSCAS 2008. 51st Midwest Symposium on](#)

Publication Date: 10-13 Aug. 2008

On page(s): 245-248

ISSN: 1548-3746

ISBN: 978-1-4244-2166-4

INSPEC Accession Number: 10203278

Digital Object Identifier: 10.1109/MWSCAS.2008.4616782

Current Version Published: 2008-09-03

### Abstract

In this paper, we present a robust watermarking method against geometric distortions and several attacks of signal processing. In the proposed watermarking method, image normalization is used to get geometric invariant feature and watermark embedding and detection are carried out in the Discrete Cosine Transform (DCT) domain. Texture based image block classification in DCT domain is also used to get major watermark imperceptibility. The proposed watermarking scheme is a public watermarking, where the original image is not available in the watermark detection stage. The experimental results show the watermark imperceptibility and robustness against geometric distortion such as rotation, scaling and various other Affine Transformation, and common signal processing attacks, such as JPEG compression and noise contamination. Also the comparison with the prior methods shows better performance of the proposed method.

### Index Terms

#### Inspe

##### Controlled Indexing

[discrete cosine transforms](#) [image classification](#) [image coding](#) [image texture watermarking](#)

##### Non-controlled Indexing

[JPEG compression](#) [affine transformation](#) [discrete cosine transform domain](#) [geometric distortion](#) [image normalization](#) [noise contamination](#) [robust watermarking](#) [signal processing attacks](#) [texture based image block classification](#) [texture classification](#) [watermark detection](#) [watermark embedding](#)

#### Author Keywords

Not Available

#### Medical Subject Heading (MeSH Terms)

Not Available

### References

No references available on IEEE Xplore.

### Citing Documents

No citing documents available on IEEE Xplore.



## Robust Image Watermarking Using Feature Points and Image Normalization

Wei Na, Kazuhiko Yamaguchi  
Dept. of Information Communication Engineering  
The University of Electro-Communications  
Chofu-shi, Tokyo, Japan.  
yama@ice.uec.ac.jp

Manuel Cedillo-Hernández, Mariko Nakano-  
Miyatake, Héctor Pérez-Meana  
Postgraduate and Research Section of ESIME  
Culhuacan. National Polytechnic Institute. Mexico.  
mcedillohdz@hotmail.com, mnakano@ipn.mx,  
hmperez@ipn.mx

*Abstract— In this paper we present a robust image watermarking method against geometric distortions and several attacks of signal processing. Initially, the original image is normalized and the feature points are then extracted. Furthermore, the locally most stable feature points are obtained and used to generate several non-overlapped circular regions. Texture-based image block classification in Discrete Cosine Transform (DCT) domain is also used to get watermark imperceptibility. The watermark is embedded and extracted into classified regions using the DCT domain. In the detector stage, the watermark can be obtained without the original image. The experimental results show the watermark robustness against geometric distortion such as rotation, scaling and various other Affine Transformation, and common signal processing attacks, such as JPEG compression and noise contamination.*

*Keywords: Image watermarking, geometric attacks, feature points, image normalization, texture classification.*

### I. INTRODUCTION

In public watermarking schemes, the synchronization loss, between the watermark embedding and detection stages, causes watermark detection error. Geometric distortions, such as rotation, scaling, translation and any Affine transformation, which are common in practice, are the principal factors of this problem. During the last two decades, numerous watermarking methods have been proposed that show robustness against common signal processing such as: JPEG compression and filtering etc., however relatively few of these methods addressed the robustness to the geometric distortions [1-11]. The watermarking methods that have been proposed to combat the geometric attacks can be classified basically into five approaches. The first one uses exhaustive search in the watermark detection stage, although the effectiveness to estimate geometric factors is superior to other approaches [1], considerable high computational complexity limits the application of this method in many practical situations. In the second one, the watermark signal is embedded in a geometrically invariant domain, such as Log Polar Mapping, Fourier-Mellin Transform domain, etc [2], [3]. This approach is effective, in theory, although it is difficult to implement without noticeable distortion due to the Log Polar Mapping and its inverse operation. In the third one, together with the watermark, a template signal is embedded to use for resynchronization [4]. The principal disadvantage

of this approach is the difficulty in keeping good quality of the watermarked image, because the template signal must be embedded additionally into the image. In the fourth approach, to embed the watermark signal, a normalized image is generated using the invariant moment factors introduced in [5]. Then the inverse normalization operation is applied to get the watermarked image. This approach is theoretically efficient, but its discrete implementation causes image quality degradation, due to the interpolation process. In [6], a multi-bits watermarking scheme based on image normalization is proposed, in which to avoid a quality degradation of the watermarked image, a watermark signal is normalized and embedded into the original version of the image. In this method, the watermark is robust to almost all geometric distortions, however to get acceptable a low Bit Error Rate (BER) of the extracted watermark sequence, watermark imperceptibility must be sacrificed. In [7], a watermarking method based on image normalization and texture classification is proposed, in which firstly image normalization is used to get geometric invariant features, next the watermark embedding and detection are carried out in the Discrete Cosine transform (DCT) domain. In this approach, watermark imperceptibility is improved using a texture-based block classification in DCT domain. This method is robust to almost all geometric attacks, except to cropping attack, which is a common problem for the image normalization-based watermarking algorithms.

The last one is the feature-based method, in which salient image features are used for resynchronization, without embedding any additional signal into the image. The methods of this category are called the second generation. The concept of second generation watermarking was firstly reported in [8]. The key idea is that the watermark information is associated with image features, which is invariant under geometric attacks. In [9] a feature-based image watermarking scheme is presented. They extracted feature points to construct a triangular tessellation and embedded the watermark in the spatial domain. In the detection stage, the scheme extracts the feature points from the possibly attacked watermarked image. Using these feature points, the original tessellation is reconstructed and the watermark is detected by correlation operation. This scheme can resist small rotation and scaling. However, because they extract many feature points and some of them

are not stable enough. As a result, the sets of triangles during watermark embedding and extraction are different. In [10], a robust image watermarking scheme using feature points is proposed. They used the Mexican Hat wavelet scale interaction to extract the feature points. Local patches are generated based on the feature points. A 16-bit long watermark is embedded into the blocks in discrete Fourier transform (DFT) domain. The watermark can resist rotation and cropping. However, it cannot resist scaling. Besides, rotation robustness is achieved only when rotation angles are smaller than 5 degree. In [11], a robust image watermarking scheme to resist rotation, scaling, and translation (RST) is presented. In the scheme, watermark is embedded into local regions of the image. These regions are extracted using Harris feature points. To resist the scaling attacks, the original image is normalized in scale before feature extraction. Locally most stable points are then used to generate several non-overlapped circular regions. The rotation normalization is carried out to generate the invariant regions, and the watermark bits are embedded into the invariant regions in DCT domain. This method can efficiently resist some signal processing attacks, RST attacks, as well as some combined attacks. However, rotation robustness is achieved only when rotation angles are smaller than 30 degree and it cannot be robust against other geometric attacks such as any affine transformation.

In this paper we present a robust image watermarking method against geometric distortions and several attacks of signal processing. Initially, the original image is normalized and the feature points are then extracted. Furthermore, the locally most stable feature points are obtained and used to generate several non-overlapped circular regions. Texture-based image block classification in DCT domain is also used to get major watermark imperceptibility. The watermark is embedded and extracted into these classified regions in the DCT domain. In the detection stage, the watermark can be obtained without the original image. The experimental results show the watermark robustness against geometric distortion such as rotation, scaling and various other Affine Transformation, and common signal processing attacks, such as JPEG compression and noise contamination. The proposed scheme is different from the scheme proposed by [11] in the following points: a) In the proposed scheme, image block is classified in DCT domain, using texture feature of each block, to determine adequate embedding energy for the watermark imperceptibility. b) Unlike [11], in which normalization in scale and rotation is used, the proposed scheme use global normalization to get robustness against wider range of geometric distortion, such as any affine transformation.

## II. PROPOSED METHOD

### A. Harris corner detector

The Harris corner detector [12] detects the feature points from the second-moment matrix  $M$  of the original image  $f(x,y)$ , which is given by (1):

$$M = \begin{bmatrix} A & C \\ C & B \end{bmatrix} = \begin{bmatrix} \left( \frac{\partial f(x,y)}{\partial x} \right)^2 * \omega & \left( \frac{\partial f(x,y)}{\partial x} \right) \left( \frac{\partial f(x,y)}{\partial y} \right) * \omega \\ \left( \frac{\partial f(x,y)}{\partial x} \right) \left( \frac{\partial f(x,y)}{\partial y} \right) * \omega & \left( \frac{\partial f(x,y)}{\partial y} \right)^2 * \omega \end{bmatrix} \quad (1)$$

where  $\omega$  is a Gaussian function and  $*$  denotes for the convolution. The determinant and the trace of  $M$  are calculated by (2) and (3) respectively:

$$Det(M) = \lambda_1 \lambda_2 = AB - C^2 \quad (2)$$

$$Tr(M) = \lambda_1 + \lambda_2 = A + B = \left( \frac{\partial f(x,y)}{\partial x} \right)^2 * \omega + \left( \frac{\partial f(x,y)}{\partial y} \right)^2 * \omega \quad (3)$$

Then, the detector response is:

$$R_H = Det(M) - k Tr^2(M) \quad (4)$$

where  $k$  is a constant in the range 0.04 to 0.15 [12].

The feature points can be detected by comparing  $R$  with a predetermined threshold, as shown (5):

$$R_H(i, j) > Th \ \& \ \max_{(i,j) \in \Omega} R_H(i, j) \quad (5)$$

According as (5), in each region  $\Omega$  a point which  $R_H$  is maximal value and exceed a predetermined threshold  $Th$ , is selected. When the threshold value is small, the number of feature points is increased, on the other hand, if the threshold value is increased; the number of feature points is decreased. Figure 1 shows an example of the extraction of the feature points.

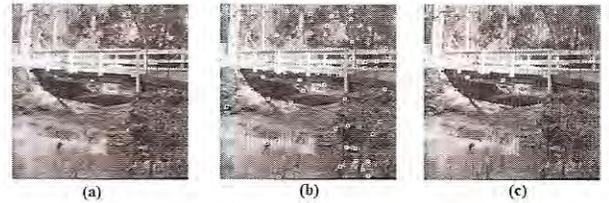


Figure 1. (a) Original image. (b) Feature points with a value threshold 10. (c) Feature points with a value threshold 100.

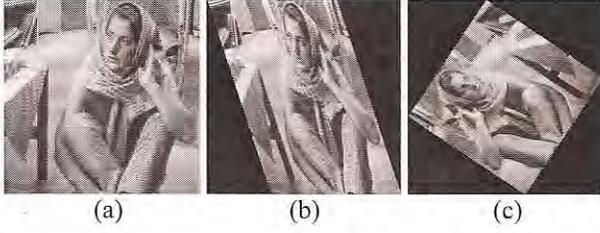


Figure 2. (a) Original image. (b) Lena image (a) with affine distortion. (c) Normalized version obtained from (a) and (b)

### B. Image normalization

The normalization procedure of an image  $f(x,y)$  consists of the following steps:

1) Center the image  $f(x,y)$ , through the Affine Transformation as given by:

$$\begin{pmatrix} x_a \\ y_a \end{pmatrix} = A \cdot \begin{pmatrix} x \\ y \end{pmatrix} - d \quad (6)$$

where matrix  $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  and the vector  $d = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$  with:

$$d_1 = \frac{m_{10}}{m_{00}}, d_2 = \frac{m_{01}}{m_{00}} \quad (7)$$

where  $m_{10}, m_{01}$  and  $m_{00}$ , are the moments of  $f(x,y)$ , and  $d_1, d_2$  are the central moments of  $f(x,y)$  [5]. This step eliminates the translation effect by assigning the center of the normalized image at the density center of the image. The resulting centered image is denoted as  $f_1(x,y)$ .

2) Apply a shearing transform to  $f_1(x,y)$  in the  $x$ -direction using the matrix  $A_x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ . The resulting image is

denoted by  $f_2(x,y)$ . This step eliminates shearing effect in the  $x$ -direction.

3) Apply a shearing transform to  $f_2(x,y)$  in the  $y$ -direction using the matrix  $A_y = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$ . The resulting image is

denoted by  $f_3(x,y)$ . This step eliminates shearing effect in the  $y$ -direction.

4) Scale  $f_3(x,y)$  in both  $x$  and  $y$  directions with the matrix  $A_s = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$  and the resulting image is denoted by  $f_4(x,y)$ .

This step eliminates the scaling effect by forcing the normalized image to a standard size. The final image  $f_4(x,y)$  is the normalized image. It is important to denote that each step in the normalization procedure is invertible; this will allow us to convert the normalized image back to its original version. The determination of transformation parameters  $\beta, \gamma, \alpha$  and  $\delta$ , associated with the transforms  $A_x, A_y$ , and  $A_s$  are shown in detail in the paper presented by [6]. In the figure 2,

an example of the original image, the image suffered an affine distortion and the normalized version of both images is shown.

### C. Invariant feature points selection

The proposed watermarking algorithm uses Harris feature point-based invariant regions to embed the watermark.

However, the Harris feature points are sensitive principally to change the image scale, impulsive and Gaussian noise contamination. To combat this problematic situation, we propose normalize image before feature detection.

According to the image normalization procedure [5], [6], the normalized image obtained from a geometric transformation procedure is invariant to any affine distortions and geometric attacks. This will ensure the integrity of the feature points in the normalized image even when the image undergoes geometric attacks. This solves the above mentioned sensibility for change of the image scale. On the other hand, to solve the Harris features sensibility against Gaussian and impulsive noise, the image is processing as follows:

1) Apply an affine transformation, Gaussian noise with median  $M=0$ , variance  $\sigma=0.01$  and impulsive noise with density  $d=0.01$  to the original image. The resulting images are denoted by  $f_{affine}(x,y)$ ,  $f_{Gaussian}(x,y)$  and  $f_{impulsive}(x,y)$  respectively.

2) Filter each image with a low pass filter, for example, a median filter.

3) Obtain the normalized image from  $f_{affine}(x,y)$ ,  $f_{Gaussian}(x,y)$  and  $f_{impulsive}(x,y)$ . The resulting images are denoted by  $f_{N-affine}(x,y)$ ,  $f_{N-Gaussian}(x,y)$  and  $f_{N-impulsive}(x,y)$  respectively.

4) Obtain Harris feature points from  $f_{N-affine}(x,y)$ ,  $f_{N-Gaussian}(x,y)$  and  $f_{N-impulsive}(x,y)$ . The resulting feature points are denoted by  $FP_{affine}$ ,  $FP_{Gaussian}$  and  $FP_{impulsive}$  respectively.

5) Obtain common invariant feature points from  $FP_{affine}$ ,  $FP_{Gaussian}$  and  $FP_{impulsive}$ .

6) Repeat steps 1-5 increasing the variance  $\sigma$  and density  $d$  from 0.01 to 0.09. The principal reason of select this interval is that the scheme should be robustness against noise contamination and at the same time, Harris features sensibility is solved. If a greater value than 0.09 is used in the Gaussian and impulsive noise respectively, the visually distortion of the image is not acceptable.

7) Obtain final common invariant feature points, comparing feature points  $FP_{affine}$ ,  $FP_{Gaussian}$  and  $FP_{impulsive}$  obtained in all previously iterations. The most common feature points are considered as resulting feature points, which are most stable feature points and robust to common attacks. This procedure shows in figure 3.

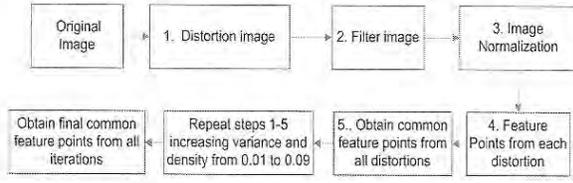


Figure 3. Invariant Harris feature points extraction.

#### D. Embedding process

The embedding process is described as follows:

- 1) Apply the normalization procedure to the original image to get the normalized image.
- 2) Apply the invariant Harris feature points extraction mentioned above to get the adequate feature points.
- 3) Once the feature points are extracted, for each feature point, a circular window with a radius  $r$  is generated. This circular window is denoted by  $S_l$ .
- 4) To obtain the non-overlapped circular regions, some feature points are discarded to satisfy (8).

$$S_2 = \{(x, y) \mid (x, y), (s, t) \in S_1, U_{x,y} \cap U_{s,t} = null\} \quad (8)$$

where  $U_{x,y}$  and  $U_{s,t}$  are circular windows. Figure 4 shows the finally selected points and the non-overlapped circular regions.

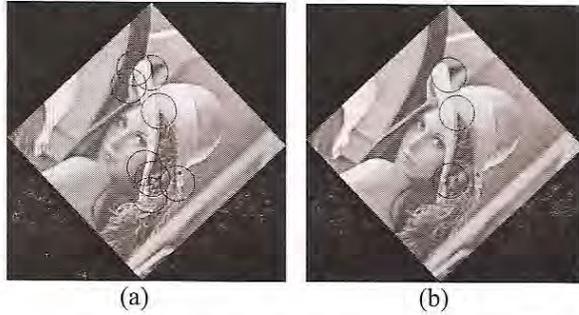


Figure 4. a) Circular regions obtained from invariant Harris feature points. b) Non-overlapped circular regions.

- 5) Construct a patch of  $N \times N$  pixels within each non-overlapped circular region.
- 6) Divide each patch in blocks of  $8 \times 8$  pixels and classify the blocks in weak and strong textures. To estimate the texture complexity, we use the technique proposed by [13]. Firstly DCT coefficients of each block are quantized using the same method as that used in JPEG. If the  $k$ -th block  $F_k(u, v), 0 \leq u, v \leq 7$  satisfies the following condition, this block is classified as strong texture block; otherwise the block is weak texture.

$$\text{if } F_k(0,0) > T_1 \text{ and } \text{number}\{F_k(u, v) / Q(u, v) \neq 0\} > T_2$$

Where, the notation  $\lfloor \cdot \rfloor$  is integer floor function, the function  $\text{number}\{\text{condition}\}$  gets number of elements satisfied the condition and  $Q(u, v)$  is the value of quantification matrix at spatial frequency  $(u, v)$ .  $T_1$  and  $T_2$  are two predefined thresholds.

7) Create a mask image  $M$ , which is a binary image, taking 1s within normalized image area and 0s elsewhere, with same scale and rotation factors as that of the normalized image. This pattern is only used as the support of the watermark.

8) Generate a watermark  $W = [w_1, w_2, \dots, w_n]$  using a user's secret key, where  $w_i = \{1, -1\}, i = 1 \dots n$ .

9) Localize each patch into the mask image  $M$ .

10) The coefficients in middle frequency range of each strong and weak texture block in the patch are replaced with the elements of watermark pattern. Previously, the elements that are inserted into the strong texture are multiplied by a gain factor  $\alpha_1$ . The same manner, the elements that are inserted into the weak texture, are multiplied by a gain factor  $\alpha_2$ . Then apply the IDCT to each watermarked block to get watermarked pattern  $M_w$ .

11) Apply the inverse normalization to the watermarked pattern  $M_w$  to get watermarked pattern  $W_p$  with same size as the cover image.

12)  $W_p$  is embedded into the original image additively with a gain factor  $\alpha_3$ . This produces the watermark image.

$$I_w = I_o + (W_p \cdot \alpha_3) \quad (9)$$

where  $I_o$  and  $I_w$  are original and watermarked image, and  $W_p$  is watermark pattern generated by step 11.

The whole procedure is equivalent to embedding the watermark into the DCT domain of the normalized image. The blocks with weak and strong texture allow embedding adequately watermark without causing any visual distortion to watermarked image.

#### E. Detection process

The process of watermark detection is:

- 1) Apply the normalization procedure to the watermarked image to get the normalized watermarked image.
- 2) Apply the invariant Harris feature points extraction to the normalized watermarked image, which is same procedure in the embed stage.
- 3) Similarly as the embed stage, obtain watermarked patches, dividing each patch into blocks of  $8 \times 8$  pixels and applying the DCT to each block. The middle range frequencies of the DCT coefficients  $C_w$  of each block are extracted. Extract the watermark  $W'$  is formed by (10)

$$W' = [w_1, w_2, \dots, w_{N-1}, w_N] \quad (10)$$

$$w_k = \text{sign}(C_{wk})$$

where  $w_k$  is the extracted watermark sequence ( $L$  bits) from  $k$ -th block and  $\text{sign}$  is a sign function. Finally, the normalized correlation is used to evaluate the similarities of the watermark:

$$N_c = \frac{\sum_{i=1}^n W(i)W'(i)}{\sqrt{\sum_{i=1}^n W(i)^2} \sqrt{\sum_{i=1}^n W'(i)^2}} \quad (11)$$

where  $n$  is the watermark length whereas  $W$  and  $W'$  are the original and the extracted watermarks. Finally, the decision is made by considering the maximal  $N_c$  value from all the patches.

### III. EXPERIMENTAL RESULTS

In the computer simulations, 8 bits grayscale images of size 512x512 were used, and two threshold values  $T_1$ ,  $T_2$ , to classify blocks into two categories: strong texture and weak texture, are set 217 and 18, respectively. The proposed scheme is evaluated from the watermark imperceptibility and robustness points of view.

#### A. Watermark imperceptibility

A 256-bit binary watermark was embedded redundantly two times into the images. The gain factor  $\alpha_3$  are increased from 0.01 to 0.1. The finally value to  $\alpha_3$  after to apply imperceptibility test is 0.03, using gain factors values 6 and 3.5 to  $\alpha_1$  (strong texture) and  $\alpha_2$  (weak texture) respectively.

In figure 5 shows an original image, watermark version and difference image between both images. The difference image is magnified for illustrated purposes.

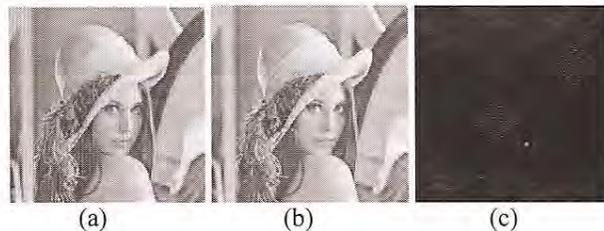


Figure 5. (a) Original Lena image. (b) Watermarked image. (c) Difference image between (a) and (b).

From figure 5, we can see that the embedded watermark in the original Lena image is not visible to the naked eye. To realize an equitable comparison with the results reported in [11], table 1 shows the peak signal to noise ratio (PSNR) of images Lena, Peppers and House.

TABLE I. PSNR OBTAINED FROM IMAGES LENA, PEPPERS AND HOUSE

Image	Proposed method by Lei-da et al. [11]	Proposed method
Lena	37.4 dB	39.3 dB
Peppers	37.0 dB	38.7 dB
House	36.1 dB	38.1 dB

Table 1 shows that the watermark imperceptibility in terms of PSNR obtained in the proposed method is better in comparison with the method by Lei-da et al. [11].

#### B. Watermark robustness

To evaluate watermark robustness in the proposed method, several attacks are applied to the watermarked images. Table 2 shows watermark robustness comparison between proposed method and results reported in the method by Lei-da et al. [11], in the terms of normalized correlation of extracted watermark.

A dash ‘-’ in table 2 indicates that the result is not reported in the document. From table 2 we show that the method proposed by Lei-da et al. [11] present better performance in some attacks with respect to the proposed method in this paper, for example, when the image is without attack, Gaussian noise contamination, scaling and combined attack compose by scaling and JPEG compression. On the other hand, our proposed method presents better performance and robustness with respect to Lei-da et al. [11] against a most variety attacks, including affine transformation, impulsive noise contamination, shearing attack, aspect ratio, flipping and sharpening, and so on.

Although the normalized correlation value obtained in the proposed method is under 1.0 even without attack, the robustness and performance presents is better with respect to the method by Lei-da et al. [11], because the normalized correlation value is great than 0.7 in all cases, therefore if a threshold value  $Th$  is set to 0.7, the proposed scheme can detect the watermark sequence correctly under a wide range of attacks.

### IV. CONCLUSIONS

In this paper we present a robust image watermarking method against the geometric distortions and several

TABLE II. NORMALIZED CORRELATION OF EXTRACTED WATERMARK AFTER ATTACKS

Attacks	Lei-da et al. [11]	Proposed method
Without attack	1.0	0.9733
Gaussian noise $M=0, \sigma=0.01$	1.0	0.9012
Impulsive noise with density $d=0.09$	-	0.9145
Median filter 3x3	0.8310	0.8106
JPEG QF=50	0.9193	0.9375
Rotation 30°	0.8930	0.9219
Scaling 1.4	1.0	0.9317
Remove row 5 cols 17	0.9973	0.9063
Rotation 30° + JPEG QF=80	0.8750	0.7902
Scaling 1.5 + JPEG QF = 80	1.0	0.8030
Affine Transformation	-	0.9120
Shearing with factor (0.7%)	-	0.9265
Aspect ratio change (1.2,1.0)	-	0.9516
Flipping Horizontal and Vertical	-	0.9428
Sharpening [0 -1 0; -1 5 -1; 0 -1 0]	-	0.8520

attacks of signal processing. Initially, the original image is normalized using a normalization procedure and the feature points are then extracted.

Furthermore, the locally most stable feature points are obtained and used to generate several non-overlapped circular regions. Texture-based image block classification in Discrete Cosine Transform (DCT) domain is also used to get major watermark imperceptibility. The watermark sequence is embedded into these classified regions in the DCT domain.

In the detection stage, the watermark sequence can be obtained without the original image. The simulation results show watermark imperceptibility and robustness to various geometrical attacks and common signal processing such as JPEG compression, filtering operation and noise contamination, etc.

The performance of the proposed algorithm is compared with basically Lei-da's algorithm [11] from watermark imperceptibility and robustness points of view. Comparison results show that the proposed algorithm presents better robustness against a most variety of attacks, including affine transformation, impulsive noise, shearing, aspect ratio, flipping and sharpening, while keeping acceptable imperceptibility of the watermark signal.

## ACKNOWLEDGMENT

The authors thank The National Science and Technology Council (CONACYT) of Mexico and to the National Polytechnic Institute of Mexico for the financial supports during realization of this research.

## REFERENCES

- [1] M. Barni, "Effectiveness of exhaustive search and template matching against watermark desynchronization", *IEEE Trans. on Signal Processing Letter*, 2005, Vol. 12, No. 2, pp. 158-261.
- [2] D. Zheng, J. Zhao and A.E. Saddik, "RST-invariant digital image watermarking based on log-polar mapping and phase correlation", *IEEE Trans. Circuits Syst. Video Technol.*, 2003, vol. 13, no. 8, pp. 753-765.
- [3] J.O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking", in *Proc. ICIP'97, 1997*, Vol. 1, pp. 536-539.
- [4] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin: "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression", *IEEE Trans. Circuits Syst. Video Technol.*, 2003, vol. 13, no. 8, pp. 776-786.
- [5] M.K. Hu, "Visual pattern recognition by moment invariants", *IRE. Trans. on Information Theory*, 1962, Vol. 8, pp. 179-187.
- [6] P. Dong, J.B. Brankov, N.P. Galatsanos, Y. Yang and F. Davoine, "Digital watermarking to geometric distortions", *IEEE Trans. on Image Processing*, 2005, Vol. 14, No. 12, pp. 2140-2150.
- [7] M. Cedillo, M. Nakano and H. Perez-Meana, "Robust watermarking to geometric distortion based on image normalization and texture classification", in *Proc. IEEE Midwest Symposium CAS, Knoxville Tennessee*, 2008, pp. 245-248.
- [8] Kutter M, Bhattacharjee S K, Ebrahimi T. "Towards second generation watermarking schemes". *Proceedings of IEEE International Conference on Image Processing*, Oct 24-28, 1999, Kobe, Japan. Piscataway, NJ, USA, IEEE, 1999, pp. 320-323
- [9] Bas P, Chassery J M, Macq B. "Geometrically invariant watermarking using feature points", *IEEE Transactions on Image Processing*, 2002, vol. 11, no. 9, pp. 1014-1028
- [10] Tang C W, Hang H M, "A feature-based robust digital image watermarking scheme", *IEEE Transactions on Signal Processing*, 2003, vol.51 no.4 pp.950-959
- [11] Lei-da L., Bao-long G., Lei G., "Rotation, scaling and translation invariant image watermarking using feature points", in *The Journal Of China Universities Of Post And Telecommunications*, 2008, vol. 15, issue 2, pp.82-87.
- [12] Harris C, Stephens M. "A combined corner and edge detector", *Proceedings of the Fourth Alvey Vision Conference*, Manchester, UK, , Aug 31-Sep 2, 1988, pp. 147-151.
- [13] J. Huang and Y. Q. Shi, "Adaptive image watermarking scheme based on visual masking", *IEEE Electronics Letter*, 1998, pp. 748-750.



# 2008 5<sup>th</sup> International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE) (Formerly known as ICEEE)

Mexico City, Mexico  
November 12 - 14, 2008

CCE  
2008



*Message from the podium*

*Keynote Speakers*

*Organizing Committee*

*Special Thanks*

*Reviewers*

*General Information*

*Program*

*Courses*

*Abstract Book*

*Author Index*

*Brochure*

*Poster*

*Sponsors*

*Technical Support Information*

**IEEE Catalog Number: CFP08827-CDR**  
**ISBN: 978-1-4244-2499-3**  
**Library of Congress: 2008903800**

© 2008 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

# Message from the Podium

---

## Editorial.

This year we are celebrating the 5th International Conference, which is highlighted by an important change in its organization that includes for the first time, the participation of three academic departments at CINVESTAV: Electrical Engineering, Computer Science and Automatic Control. This marks an important step for a Conference that was born in the last decade of the past century (1995) as an effort of the Department of Electrical Engineering to open a specialized forum where the local research groups could expose their investigation results and proposals, interact with each other, and to have the opportunity to become aware of the recent research and developments from leading institutions abroad, too. Also, the interaction with technological industry managers and government officials, has had since then, a special place in the activities of the conference. Evidently, the conference has experienced a continuous evolution that is reflected in its enhancements throughout its existence. First, it was a national event; then, in 2004 it was projected as an international conference. This year, its organization has been extended to include the participation of two departments that emerged as specialities with their own personalities and structures within CINVESTAV, namely, the Computer Science Department and the Automatic Control Department, whose contributions have been very valuable. Such a new stage has arisen many expectations and opens endless possibilities for the future. We hope that our objective of spanning interest to a wider engineering audience can be fulfilled, keeping always in mind the goal of having an event of better quality each year.

As expected, the participation to the conference has increased. This year, we received 166 submissions from 14 countries (including Mexico), from which 94 were accepted for oral presentation. The 39 submissions from abroad came from countries such as the USA, India, Spain, China, Egypt, Argentina and Brazil, among others, reflecting the renewed efforts conjugated to broaden the participation beyond our borders, so that this conference can be considered in the near future, as an important and challenging forum.

As Presidents of CCE 2008, we wish to thank the Organizing Committee, the anonymous referees and the supporting personnel for their valuable time and efforts for they make possible to hold a successful 2008 5<sup>th</sup> International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE).

To all our attendees, we give them a warm welcome wishing them a very fruitful and enriching conference, hoping that all their expectations are fulfilled.

Dr. José Antonio Moreno Cadenas

Dr. Carlos A. Coello Coello

Dr. Alexander Poznyak Gorbach

# Program

**Automatic Control**

**Biomedical Engineering**

**Communications Systems**

**Computer Science and Computer Engineering**

**Mechatronics**

**Solid-State Materials, Electron Devices and  
Integrated Circuits**

**Workshop CASI 2008**

# Computer Science and Engineering

---

## 16. CS2: Computer Science and Computer Engineering

Wednesday (15:00-17:00) Room 2

Session Chair: Francisco Rodríguez Henríquez

### 15:00-15:20 **A Reversible Data Hiding Algorithm for Radiological Medical Images**

*Zobeida Jezabel Guzman Zavaleta, Institution: National Institute for Astrophysics, Optics and Electronics, INAOE, MEXICO*

*Claudia Feregrino Uribe, Institution: National Institute for Astrophysics, Optics and Electronics, INAOE, MEXICO*

*Jose Alberto Martinez Villanueva, Institution: National Institute for Astrophysics, Optics and Electronics, INAOE, MEXICO*

*Rene Cumplido, Institution: National Institute for Astrophysics, Optics and Electronics, INAOE, MEXICO*

### 15:20-15:40 **Geometric Distortions Resilient Watermarking Technique Based on 2D Color Histogram Modification**

*Manuel Cedillo-Hernandez, Institution: National Polytechnic Institute*

*Mariko Nakano-Miyatake, Institution: National Polytechnic Institute*

*Hector Manuel Perez-Meana, Institution: National Polytechnic Institute*

### 15:40-16:00 **Content Authentication Schemes for Digital Images**

*Jose Antonio Mendoza, Institution: National Polytechnic Institute*

*Clara Cruz Ramos, Institution: National Polytechnic Institute*

*Mariko Nakano-Miyatake, Institution: National Polytechnic Institute*

*Hector Manuel Perez-Meana, Institution: National Polytechnic Institute*

## Geometric Distortions Resilient Watermarking Technique Based on 2D Color Histogram Modification

M. Cedillo Hernandez, M. Nakano Miyatake, H.M. Perez Meana

Section of Investigation and Postgrade Studies, ESIME Culhuacán-IPN, México D.F., México  
Phone (525) 7 29 60 00 Ext. 73262 Fax (525) 6 56 20 58 E-mail: mariko@calmecac.esimecu.ipn.mx

**Abstract** — This paper presents a robust watermarking technique against geometric distortions. The proposed technique is based on the modification of the 2D color histogram. Because the histogram of an image is one of the image geometric invariant representations, if the watermark can be embedded into the histogram, it should survive to most geometric transformations. The difficulty of the watermarking based on histogram modification is that the relationship between the histogram representation and the pixel representation is not linear; therefore the distortion caused by the histogram modification cannot be measured in advance. In the proposed method, the values of the RGB bins are modified according to watermark bit sequences. The experimental results show robustness against several geometric distortions, such as rotation, scaling, Affine Transformation, cropping among other geometric attacks.

**Keywords** — Digital watermark, color histogram, geometric attacks, copyright protection, watermark, RGB bins.

### I. INTRODUCTION

In the public watermarking scheme, the synchronization loss, between the watermark embedding and the detection stages, causes watermark detection errors. Geometric distortions, such as rotation, scaling, translation and any Affine transformation, are the main causes of this problem, however this type of distortion is common in practice; and then several approaches have been proposed in the literature to combat the geometric attacks, which can be classified basically into six approaches [1].

The first approach uses exhaustive search in the watermark detection stage, even if the effectiveness to estimate geometric factors is better than other approaches [2], the extremely high computational complexity makes this method impractical. In the second approach, the watermark signal is embedded in a geometrically invariant domain, such as the Fourier-Mellin Transform (FMT) [3]. This approach is effective in theory, but it is difficult to implement, due to the Log Polar Mapping and its inverse operation. In the third approach, together with the watermark signal, the template signal is embedded to use them in the resynchronization [4]. A main disadvantage of this approach is the difficulty in keeping good a quality of the watermarked image, because the template signal must be additionally embedded into the

image. The fourth approach is a features based approach [5, 6], in which salient features of the image are used for resynchronization, this approach doesn't embed additional signal into the image, however generally a high computational complexity is required to extract the salient feature in both, embedding and detection, stages.

In the fifth approach, the watermark signal is embedded into the normalized image generated by invariant moment factors introduced by [7]. Next an inverse normalization operation is applied to the processed image, to obtain the watermarked image. This approach is theoretically efficient, but the discrete implementation causes quality degradation of the image, due to the required interpolation process. In [1,8], to avoid a quality degradation of the watermarked image, a watermark signal is normalized and embedded into the original version of the image. Authors of [1] show watermark robustness to several geometric distortions, however to get acceptable lower Bit Error Rate (BER) of the extracted watermark sequence, watermark imperceptibility must be sacrificed.

The final approach uses the histogram information of the image. The histogram is one of the geometric invariant representations, and therefore the theoretically watermark embedded into histogram must survive geometric distortions, such as translation, rotation, scaling, etc. Especially for color images, the amount of histogram information is enough to embed watermark sequence with a reasonable length.

The use of image histograms, as watermark embedding domain, has been previously reported [9-11]. In [9], exact histogram specification is used to embed watermark into the images. An exact histogram-specification algorithm, based on combining a statistical model of the images and the lattice structure that is assumed on the basis of discrete images, was proposed. This method is resistant to various common image attacks. Chareyron et al [10] extended the histogram-specification method proposed by [9] to chromatic histograms, and then to color 3D histograms. The method embeds a watermark in the xy chromatic plane of the color image. This method aims to resist geometric distortion and cropping. A special pattern generated using a secret key is used to modify the chromatic distribution of the image. Then, the chromatic values associated with the pattern are modified to embed the watermark. Experimental results show that this watermark strategy resists a change in scaling and cropping. Roy et al [11]

proposed a method of watermarking using a color histogram based in constrained Earth Mover Distance (EMD) optimization to modify an image to a target histogram. The use of constrained EMD helps in ensuring that the image and its watermarked version are perceptually similar. This method is robust against several geometric and signal processing attacks. However its high computational complexity may limit its use in some practical applications.

In this paper, we propose an image watermarking method that is based on 2D image color histogram modification. In this modification, values of histogram bins are modified according to the watermark bit sequence. The simulation results show robustness of the proposed method against several geometric distortions including rotation, scaling, Affine transformation, cropping and among other geometric attacks.

## II. PROPOSED METHOD

In computer graphics and photography, a color histogram is a representation of the distribution of colors in a given image. The number of pixels of each color is represented by two-dimensional (2D) or three-dimensional (3D) color space. Fig. 1 shows the Lena image and their 2D color histogram, using the Green and Blue components of RGB model as x-axis and y-axis, respectively.



Fig. 1. Original image and their 2D color histogram, using Green component and Blue component..

The proposed watermarking method based on color histograms is divided in two processes: embedding and detection process which are described below:

### A. Embedding Process

The watermark generation and embedding process are carried out as follows:

- 1) Decompose the original image  $I$  in three components of RGB color space.
- 2) Obtain the 2D G-B color histogram  $H$  of the original image  $I$ .

- 3) Segment the 2D color histogram  $H$  in blocks of  $N \times N$  pixels.
- 4) Generate the 2D pseudo-random binary watermark pattern  $W$  of the  $N \times N$  elements using a user's secret key.
- 5) Select a block of the histogram  $H$  and modify the bins of the G and B components according to the watermark  $W$ .
- 6) Using the modified G and B components, the watermarked image  $I_w$  is constructed.

The histogram modification is based in the next rules:

#### Rule 1:

*If  $W(j, k) = 1$ , where  $j, k = 1, \dots, N$ , Do*  
*If  $H(j, k) \neq 0$  then  $H(j, k)$  is not changed*  
*If  $H(j, k) = 0$  then  $H(j, k)$  is assigned neighbor non zero value*

#### Rule 2:

*If  $W(j, k) = 0$ , where  $j, k = 1, \dots, N$  Do*  
*If  $H(j, k) = 0$  then  $H(j, k)$  is not changed*  
*If  $H(j, k) \neq 0$  then  $H(j, k) = 0$  and their values pass to the nearest neighbor.*

Figure 2 shows the schematic diagram of watermarking embedding process.

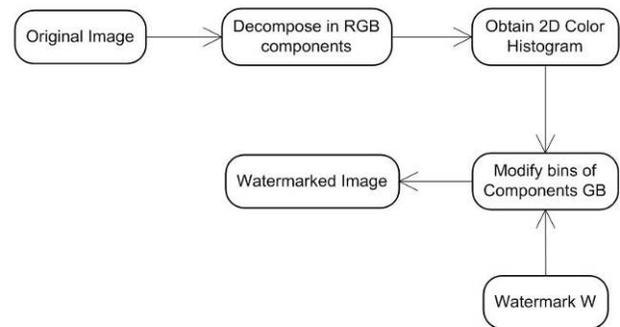


Fig. 2. Schematic diagram of watermark embedding process.

The modification rules ensure the watermark imperceptibility in the image, because the modified values are obtained of the neighbor values, so that there are slight changes in the colors of the image and the total number of bins is not altered with respect the original data.

The watermark pattern size  $N$  is conditioned by the 2D histogram dimensions, due to that size of the histogram is always  $256 \times 256$ , because the range of bin values is 0 to 255, thus, the value of  $N$  is  $1 \leq N \leq 255$ .

Choose a small value for  $N$ , the payload of watermark is reduced and the robustness against geometric attacks is severely affected. On the other hand, choose a big value for  $N$ , the robustness against geometric attacks is increased, but the imperceptibility of watermark is affected. Hence, it is recommended to select a value  $N$  that provides robustness against geometric attacks and at the same time the watermark is imperceptible.

In summary, the proposed watermarking scheme has the following features:

- Blind detection, because the original image is not necessary to detect the watermark.
- Robust against geometrical distortions.
- Applicable to color images.
- Low computational complexity.
- Good quality of the watermarked image.

### B. Detection Process

The watermark detection process is described as follows:

- 1) Decompose the watermarked image  $I_w$  in three components of RGB model.
- 2) Obtain the 2D G-B color histogram  $H_w$  of the watermarked image  $I_w$ .
- 3) Segment  $H_w$  into blocks of  $N \times N$  pixels.
- 4) Calculate the cross correlation  $c$  between the owner's binary watermark pattern and the watermarked region of  $H_w$  as follows:

$$c = \sum_{i=1}^N \sum_{j=1}^N H_{w(i,j)} \cdot W'_{(i,j)} \quad (1)$$

Figure 3 shows the schematic diagram of watermarking detection process.

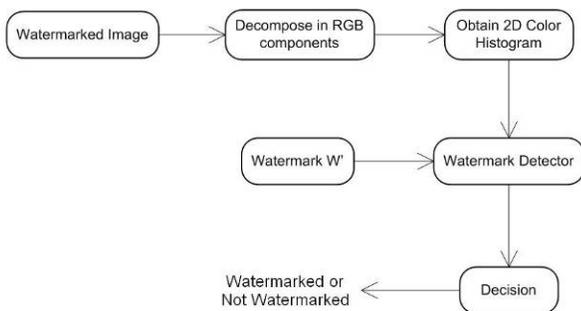


Fig. 3. Schematic diagram of watermark detection process.



Fig. 4. Watermarked Lena image and the modified histogram.

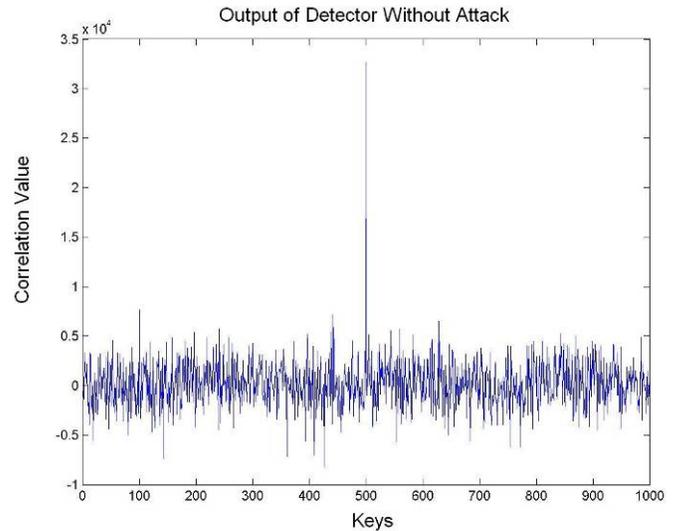


Fig. 5. The detector response without attack.

## III. EXPERIMENTAL RESULTS

In this section, some experimental results are shown in which color images of size 512 x 512 are used. The size of segmented region of the histogram  $N$  is set equal to 32. Here the watermark imperceptibility and robustness are considered for selection of the value  $N$ . If we select a smaller value than 32 for  $N$ , the robustness of the watermark against several geometric attacks is compromised, while if we select a bigger value than 32, a visual artifact occurred in the watermarked image. The watermark is a 2D pseudo-random binary pattern with values 1's and 0's and the value of secret key was 500. The 2D histogram is modified according to the rules mentioned in the section II.

### A. Watermark imperceptibility

The watermarked image and their modified histogram without geometric attack applied are shown in Fig. 4. The Peak Signal to Noise Ratio (PSNR) of the watermarked image respect to the original one is equal to 36.44 dB. Figure 5 shows the detector response. Here we observe

that the watermark pattern generated by owner's secret key (500) is detected without any ambiguity.

### B. Geometric Attacks.

In this section, we show the results when geometric attacks are applied to watermarked image. The geometric attacks considered are shown in table I.

TABLE I  
GEOMETRIC ATTACKS

	Attack
a)	Rotation by 45°
b)	Scaling with $F_s = 1.4$
c)	Cropping and Scaling 512x512
d)	Affine Transformation with matrix $A = \begin{bmatrix} 1 & 0 \\ 0.5 & 0.8 \end{bmatrix}$
e)	Shearing (0, 0.7%), where each pair of numbers indicate the amount of shearing in the $x$ and $y$ and directions, respectively.
f)	Aspect ratio (1.0, 1.5), where each pair of numbers indicate the amount of scaling in the $x$ and $y$ and directions, respectively.
g)	Rotation 55°, Cropping and Scaling 512x512.

The detector outputs with several geometric attacks are shown Figs. 6 and 7.

The experimental results show the watermark robustness of the proposed method against different geometric distortions and its combined attacks.

From Fig. 6, we can conclude that the proposed method is robust enough to geometric distortions, such as rotation, scaling, cropping, shearing and aspect changes.

### IV. CONCLUSIONS

In this paper we presented a robust watermarking technique against geometric distortions, which is based on the 2D color histogram modification. The method works on the RGB model, modifying the bins values of the G and B components according to the watermark bit sequence and embedding rules. Also the proposed method uses segmentation by blocks of the histogram to provide robustness and imperceptibility of the watermark sequence.

The simulation results show that in the proposed method, watermark sequence is robust to several geometric attacks, such as rotation, scaling, cropping,

Affine Transformation, Shearing, Aspect ratio and its combined attacks.

### ACKNOWLEDGMENT

The authors thank The National Science and Technology Council (CONACyT) of Mexico and to the National Polytechnic Institute of Mexico for the financial supports during realization of this research.

### REFERENCES

- [1] M. Cedillo, M. Nakano and H. Perez, "Robust Watermarking Échème to Geometric Distortion Base don Image Normalization", to be published in Proc of IEEE Midwest Symposium CAS 2008.
- [2] M. Barni, "Effectiveness of exhaustive search and template matching against watermark desynchronization", IEEE Trans. on Signal Processing Latter, vol. 12, no. 2, 2005, pp. 158-161.
- [3] J. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking", in Proc. ICIP' 97, Atlanta, vol. 1, 1997, pp. 536-539.
- [4] S. Pereira, and T. Pun, "Robust template matching for affine resistant image watermarks", IEEE Trans. on Image Processing, vol. 9, no. 6, 2000, pp. 1123-1129.
- [5] E. Izquierdo, "Using Invariant Image Features for Synchronization ", Eurasip Journal on Applied Signal Processing, vol. 2, 2002, pp. 410-417.
- [6] C. Tang and H. M. hang, "A Feature-Based Robust Digital Image Watermarking Scheme", IEEE Trans on Signal Processing, vol. 51, no. 4, 2003, pp. 950-959.
- [7] M. K. Hu, "Visual Pattern Recognition by Moment Invariants", IRE Trans. on Information Theory, vol. 8, 1962, pp. 179-187.
- [8] P.Dong, J.B. Brankov, N.P. Galatsanos, Y. Yang and F. Davoine, "Digital Watermarking robust to geometric distortions,", IEEE Trans. On Image Processing, vol. 14, no. 12, 2005, pp. 2140-2150.
- [9] Coltuc, D., and Bolon, Ph.: 'Robust watermarking by histogram specification'. 6th IEEE Conf. on Image Processing (ICIP'99), Kobe, Japan, October 1999, vol. 2, pp. 236-239.
- [10] Chareyron, G., Macq, B., and Tremeau, A.: 'Watermarking of color images based on segmentation of the XYZ color space'. CGIV 2004 - Second Eur. Conf. on Color in Graphics, Imaging and Vision, Aachen, Germany, April 2004, pp. 178-182.
- [11] Roy, S., and Chang, E.C.: 'Watermarking color histogram'. Proc IEEE Int. Conf. on Image Processing, Vol. 4, pp. 24-27, 2004.

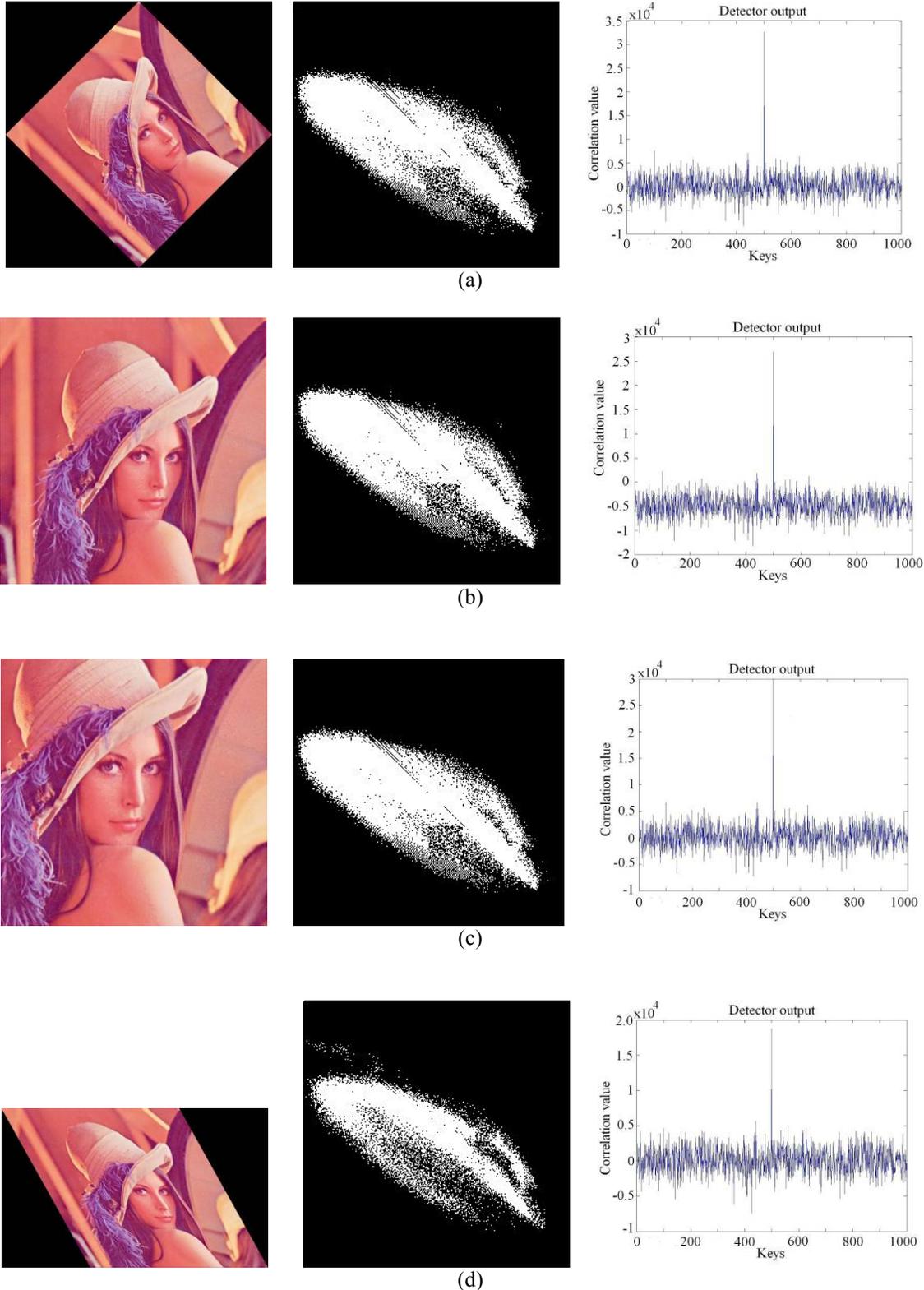


Fig. 6. Detector response when the watermarked image has suffered different geometric attacks: (a) rotation, (b) scaling, (c) cropping and scaling (d) Affine transformation. In all cases the attacked watermarked imaged, its histogram and the detector performance using 1000 different keys is shown.

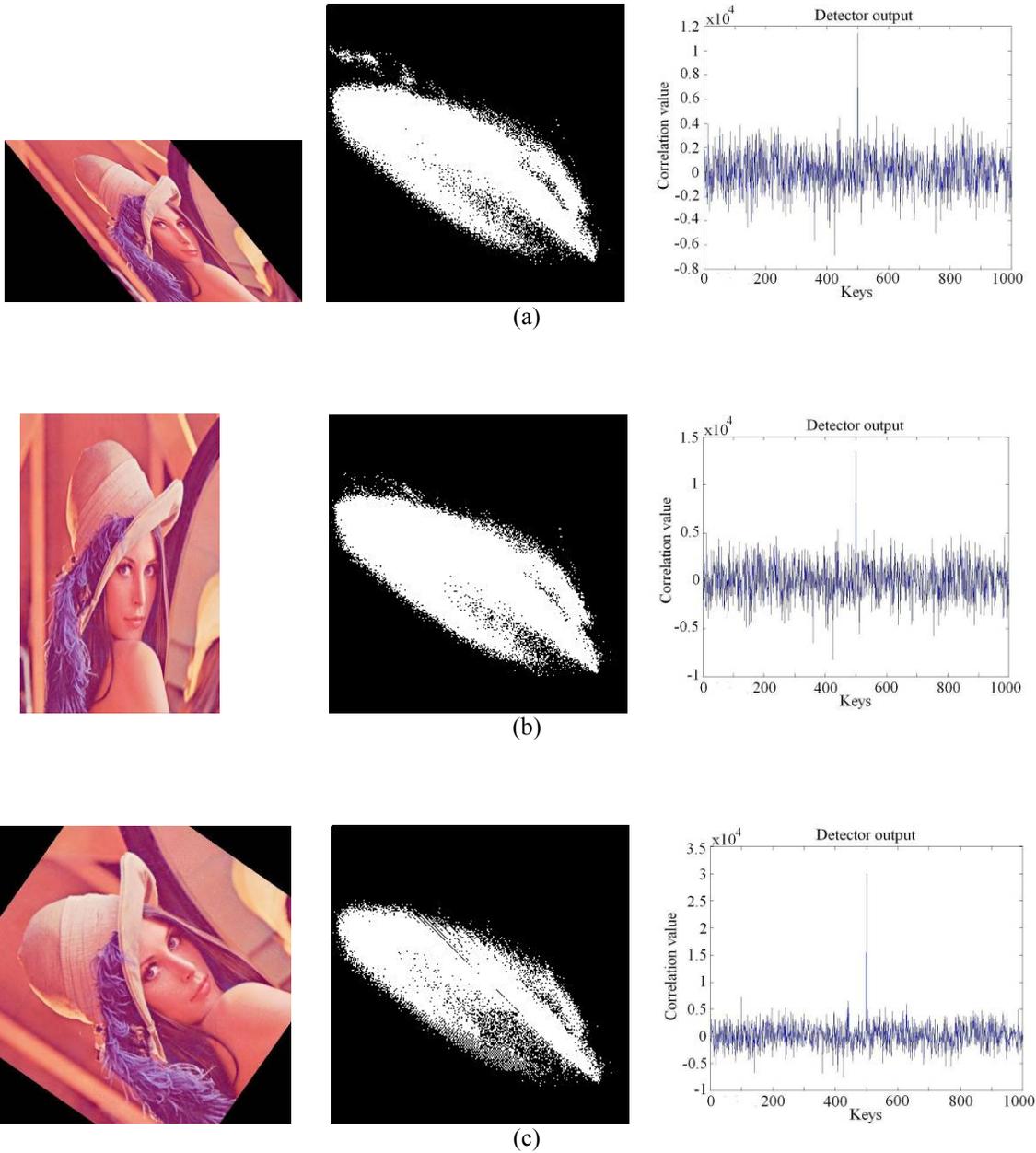


Fig. 7. Detector response when the watermarked image has suffered different geometric attacks: (a) shearing, (b) aspect ratio, (c) cropping and scaling. In all cases the attacked watermarked image, its histogram and the detector performance using 1000 different keys is shown.

# Anexo C

## Glosario

**Ataque no intencional.-** *Ataques que se aplican a una imagen marcada sin el propósito de eliminar la marca de agua. La compresión JPEG y algunos filtros se consideran ataques accidentales.*

**Ataque de colusión.-** *Son ataques que intentan eliminar la marca de agua analizando y utilizando diferentes imágenes que contienen la misma marca de agua.*

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

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

**Ataques geométricos compuestos.-** *Aplicación de más de un ataque geométrico en una misma imagen.*

**Ataques geométricos globales.-** *Distorsiones geométricas que se aplican a toda la imagen.*

**Ataques geométricos locales.-** *Se trata de distorsiones geométricas que se aplican a una o más regiones dentro de una imagen.*

**Detección ciega.-** *Proceso en el cual la imagen original no se encuentra disponible al momento de realizar la detección.*

**DFT.-** *Transformada de Fourier Discreta (por sus siglas en inglés: Discrete Fourier Transform).*

**DCT.-** *Transformada de Coseno Discreta (por sus siglas en inglés: Discrete Cosine Transform).*

**DWT.-** *Transformada Wavelet Discreta (por sus siglas en inglés: Discrete Wavelet Transform).*

**DVD.-** *Disco Versátil Digital (por sus siglas en inglés: Digital Versatile Disc).*

**Falso negativo.-** *Situación en la que el resultado del detector indica a una imagen como no marcada, cuando en realidad sí lo está.*

**Falso positivo.-** *Situación en la que el resultado del detector indica a 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.*

**Histograma de imagen.-** *El histograma de una imagen representa la frecuencia relativa de los niveles de gris de la imagen.*

**IDCT.-** *Transformada de Coseno Discreta Inversa (por sus siglas en inglés: Inverse Discrete Cosine Transform).*

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

**Pérdida de sincronización.-** *Situación que no permite al detector de marca de agua realizar una correcta detección principalmente por 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 inserción.-** *Proceso en donde se oculta una marca de agua en una señal digital.*

**PSNR.-** *Relación Señal a Ruido Pico (por sus siglas en inglés: Peak Signal-to Noise Ratio. Medida utilizada para comparar la distorsión causada por diferentes esquemas de marcas de agua.*

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

## Anexo D

### Imágenes Utilizadas

Los experimentos realizados en el esquema propuesto en el capítulo tres, hacen uso de imágenes con formato BMP de tamaño 512 x 512, 8/píxel con 256 niveles de gris. Las imágenes fueron elegidas por ser utilizadas frecuentemente en el procesamiento de imágenes, y porque visualmente presentan diferentes criterios de complejidad.

Barbara



Boat



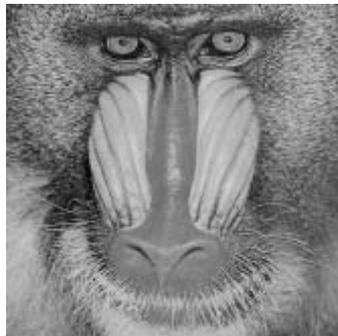
Goldhill



Lena



Mandrill



Bridge



Camera



Peppers



Bird



Lake

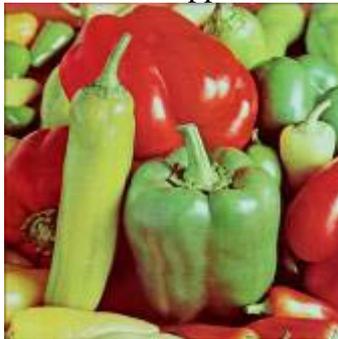


Los experimentos realizados en el esquema propuesto en el capítulo cuatro, hacen uso de imágenes de color de tamaño 512 x 512. Las imágenes fueron elegidas por ser utilizadas frecuentemente en el procesamiento de imágenes, y porque visualmente presentan diferentes criterios de complejidad.

Airplane



Peppers



Car



House



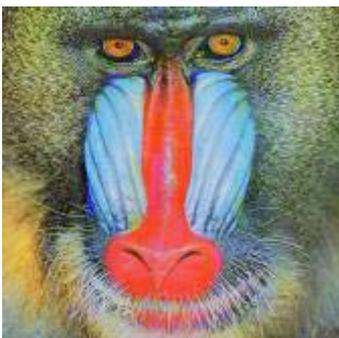
Lena



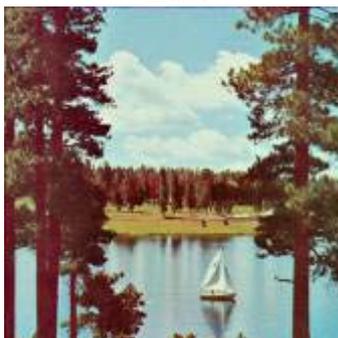
Tiffany



Mandrill



Lake



Tree



Splash

