ANEXO V. Pruebas de robustez realizadas a los algoritmos. Resultados

En este anexo mostramos de manera desarrollada y extensa algunos de los resultados más significativos obtenidos en el estudio de la robustez de los algoritmos implementados frente a los diferentes ataques llevados a cabo. Se trata de una extensión del capítulo 6 del presente proyecto dedicado al estudio de las características de los diferentes métodos de watermarking desarrollados.

La estructura del anexo está dividida en tantas partes como diferentes categorías o clases de ataques se han implementado, mostrándose en cada apartado tablas y gráficas ilustrativas de los resultados, (en cuanto a características de detección correcta de la marca de agua y/o probabilidad de error de bit), obtenidos para cada uno de los algoritmos que se han implementado.

Los resultados se irán mostrando de manera que los algoritmos de características más parecidas se presenten de forma prácticamente paralela de manera que resulte más sencilla la comparación de características. Es por ello que en ciertos casos alteramos el orden de presentación. Notar que, en general, se ilustran los resultados obtenidos en caso de trabajar con imágenes en escala de grises, puesto que los obtenidos con imágenes en color RGB muestran tendencias similares. No obstante también se muestran resultados de robustez en imágenes RGB marcadas, ya sea para corroborar tendencias de comportamiento similares a las de las imágenes marcadas en escala de grises o para denotar alguna diferencia apreciable.

V.1 Ataque de filtrado de mediana

El filtrado de mediana se aplica a las imágenes para suavizar los cambios bruscos que aparecen en las mismas, tipo ruido “salt & pepper”.

V.1.1 Algoritmos 1 y 3

V.1.1.1 Algoritmo 1

Los resultados obtenidos frente a este tipo de ataque en las imágenes marcadas según las características del algoritmo 1 muestran una buena respuesta de la técnica de watermarking implementada. En la gráfica de la figura

V.1 se ilustran las probabilidades de error promedio obtenidas para las marcas de agua estimadas en las diferentes imágenes y según los dos métodos de detección utilizados, (para imágenes en escala de grises).

Se observa que la diferencia entre los resultados obtenidos en la detección por resta y por ICA es prácticamente inapreciable. Las probabilidades de detección globales pueden verse en la tabla V.2, en la que se muestran también las correspondientes al algoritmo 3.

Los resultados obtenidos para las imágenes en color presentan tendencias similares a las mostradas en la figura V.I.

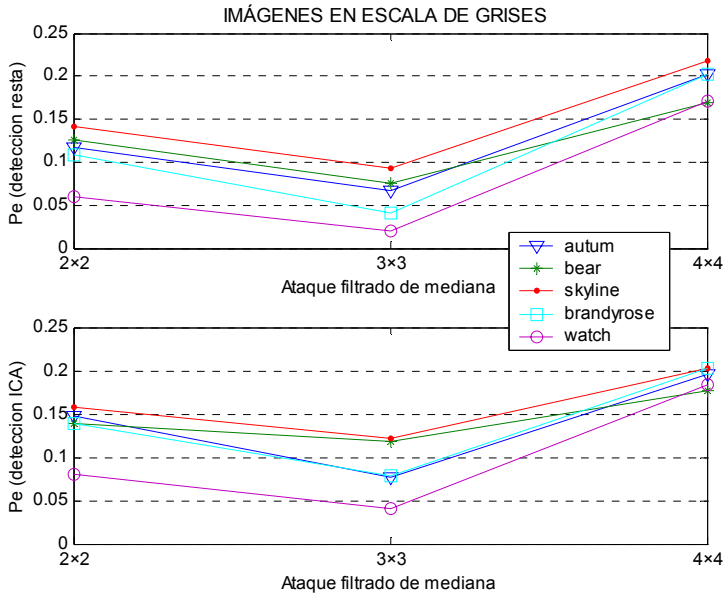


FIGURA V. Probabilidad de error de bit en función de la severidad del ataque de filtrado de mediana para cada imagen, (véase leyenda). Resultados de la detección por sustracción (gráfica superior) y mediante ICA (imagen inferior). Para imágenes marcadas en escala de grises. Algoritmo 1.

V.1.1.2Algoritmo 3

En la figura V.2 se muestran los valores obtenidos para la probabilidad de error de bits en las estimaciones frente a diferentes grados de ataques de filtrado de mediana. Se observa cómo las diferencias entre usar detección por resta o por ICA son aún menos apreciables que en el algoritmo 1. Lo que puede hacernos pensar que la combinación de DWT con ICA pueda resultar interesante.

La probabilidad de detección correcta promedio frente a ataques de filtrado de mediana de la imagen, en función de la severidad del ataque y en general pueden verse en la tabla V.1.

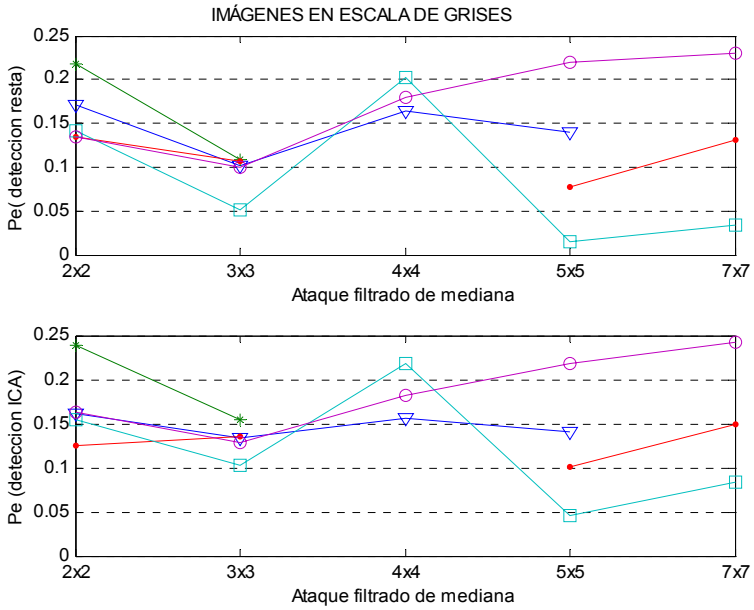


FIGURA V.2. Idem V.1 para el algoritmo 3.

En la siguiente tabla ilustramos los valores de probabilidades de detección correcta obtenidos para ambos algoritmos y según el método de detección usado.

ALGORITMO 1 (Dominio DCT de la imagen)					
Método de detección	**ATAQUE FILTRADO DE MEDIANA**				
	2×2	3×3	4×4	5×5	7×7
Sustracción directa	0.98	1.0	0.48	0.64	0.48
ICA	0.88	0.98	0.42	0.60	0.48
ALGORITMO 3 (Dominio DWT y DCT de la imagen)					
Método de detección	**ATAQUE FILTRADO DE MEDIANA**				
	2×2	3×3	4×4	5×5	7×7
Sustracción directa	0.74	0.96	0.18	0.84	0.60
ICA	0.56	0.94	0.14	0.76	0.50

TABLA V.1. Valores de probabilidad de detección frente al ataque de filtrado de mediana. En función de la severidad del ataque y promedio, para ambos tipos de detección. Obtenidas para los algoritmos 1 (arriba) y 3.

V.1.2 Algoritmos 2 y 4

En ambos algoritmos se observa una buena respuesta frente al ataque de filtrado de mediana realizado a las imágenes bajo prueba según diferentes grados de severidad. Puede verse cómo la respuesta frente a la convolución con filtros de orden par presenta peores resultados que los que se obtienen para filtros de mediana de órdenes impares.

ALGORITMO 2 (Dominio DCT de la imagen)				
Método de detección	**ATAQUE FILTRADO DE MEDIANA**			**Valor promedio de detección frente a filtrado de mediana**
	2×2	3×3	4×4	
Sustracción directa	0.9	1	0.87	0.90
ICA	0.95	0.98	0.63	0.85
ALGORITMO 4 (Dominio DWT y DCT de la imagen)				
Método de detección	**ATAQUE FILTRADO DE MEDIANA**			**Valor promedio de detección frente a filtrado de mediana**
	2×2	3×3	4×4	
Sustracción directa	0.88	0.90	0.60	0.80
ICA	0.88	0.90	0.60	0.80

TABLA V.2. Probabilidad de detección correcta frente al ataque de filtrado de mediana en los algoritmos 2 y 4.

V.2 Ataque FMLR

El ataque FMLR es un ataque de borrado que aplica el operador laplaciano a la imagen, de manera que consigue eliminar el rizado presente en la misma, rizado que puede corresponderse con la marca de agua insertada.

V.2.1 Algoritmos 1 y 3

V.2.1.1 Algoritmo 1

La figura V.3 muestra las probabilidades de error de bit promedio obtenidas para los dos métodos de detección utilizados, tanto para imágenes en escala de grises como para imágenes en color RGB. En ella se observan probabilidades de error similares con un valor ligeramente superior para el caso de detección por resta.

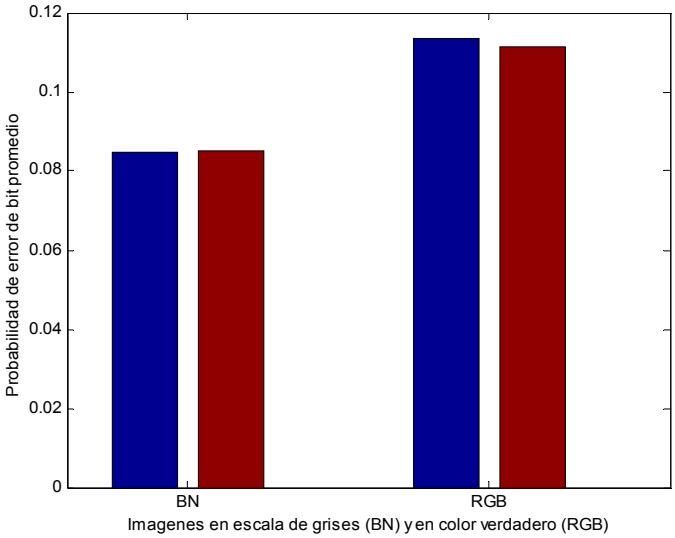


FIGURA V.3. Probabilidad de error de bit promedio frente al ataque FMLR. Para ambos métodos de detección e imágenes en color y en escala de grises. Algoritmo 1.

V.2.1.2Algoritmo 3

La figura V.4 ilustra el valor de las probabilidades de error de bit promedio obtenidas para las marcas de agua estimadas según los dos métodos de detección utilizados. En la tabla V.3 mostramos el valor promedio de la probabilidad de detección correcta de la marca de agua frente al ataque FMLR tanto para este algoritmo como para el anterior.

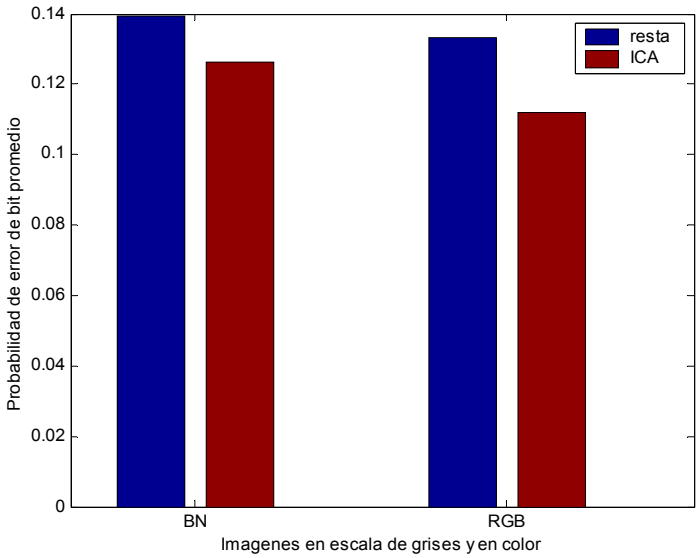


FIGURA V.4. Probabilidad de error de bit promedio frente al ataque FMLR. Para ambos métodos de detección e imágenes en color y en escala de grises. Algoritmo 3.

	ATAQUE FMLR	
Método de detección	**ALGORITMO 1 (DCT)**	**ALGORITMO 3 (DCT y DWT)**
Resta	1(0.82)	0.98 (0.82)
ICA	1(0.80)	0.98 (0.78)

TABLA V.3. Probabilidad de detección correcta de marca de agua, resultados obtenidos para los algoritmos 1 y 3 en el caso de detección en imágenes marcadas en escala de grises y en color entre paréntesis.

V.2.2 Algoritmos 2 y 4

Valores de probabilidad de detección correcta frente al ataque FMLR en los algoritmos 2 y 4 se ilustran en la tabla V.5.

	ATAQUE FMLR	
Método de detección	**ALGORITMO 2**	**ALGORITMO 4**
Resta	0.98	0.9
ICA	0.98	0.9

TABLA V.5. Probabilidad de detección correcta obtenida frente al ataque FMLR. Para los dos métodos de detección propuestos en los algoritmos 2 y 4.

V.3 Ataque de borrado simétrico/asimétrico de filas y columnas

Se trata de un ataque que pretende eliminar la sincronización mediante la eliminación de un número reducido de filas y/o columnas en la imagen, seleccionadas de forma aleatoria. Las posibilidades implementadas en este tipo de ataque son las indicadas en el eje de abscisas de las figuras IV.4 y IV.5, (también indicadas en la tabla en la que se detallan todos los ataques realizados, véase capítulo 6, tabla 6.10).

La respuesta de los algoritmos implementados frente a este ataque de eliminación de la sincronización en el receptor es, en general, muy buena, se muestran los resultados obtenidos para todos ellos.

V.3.1 Algoritmos 1 y 3

V.3.1.1 Algoritmo 1

En el algoritmo 1 se observa que la imagen que mejor responde a este tipo de ataque es la conocida como *skyline_arch.jpg* (en ambos métodos de detección, pues muestran la misma tendencia, como se puede observar en figura V.4), que es una imagen con gran cantidad de bordes y texturas.

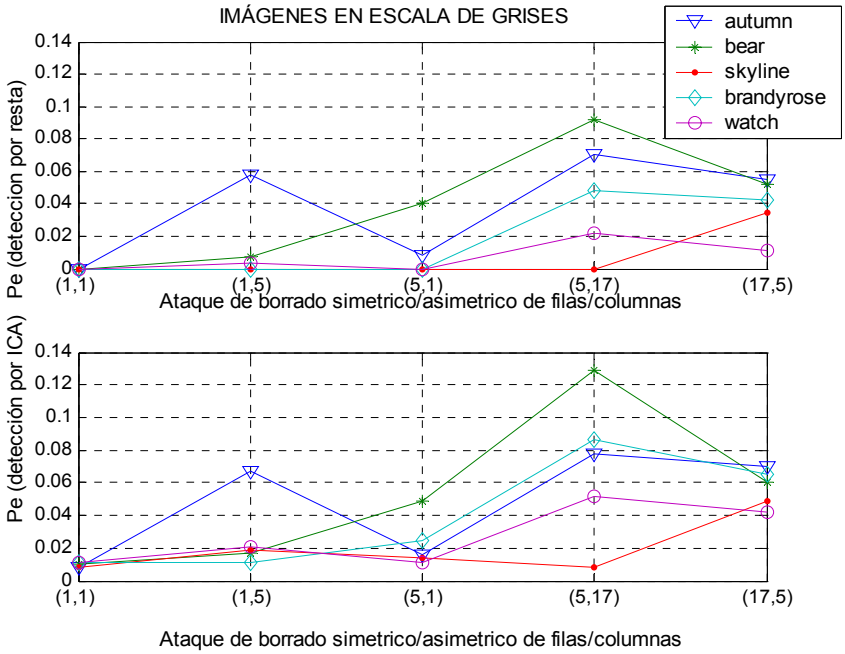


FIGURA V.4. Probabilidad de error de bit promedio para cada tipo de imagen frente al ataque de eliminación de sincronización por medio de borrado simétrico/asimétrico de filas/columnas. Para los dos mecanismos de detección empleados: detección por sustracción (figura superior) o mediante ICA (imagen inferior) en imágenes en escala de grises.

Valores de probabilidad de detección correcta muy cercana a la unidad para todos los ataques de borrado especificados, para los dos métodos de detección propuestos.

V.3.1.2 Algoritmo 3

Los resultados obtenidos se ilustran en la figura V.5, en la que se observa, al igual que para el algoritmo anterior, una excelente respuesta para las estimas recuperadas en la imagen skyline_arch.jpg., así como una tendencia similar en las respuestas de las diferentes imágenes frente al ataque de

eliminación de la sincronización, aunque los valores obtenidos para las probabilidades de error son algo superiores a los del algoritmo 1.

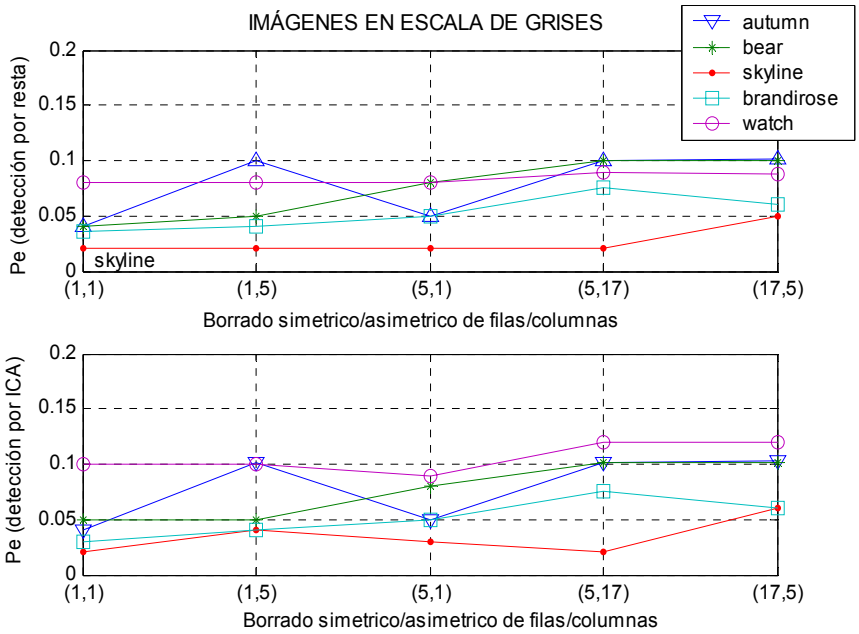


FIGURA V.5. Valores de probabilidad de error de bits obtenida en el algoritmo 3 para cada tipo de imagen y grado del ataque, para ambos métodos de detección estudiados, en imágenes en escala de grises.

Valores de probabilidades de detección correcta globales cercanos a la unidad, obtenidas para ambos métodos de detección.

Obsérvese que aunque las probabilidades de error, son, en general, superiores a las obtenidas en la figura V.4 (correspondiente al algoritmo 1), la distancia entre los valores obtenidos mediante detección por ICA y por resta se reduce (prácticamente se anula).

V.3.2 Algoritmos 2 y 4

Se observan valores de probabilidades de detección correcta cercanos a la unidad. Véase tabla V.6, en la que puede verse que el algoritmo que mejor responde a este ataque es el que combina el uso de las transformadas Wavelet y DCT. Los valores mostrados se refieren a imágenes en escala de grises, para las versiones marcadas en color se observan resultados algo inferiores pero muy similares.

ALGORITMO 2 (Dominio DCT de la imagen)						
Método de detección	**BORRADO DE FILAS/COLUMNAS**					**Valor promedio de detección**
	(1,1)	(1,5)	(5,1)	(5,17)	(17,5)	
Sustracción directa	1	1	0.90	0.95	1	0.97
ICA	1	1	0.90	0.95	1	0.97
ALGORITMO 4 (Dominio DWT y DCT de la imagen)						
Método de detección	**BORRADO DE FILAS/COLUMNAS**					**Valor promedio de detección**
	(1,1)	(1,5)	(5,1)	(5,17)	(17,5)	
Sustracción directa	1	1	1	1	1	1
ICA	1	1	1	1	1	1

TABLA V.6. Probabilidades de detección correcta en función de la fortaleza del ataque de borrado aleatorio de filas y/o columnas en la imagen, según los dos métodos de detección estudiados y para los algoritmos 1 y 3. En el caso de imágenes en escala de grises.

V.4 Ataque de desplazamiento lineal general

En este ataque se lleva a cabo un ligero desplazamiento a lo largo y ancho de la imagen además de una compresión JPEG de la imagen transformada con un valor del factor de calidad de noventa. En general, los algoritmos implementados no presentan buenos resultados frente a este procesado, no observándose un porcentaje global de detección aceptable.

V.4.1 Algoritmos 1 y 3

En ambos algoritmos, se observa detección apreciable (para ciertos parámetros del ataque) sólo en el caso de que la imagen bajo estudio sea la referida como *wach.jpeg.* Por lo que resulta un ataque muy efectivo en el sentido en que provoca la caída de la detección sin alterar demasiado la calidad de la imagen.


(a)

(b)

(c)

FIGURA V.6. Imagen "watch.jpg", la única que resiste en cierta medida al ataque implementado de desplazamiento lineal en ambas dimensiones de la imagen. Imagen (a) resultado de realizar el ataque con parámetros (a,b,c,d)= (1.013, 0.008, 0.011, 1.008). En la imagen (b) los parámetros del ataque son (a,b,c,d)= (1.010,0.013, 0.009, 1.011) y (c) (a,b,c,d)=(1.007, 0.010, 0.010, 1.012). El significado de los parámetros (a,b,c,d) se indica en la tabla 6.22. Las imágenes mostradas se corresponden con imágenes marcadas según características del algoritmo 1.

V.4.2 Algoritmos 2 y 4

Los resultados obtenidos muestran una menor efectividad del ataque en las imágenes marcadas según las características de los algoritmos 2 y 4 (con respecto a las marcadas según los algoritmos 1 y 3), no obstante, los resultados siguen siendo poco alentadores. En la tabla V.7 ilustramos los valores de probabilidades de detección correcta determinados en función de la especificación del ataque y en general.

En el algoritmo 2 se observa que para la imagen *watch.jpeg* hay un 100% de detección correcta.

ALGORITMO 2 (Dominio DCT de la imagen)				
Método de detección	**ATAQUE DESPLAZAMIENTO LINEAL**			**Valor promedio de detección**
	A	B	C	
Sustracción directa	0.40	0.35	0.50	0.42
ICA	0.40	0.33	0.50	0.41

ALGORITMO 4 (Dominio DWT y DCT de la imagen)				
Método de detección	**ATAQUE DESPLAZAMIENTO LINEAL**			**Valor promedio de detección**
	A	B	C	
Sustracción directa	0.33	0.33	0.46	0.38
ICA	0.33	0.33	0.46	0.38

TABLA V.7. Valores de probabilidad de detección correcta frente al ataque de desplazamiento lineal realizado a la imagen en los algoritmos 2 y 4. Donde A, B y C se refieren al grado de fortaleza del ataque. Es decir a los valores de los parámetros (a,b,c,d) de la tabla 6.10 del capítulo 6, con A: (a.b.c.d)=(1.007, 0.010,0.010,1.012), B: (a,b,c,d)= (1.010,0.013,0.009,1.011) y C: (a,b,c,d)= (1.013,0.008,0.011,1.008).

V.5 Ataque de cambio en la relación de aspecto

Los resultados obtenidos, para ambos métodos de detección usados e imágenes en escala de grises y en color, muestran una muy buena respuesta las técnicas de sellado invisible estudiadas frente a ataques que cambian la relación existente entre las dos dimensiones de la imagen (anchura y altura) marcada.

V.5.1 Algoritmos 1 y 3

V.5.1.1Algoritmo1

La figura V.7 muestra los resultados obtenidos frente al ataque de cambio en la relación de aspecto. Se observa la mínima (prácticamente nula) efectividad de este ataque en el algoritmo bajo estudio.

V.5.1.2Algoritmo 3

También se muestran los resultados de detección del algoritmo 3 (figura V.8), en los que se observa un aumento en los valores de probabilidades de error de bit con respecto a los obtenidos para el algoritmo1, así como una mejor respuesta del método ICA frente al de sustracción directa de la imagen original a la atacada. En el eje de abscisas se representan los diferentes valores asignados al ataque, véanse equivalencias en figura V.7.

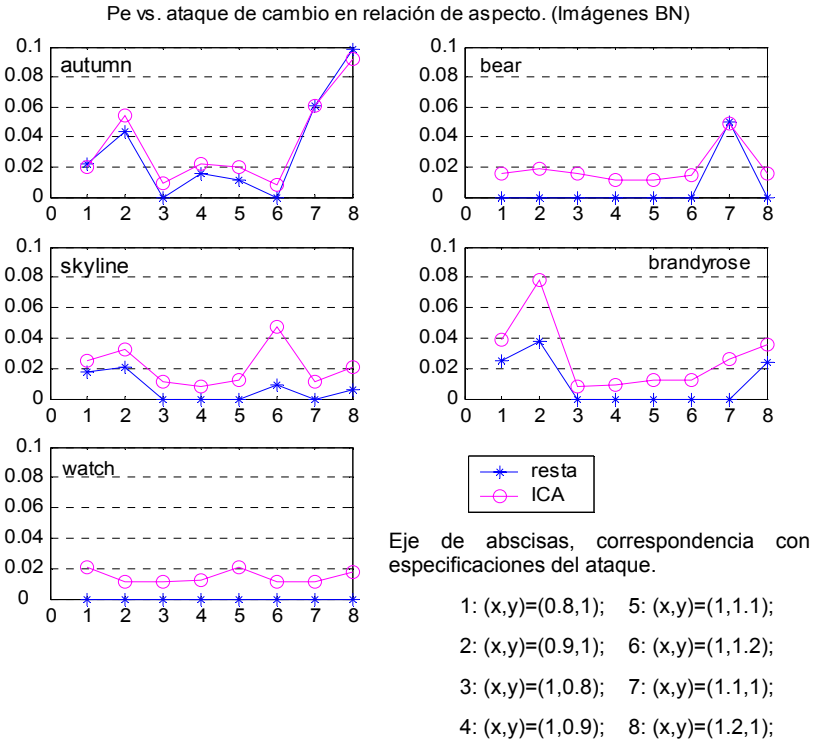


FIGURA V.7. Probabilidad de error de bit según especificación del ataque de modificación de la relación de aspecto. Mostrado según las diferentes imágenes estudiadas y método de detección usado. Resultados de la detección en imágenes en escala de grises, tendencias similares en imágenes en color. Algoritmo1.

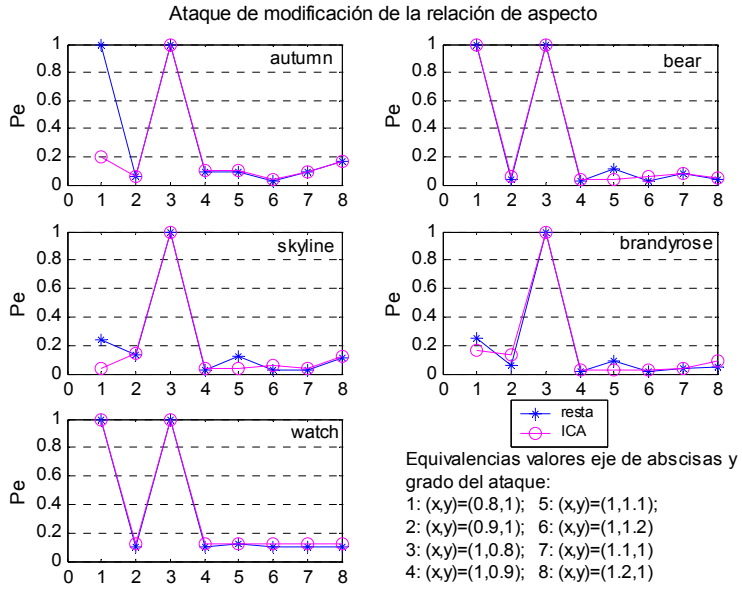


FIGURA V.8. Idem IV.7 para el algoritmo 3.

En la tabla V.8 se muestran las probabilidades de detección correcta de la marca de agua para ambos algoritmos, en general y según el grado o especificación del ataque. Se observa la excelente característica de detección

del algoritmo 1 frente a este tipo de ataque. El algoritmo 3 presenta ciertas debilidades frente a los ataques de especificaciones *(x,y)=(0.8,1) y (x,y)=(1,0.8),* con respuestas muy parecidas en todas las imágenes atacadas.

ALGORITMO 1 (Dominio DCT de la imagen)

Método de detección	CAMBIO EN RELACIÓN DE ASPECTO								Valor promedio detección
	(0.8,1)	(0.9,1)	(1,0.8)	(1,0.9)	(1,1.1)	(1,1.2)	(1.1,1)	(1.2,1)	
Sustracción directa	1	1	1	1	1	1	1	1	1
ICA	1	1	1	1	1	1	1	1	1

ALGORITMO 3 (Dominio DWT y DCT de la imagen)

Método de detección	CAMBIO EN RELACIÓN DE ASPECTO								Valor promedio detección
	(0.8,1)	(0.9,1)	(1,0.8)	(1,0.9)	(1,1.1)	(1,1.2)	(1.1,1)	(1.2,1)	
Sustracción directa	0.05	0.95	0	1	0.9	1	1	1	0.74
ICA	0.35	0.85	0	1	1	1	1	1	0.78

TABLA V.8. Probabilidades de detección correcta frente al ataque de cambio en la relación de aspecto de la imagen en escala de grises (en color valores semejantes), mostradas según mecanismo de detección usado y para los algoritmos 1 y 3.

En el algoritmo 3 puede observarse cierta mejora en la probabilidad de detección correcta obtenida mediante ICA, incluso, en ciertas situaciones, sólo se detecta la marca de agua mediante este mecanismo de estimación de marcas de agua. Véase en figura V.8 la gráfica correspondiente a la imagen *autumn.tif* para observar lo indicado.

V.5.2 Algoritmos 2 y 4

Los algoritmos que hacen uso de técnicas de espectro expandido en la generación de la marca de agua presentan detección en todas las imágenes procesadas y probabilidades de error nulas en las estimaciones obtenidas en ambos métodos de detección, aspecto, este último ya señalado con anterioridad. En la siguiente tabla se ilustra lo indicado.

ALGORITMO 2 (Dominio DCT de la imagen)

Método de detección	CAMBIO EN RELACIÓN DE ASPECTO								Valor promedio detección
	(0.8,1)	(0.9,1)	(1,0.8)	(1,0.9)	(1,1.1)	(1,1.2)	(1.1,1)	(1.2,1)	
Sustracción directa	0.98	0.95	0.98	0.98	0.98	0.98	0.98	0.95	0.97
ICA	0.98	0.95	0.98	0.98	0.98	0.98	0.98	0.95	0.97

ALGORITMO 4 (Dominio DWT y DCT de la imagen)

Método de detección	CAMBIO EN RELACIÓN DE ASPECTO								Valor promedio detección
	(0.8,1)	(0.9,1)	(1,0.8)	(1,0.9)	(1,1.1)	(1,1.2)	(1.1,1)	(1.2,1)	
Sustracción directa	1	1	1	1	1	1	1	1	1
ICA	1	1	1	1	1	1	1	1	1

TABLA V.9. Probabilidad de detección correcta, según algoritmo estudiado (algoritmos 2 y 4) y método de detección (resta e ICA) para todos los grados del ataque de cambio en la relación de aspecto y en general.

V.6 Ataque de rotación de la imagen

Dentro de este tipo de ataques consideramos los de rotación de la imagen por un ángulo pequeño, tanto positivo como negativo, así como por un ángulo grande positivo. Asimismo, se considera la posibilidad de escalar la imagen resultado de la rotación a las dimensiones de la original o no. De la observación de los resultados obtenidos, se comprueba que, en general, los algoritmos implementados responden de un modo aceptable para rotaciones de la imagen en torno a un grado (sea positivo o negativo). Para ángulos grandes de rotación existe detección sólo en casos excepcionales por lo que no los mostramos. Ilustramos sólo aquellos resultados para los que hay cierto valor de detección correcta apreciable.

V.6.1 Algoritmos 1 y 3

En la tabla siguiente se muestran los probabilidades de detección correcta frente a ataque de rotación positiva (hasta 0.75º) y cortado de la imagen, con la opción de escalado a las dimensiones originales (valores entre paréntesis) o no (resto de valores), para los algoritmos 1 y 3.

ALGORITMO 1 (Dominio DCT de la imagen)				
Método de detección	**ROTACIÓN POSITIVA (ESCALADO)**			**Valor promedio de detección**
	0.25º	0.50º	0.75º	
Sustracción directa	0.96 (1)	0.72(0.44)	0.28(0.26)	0.65 (0.57)
ICA	0.90(1)	0.72(0.46)	0.32(0.32)	0.65(0.60)
ALGORITMO 3 (Dominio DWT y DCT de la imagen)				
Método de detección	**ROTACIÓN POSITIVA (ESCALADO)**			**Valor promedio de detección**
	0.25º	0.50º	0.75º	
Sustracción directa	0.64 (0.76)	0.70 (0.34)	0.26 (0.20)	0.53 (0.43)
ICA	0.62 (0.70)	0.64 (0.36)	0.22 (0.18)	0.50 (0.41)

TABLA V.10. Probabilidad de detección correcta frente a ataque de rotación de la imagen por un ángulo positivo y pequeño, en los algoritmos 1 y 3 y según ambos métodos de detección. Opción de escalado a las dimensiones de la imagen original entre paréntesis.

ALGORITMO 1 (Dominio DCT de la imagen)				
Método de detección	**ROTACIÓN NEGATIVA (ESCALADO)**			**Valor promedio de detección**
	0.25º	0.50º	0.75º	
Sustracción directa	0.94 (1)	0.64 (0.56)	0.24 (0.24)	0.61 (0.6)
ICA	0.94 (1)	0.64 (0.42)	0.24 (0.1)	0.61 (0.51)
ALGORITMO 3 (Dominio DWT y DCT de la imagen)				
Método de detección	**ROTACIÓN NEGATIVA (ESCALADO)**			**Valor promedio de detección**
	0.25º	0.50º	0.75º	
Sustracción directa	0.66 (0.78)	0.68 (0.38)	0.28 (0.1)	0.53(0.42)
ICA	0.64 (0.74)	0.60 (0.26)	0.24 (0.1)	0.49(0.37)

TABLA V.11. Probabilidad de detección correcta frente a ataque de rotación de la imagen por un ángulo negativo y pequeño, en los algoritmos 1 y 3 y según ambos métodos de detección. Opción de escalado a las dimensiones de la imagen original entre paréntesis.

Para ángulos grandes se observa detección en casos aislados por lo que no se considera que exista detección correcta de marcas de agua en imágenes rotadas por ángulos mayores de un grado. Los valores obtenidos para las

probabilidades de error de bits en las estimaciones por resta y por ICA son, prácticamente idénticos, oscilando en el rango de valores (0.10, 0.20).

V.6.2 Algoritmos 2 y 4

Los valores de probabilidades de detección en los algoritmos 2 y 4 presentan cierta mejora frente a los obtenidos para los algoritmos 1 y 3, aún así siguen mostrando una gran debilidad de las técnicas de marcado estudiadas frente a rotaciones de las imágenes marcadas.

ALGORITMO 2 (Dominio DCT de la imagen)				
Método de detección	**ROTACIÓN POSITIVA (ESCALADO)**			**Valor promedio de detección**
	0.25º	0.50º	0.75º	
Sustracción directa	0.98(0.98)	0.90(0.88)	0.75(0.70)	0.88(0.85)
ICA	0.98(0.98)	0.90(0.88)	0.75(0.68)	0.88(0.85)
ALGORITMO 4 (Dominio DWT y DCT de la imagen)				
Método de detección	**ROTACIÓN POSITIVA (ESCALADO)**			**Valor promedio de detección**
	0.25º	0.50º	0.75º	
Sustracción directa	0.95 (0.95)	0.88 (0.80)	0.59 (0.56)	0.81 (0.77)
ICA	0.95 (0.95)	0.88 (0.80)	0.59 (0.56)	0.81 (0.77)

TABLA V.12. Probabilidad de detección correcta frente a ataque de rotación de la imagen por un ángulo positivo y pequeño, en los algoritmos 1 y 3 y según ambos métodos de detección. Opción de escalado a las dimensiones de la imagen original entre paréntesis.

ALGORITMO 2 (Dominio DCT de la imagen)				
Método de detección	**ROTACIÓN NEGATIVA (ESCALADO)**			**Valor promedio de detección**
	0.25º	0.50º	0.75º	
Sustracción directa	0.98(0.95)	0.93(0.88)	0.65(0.63)	0.86(0.82)
ICA	0.98(0.95)	0.93(0.88)	0.65(0.63)	0.86(0.82)

ALGORITMO 4 (Dominio DWT y DCT de la imagen)				
Método de detección	**ROTACIÓN NEGATIVA (ESCALADO)**			**Valor promedio de detección**
	0.25º	0.50º	0.75º	
Sustracción directa	0.95(0.98)	0.88 (0.90)	0.63 (0.64)	0.82 (0.84)
ICA	0.95(0.98)	0.90(0.88)	0.61(0.62)	0.82 (0.84)

TABLA V.13. Probabilidad de detección correcta frente a ataque de rotación de la imagen por un ángulo negativo y pequeño, en los algoritmos 1 y 3 y según ambos métodos de detección. Opción de escalado a las dimensiones de la imagen original entre paréntesis.

V.7 Ataque de escalado de la imagen

Mediante este ataque se amplía/reduce la imagen según un valor determinado del factor de escalado, manteniéndose intacta la relación de aspecto de la misma. En el proceso de detección/recuperación de la marca de agua frente a un ataque de este tipo se realiza un preprocesado básico de la imagen mediante su ampliación o reducción a las dimensiones originales. Se muestran los resultados obtenidos para la probabilidad de error de bits promedio de las marcas de agua estimadas tanto por resta como por ICA y para imágenes en escala de grises y en color, en los procesos de detección de los algoritmos 1 y 3, así como los valores promedio de probabilidad de detección correcta para todos los algoritmos estudiados.

V.7.1 Algoritmos 1 y 3

En la figuras de la página siguiente (figuras V.9 y V.10) se muestran los resultados obtenidos para las probabilidades de error de bits en las marcas de agua recuperadas según las características de los algoritmos 1 y 3. En ellas se observan ciertos aspectos interesantes. Por un lado, se aprecia una ligera diferencia entre los valores obtenidos en el algoritmo 1 por resta y por ICA, (siendo algo mayor la Pe de las estimaciones mediante ICA, en imágenes en escala de grises), lo que no ocurre en el algoritmo 3, en el que los valores obtenidos mediante los dos métodos de detección, (si bien son ligeramente superiores a sus homólogos del algoritmo 1) son idénticos o algo menores para las estimaciones por ICA. Aspecto éste que se repite en muchos de los resultados obtenidos hasta el momento y que nos hace pensar que la combinación DWT e ICA pueda resultar interesante.

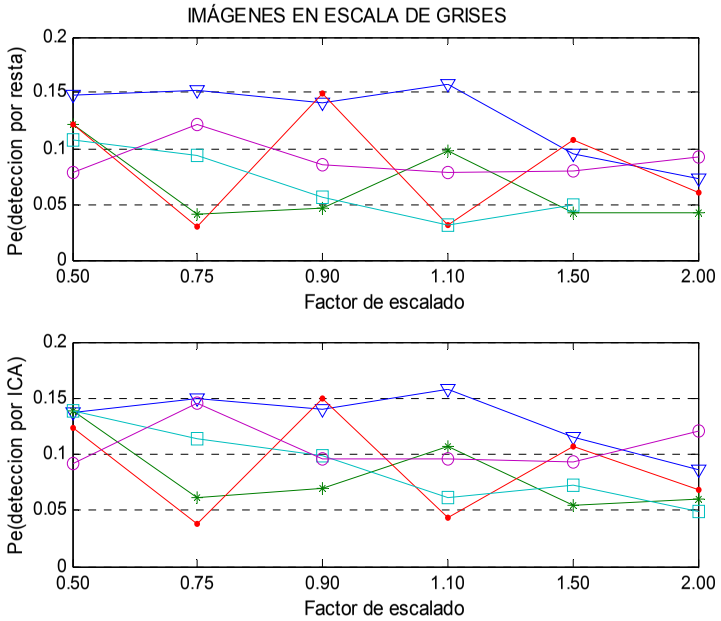
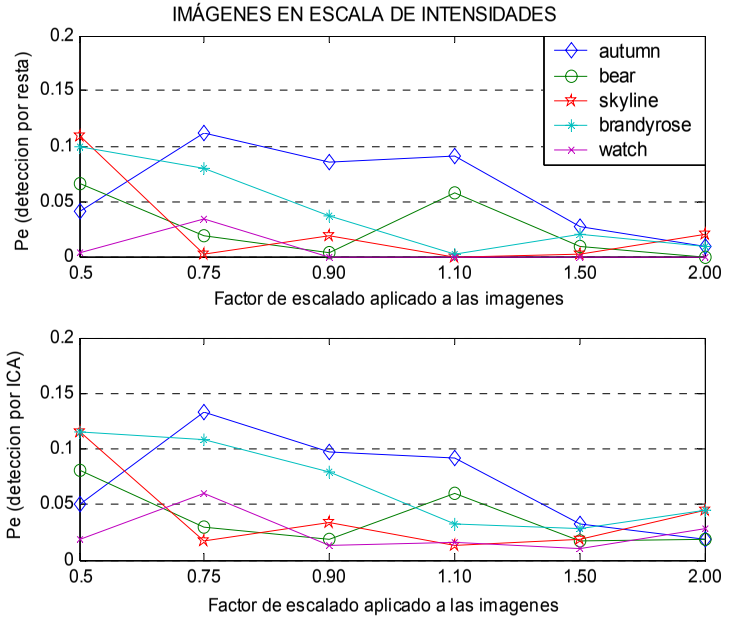


FIGURA V.9. Probabilidades de error de bits según imagen y fortaleza del ataque de escalado, para imágenes en escala de grises (figura superior) y en color RGB (figura superior). Resultados obtenidos en el algoritmo 1.



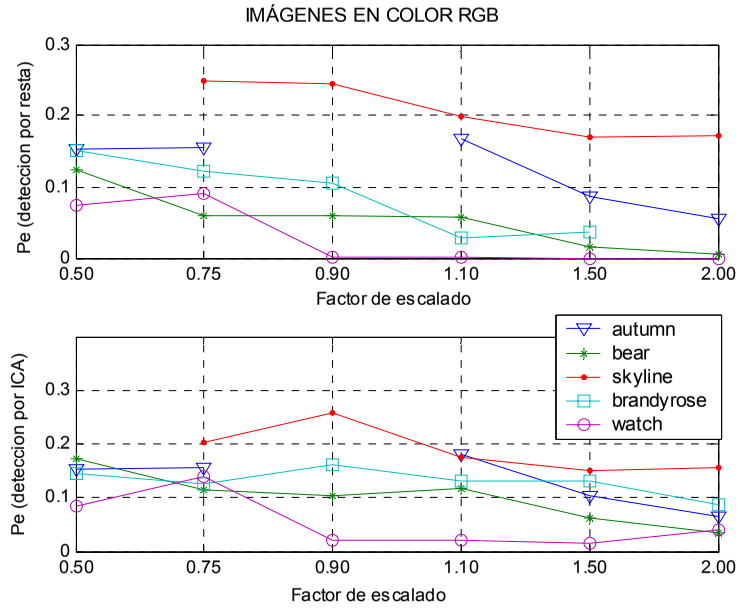
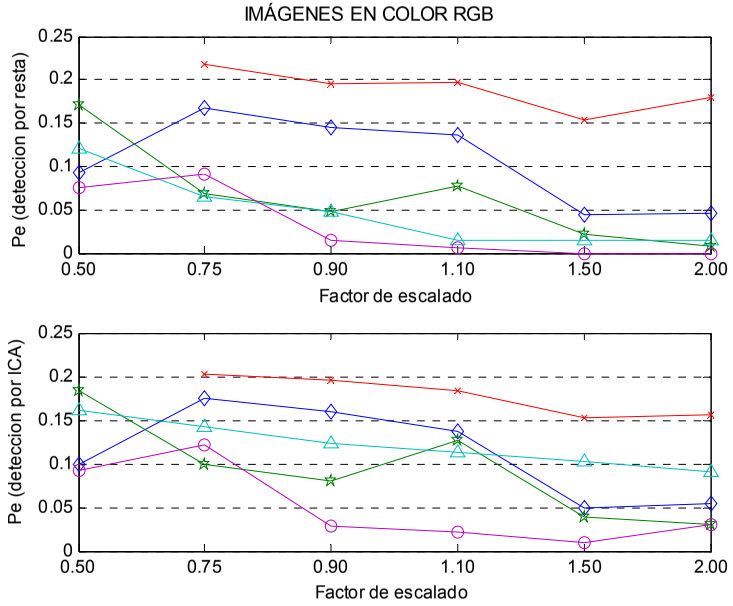


FIGURA V.10. Idem V.9, pero resultados obtenidos en el algoritmo 3.



Los valores de probabilidades de detección para ambos algoritmos se muestran en la siguiente tabla.

ALGORITMO 1 (Dominio DCT de la imagen)

Método de detección	ATAQUE DE ESCALADO DE LA IMAGEN						Valor promedio de detección
	0.50	0.75	0.90	1.10	1.50	2	
Sustracción directa	0.98	1	1	1	1	1	0.996 (0.87)
ICA	0.98	0.98	1	1	1	1	0.993 (0.84)

ALGORITMO 3 (Dominio DWT y DCT de la imagen)

Método de detección	ATAQUE DE ESCALADO DE LA IMAGEN						Valor promedio de detección
	0.50	0.75	0.90	1.10	1.50	2	
Sustracción directa	0.90 (0.76)	0.94 (0.68)	0.8 (0.66)	0.96 (0.80)	0.98 (0.92)	0.9 (0.70)	0.92 (0.75)
ICA	0.82 (0.60)	0.82 (0.62)	0.72 (0.52)	0.96 (0.86)	1 (0.96)	1 (0.86)	0.89 (0.74)

TABLA V.13. Valor de probabilidades de detección correcta promedio general y en función del grado de escalado aplicado a la imagen. Mostrados para los algoritmos 1 y 3 en imágenes de escala de grises (entre paréntesis valores de detección para imágenes en color RGB).

Se aprecia cómo ICA funciona mejor frente a ataques de escalado de aumento de la imagen.

V.7.2 Algoritmos 2 y 4

La tabla V.14 muestra los resultados obtenidos para los algoritmos 2 y 4, se observa una excelente respuesta en ambos métodos frente al ataque de escalado de la imagen, ya sea de aumento o reducción de la misma.

ALGORITMO 2 (Dominio DCT de la imagen)

Método de detección	ATAQUE DE ESCALADO DE LA IMAGEN						Valor promedio de detección
	0.50	0.75	0.90	1.10	1.50	2.00	
Sustracción directa	0.98	0.98	0.95	0.98	0.98	0.98	0.98
ICA	0.98	0.98	0.95	0.98	0.98	0.98	0.98

ALGORITMO 4 (Dominio DWT y DCT de la imagen)							
Método de detección	**ATAQUE DE ESCALADO DE LA IMAGEN**						**Valor promedio de detección**
	0.50	0.75	0.90	1.10	1.50	2	
Sustracción directa	1	0.98	0.95	1	1	1	0.99
ICA	1	0.98	0.95	1	1	1	0.99

TABLA V.14. Resultados de probabilidades de detección correcta obtenidos para los algoritmos 2 y 4, mostrados en el caso de imágenes en escala de grises, pues las imágenes en color muestran la misma respuesta frente a este ataque de escalado.

V.8 Ataque shearing

Las técnicas de sellado invisible implementadas no responden demasiado bien frente a ataques de tipo shearing. Este ataque consiste en aplicar un cierto desplazamiento en uno de los ejes de la imagen o en los dos. Las posibilidades de ataque realizadas son*; (0,1), (0,5) (1, 0), (5, 0), (1, 1) y (5, 5)*. La primera componente marca el desplazamiento en la dirección X (porcentaje del ancho) y la segunda el desplazamiento en la dirección Y (porcentaje de la altura).

V.8.1 Algoritmos 1 y 3

V.8.1.1 Algoritmo 1

El porcentaje de detecciones correctas se reduce con respecto a otros resultados, siendo, aproximadamente, de un 50%. Además existe una notoria diferencia entre los resultados obtenidos según la imagen bajo estudio, observándose que la única imagen en la que se consiguen probabilidades de detección elevadas para cualquier grado de severidad del ataque realizado es, de nuevo, la imagen *watch.jpg,* seguida de *brandyrose.jpg*. En la figura V.11 se ilustran los resultados (probabilidades de error de bits) según el tipo de imagen y método de detección, notar que sólo se muestran aquellos casos en los que existe detección correcta y que únicamente frente al ataque especificado como $x=1,y=0$ existe detección en todas las imágenes. Es decir, este ataque es el que resulta menos efectivo.

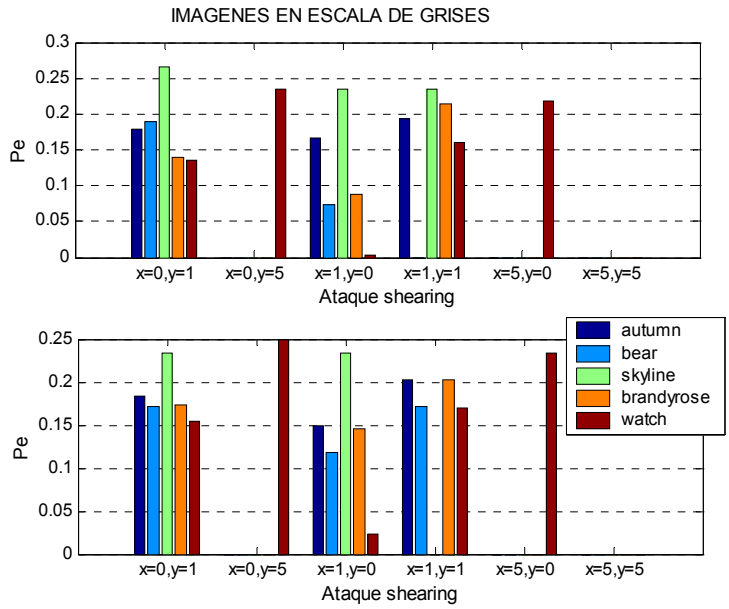


FIGURA V.11. Probabilidades de error de bit frente a distintos tipos de ataque shearing. La figura de arriba es para estimaciones obtenidas por resta mientras que la inferior muestra el mismo resultado para estimaciones a partir de ICA. Notar que las barras no mostradas se corresponden con las imágenes para las que no se consigue la detección correcta de la marca de agua. Algoritmo 1.

V.8.1.2 Algoritmo 3

Los resultados obtenidos en este algoritmo muestran que la técnica de inserción implementada no resulta tan robusta como sería deseable frente a este tipo de ataque. En general, la probabilidad de detección de la marca de agua insertada en las imágenes que han sufrido un ataque de este tipo, es prácticamente nula salvo en el caso del ataque shearing en el que solo se modifica el eje X (ataque clasificado como $(1,0)$)en el que el porcentaje de detección correcta está en torno al 80% (tanto por sustracción como por ICA) y la probabilidad de error de bit media se alza a un valor promedio de 0.1240 para el caso de detección por resta y 0.1246 para la detección por ICA. En cuanto a las imágenes, la que mejores características presenta frente a este tipo de ataque es *watch.jpeg* (al igual que en el algoritmo 1) para la que encontramos, además de gran robustez frente al ataque mencionado una probabilidad de detección en torno al 50% en los ataques clasificados como $(0,1)$ y $(1,1)$. La imagen 3 presenta mejores probabilidades de detección en el ataque $(0,1)$, (100% de detección frente a este ataque). Véase figura V.12.

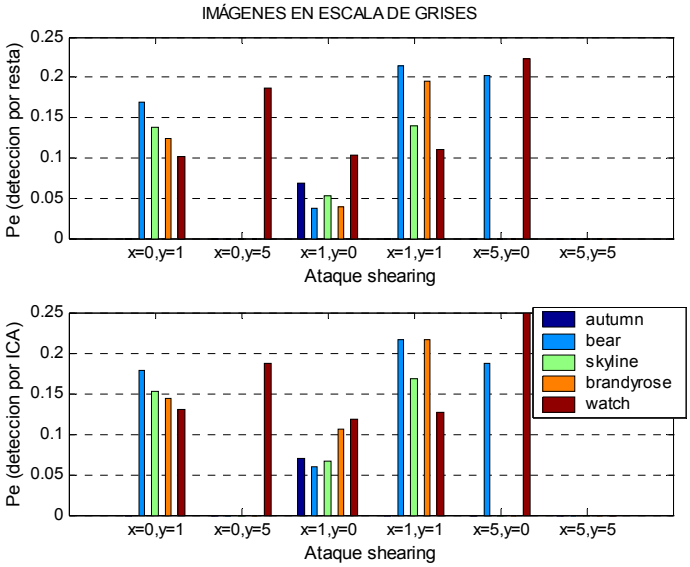


FIGURA V.12. Idem FIGURA V.11 para algoritmo 3. Los valores de detección obtenidos de promediar entre todos los tipos de ataques e imágenes, para resta e ICA, fueron:

Pd_resta=0.43

Pd_ica = 0.40

V.8.2 Algoritmos 2 y 4

El empleo de técnicas de espectro expandido en la generación de la marca de agua presenta cierta mejora, aunque poco significativa, en la respuesta de los algoritmos frente al ataque tipo shearing.

ALGORITMO 2 (Dominio DCT de la imagen)							
Método de detección	**ATAQUE SHEARING**						**Valor promedio de detección**
	(0,1)	(0,5)	(1,0)	(1,1)	(5,0)	(5,5)	
Sustracción directa	0.925	0	0.95	0.90	0	0	0.46
ICA	0.90	0	0.95	0.90	0	0	0.46
ALGORITMO 4 (Dominio DWT y DCT de la imagen)							
Método de detección	**ATAQUE SHEARING**						**Valor promedio de detección**
	(0,1)	(0,5)	(1,0)	(1,1)	(5,0)	(5,5)	
Sustracción directa	0.90	0	1	0.93	0	0	0.47
ICA	0.90	0	1	0.93	0	0	0.47

TABLA V.15. Valores promedio de detección correcta por ambos métodos de detección y para los algoritmos 2 y 4. Se muestran los resultados de la recuperación de las marcas de agua a partir de imágenes atacadas en escala de intensidad (las imágenes en color muestran una tendencia similar).

V.9 Ataque de filtrado gaussiano

Al aplicar un filtrado gaussiano a una imagen se está realizando un suavizado de la misma, dadas las características paso bajo del filtro empleado.

Los resultados obtenidos frente a este tipo de ataque, muestran, en general, una buena respuesta de las técnicas de sellado invisible implementadas.

V.9.1 Algoritmos 1 y 3

En las tablas V.16a y IV.16b mostramos los resultados, en cuanto a probabilidades de detección correcta y de error de bits, obtenidos en los procesos de detección de los algoritmos 1 y 3, en general.

ATAQUE FILTRADO GAUSSIANO			ATAQUE FILTRADO GAUSSIANO		
Método de detección	**ALGORITMO 1 (DCT) Pd**	**ALGORITMO 3 (DCT y DWT) Pd**	**Método de detección**	**ALGORITMO1 (DCT) Pe**	**ALGORITMO 3 (DCT y DWT) Pe**
Resta	1 (0.94)	0.98 (0.90)	**Resta**	0.018 (0.061)	0.067(0.052)
ICA	1 (0.96)	0.98 (0.90)	**ICA**	0.025(0.081)	0.075 (0.076)

FIGURA V.16a. Probabilidades de detección correcta para imágenes en escala de grises (en paréntesis para imágenes en color) y ambos métodos de detección

FIGURA V.16b. Probabilidades de error de bits de las marcas de agua estimadas según los dos métodos de detección usados para imágenes en escala de grises (en paréntesis para RGB)

V.9.2 Algoritmos 2 y 4

Los valores de detección correcta para los algoritmos que emplean técnicas de espectro expandido en la generación de las marcas de agua se muestran en la tabla V.17.

Se observa en la tabla una respuesta similar y excelente en ambos algoritmos estudiados frente al ataque de filtrado gaussiano de las imágenes marcadas.

ATAQUE FILTRADO GAUSSIANO		
Método de detección	**ALGORITMO 2 (DCT)**	**ALGORITMO 4 (DCT y DWT)**
Resta	0.95	1
ICA	0.95	1

FIGURA V.17. Probabilidades de detección correcta de las marcas de agua en los algoritmos 2 y 4.

V.10 Ataque de filtrado sharp

Cuando el ataque consiste en realizar un filtrado de mejora para aumentar el contraste de la imagen (como puede ser el efecto del filtro sharp utilizado), los resultados que se obtienen en la detección y recuperación de la marca de agua para cada uno de los algoritmos implementados se ilustran a continuación.

V.10.1 Algoritmos 1 y 3

El algoritmo 3 presenta detección baja frente al ataque de filtrado sharp de la imagen marcada, se puede comprobar que las imágenes selladas según las características de mencionado algoritmo que mejor responden al filtrado sharp son las conocidas como *bear.jpg* y *brandyrose.jpg* en las que las probabilidades de detección correcta son cercanas a la unidad para ambos métodos de detección. El algoritmo 1 presenta buenos resultados, en general.

ATAQUE FILTRADO SHARP		
Método de detección	**ALGORITMO 1 (DCT) Pd**	**ALGORITMO 3 (DCT y DWT) Pd**
Resta	0.90	0.60
ICA	0.80	0.58
ATAQUE FILTRADO SHARP		
Método de detección	**ALGORITMO 1 (DCT) Pe**	**ALGORITMO 3 (DCT y DWT) Pe**
Resta	0.1258	0.1578
ICA	0.1455	0.1765

TABLA V.18. Valores de probabilidades de detección correcta (arriba) y de error de bits (parte inferior) en los algoritmos 1 y 3, para los dos métodos de detección indicados e imágenes en escala de grises.

V.10.2 Algoritmos 2 y 4

De nuevo, el uso de técnicas de espectro expandido en la generación de las marcas de agua a insertar en la imagen, añaden información de redundancia a la imagen que permite que la detección suba un valor considerable con respecto a los resultados obtenidos en los algoritmos 1 y 3.

ATAQUE FILTRADO SHARP		
Método de detección	**ALGORITMO 2 (DCT)**	**ALGORITMO 4 (DCT y DWT)**
Resta	0.95	0.93
ICA	0.95	0.88

TABLA V.19. Valores de probabilidades de detección correcta en los algoritmos 2 y 4 para los dos métodos indicados.

V.11 Ataque stirmark

El proceso realizado a la imagen referido con el nombre *stirmark*, se realiza aplicando distorsiones geométricas locales no lineales a la imagen, tanto en su dimensión horizontal como vertical, e interpolando luego la misma, a la que además se le añade ruido y una pequeña compresión (con valor del factor de calidad de noventa), véase capítulo 3 de la primera parte y anexo III dedicado al banco de pruebas.

En general, las imágenes selladas que son atacadas con stirmark mantienen prácticamente intacta su calidad visual, es decir, no se aprecia modificación alguna en la imagen, sin embargo la pérdida de sincronización generada, provoca lo no detección de la marca de agua. Salvo en el caso de la imagen *watch.jpeg,* en la que la presencia de elementos de sincronización permite recuperar el sello con un porcentaje de aciertos notable. Se observa, pues, la dependencia entre la efectividad del ataque y las características de la imagen.

V.11.1 Algoritmos 1 y 3

Como se ha indicado, la imagen creada por ordenador *(watch.jpg)* es la que presenta mejores propiedades frente al ataque implementado bajo el nombre de stirmark, mostramos por tanto los valores de probabilidades de detección correcta y de error de bits obtenidas para la misma en los procesos de

detección de los algoritmos 1 y 3. Indicamos aquí que en las imágenes *brandyrose.jpg* y *bear.jpg* también se observa cierta detección, aunque poco significativa.

ATAQUE STIRMARK		
Método de detección	**ALGORITMO 1 (DCT)**	**ALGORITMO 3 (DCT y DWT)**
Resta	0.1163(0.90)	0.15 (0.6)
ICA	0.1563(0.80)	0.15 (0.6)

TABLA V.20. Valores de probabilidades de error de bits y de detección (entre paréntesis) correcta en los algoritmos 1 y 3 para los dos métodos de estimación de marcas de agua indicados. Valores obtenidos únicamente para la imagen *watch.jpg*

V.11.2 Algoritmos 2 y 4

Se observa, en general una pobre respuesta de los algoritmos bajo estudio frente a ataques de distorsión aleatoria como stirmark.

ATAQUE STIRMARK		
Método de detección	**ALGORITMO 2 (DCT)**	**ALGORITMO 4 (DCT y DWT)**
Resta	0.28	0.25
ICA	0.28	0.25

TABLA V.21. Valores de probabilidad de detección correcta promedio en los algoritmos 2 y 4 para los dos métodos indicados frente al ataque stirmark.

V.12 Ataque de compresión JPEG

Puesto que la técnica de inserción de la información escondida en la imagen se basa en el marcado de los coeficientes DCT más significativos, es lógico pensar, que los algoritmos propuestos deben funcionar bien frente a técnicas de compresión basadas en la transformada discreta del coseno, como es el caso de la compresión JPEG. Los resultados obtenidos corroboran este supuesto. Como puede apreciarse en las gráficas mostradas en esta sección.

V.12.1 Algoritmos 1 y 3

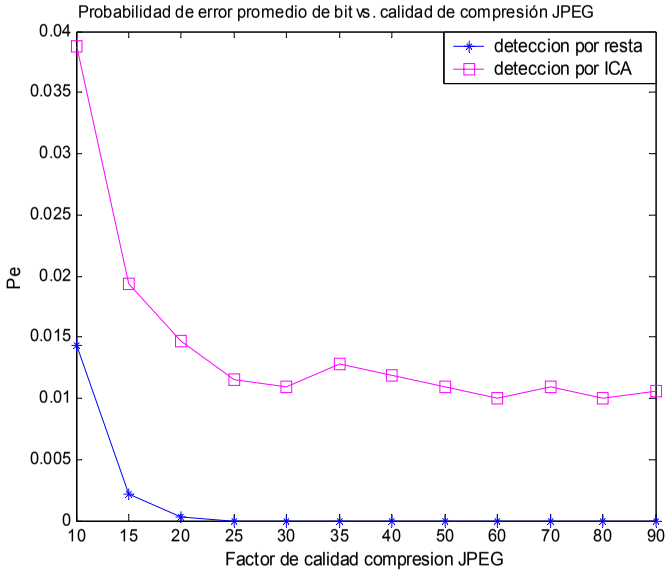
En las figuras V.13 y V.14 se muestran los valores de probabilidad de error de bits obtenidos en las marcas de agua recuperadas en el algoritmo 1. Los resultados de la técnica de watermarking implementada en el algoritmo 3 se muestran en la figura V.15. (Páginas siguientes).

V.12.2 Algoritmos 2 y 4

Valores de probabilidad de detección correcta obtenidos en los algoritmos 2 y 4, muestran las excelentes características de los algoritmos implementados, en particular el algoritmo 4, en el que se observa una probabilidad de detección correcta de valor unidad incluso para imágenes comprimidas con factor de calidad diez.

ALGORITMO 2 (Pd promedio de 0.95)												
METODO DE DETECCIÓN	FACTOR DE CALIDAD DE COMPRESIÓN JPEG											
	10	15	20	25	30	35	40	50	60	70	80	90
RESTA	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95
ICA	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95
ALGORITMO 4 (Pd promedio de 1)												
METODO DE DETECCIÓN	FACTOR DE CALIDAD DE COMPRESIÓN JPEG											
	10	15	20	25	30	35	40	50	60	70	80	90
RESTA	1	1	1	1	1	1	1	1	1	1	1	1
ICA	1	1	1	1	1	1	1	1	1	1	1	1

TABLA V.21. Probabilidad de detección correcta frente a ataque de compresión JPEG, según diferentes factores de compresión (referidos según factor de calidad de la imagen comprimida) y en general. Algoritmos 2 y 4.



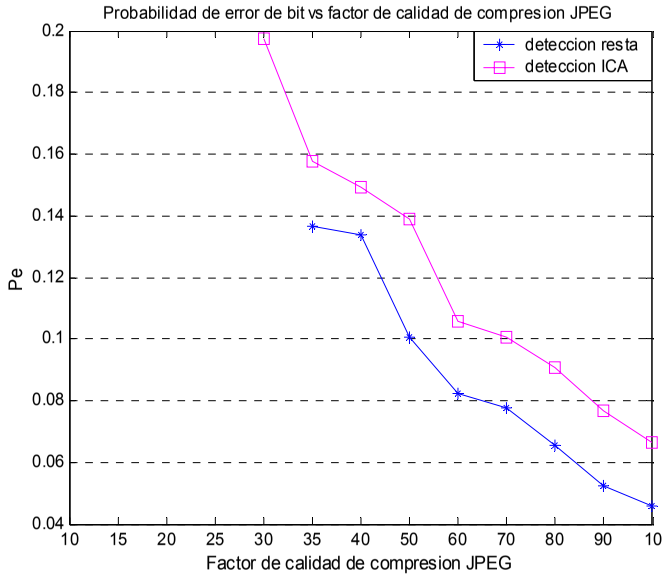
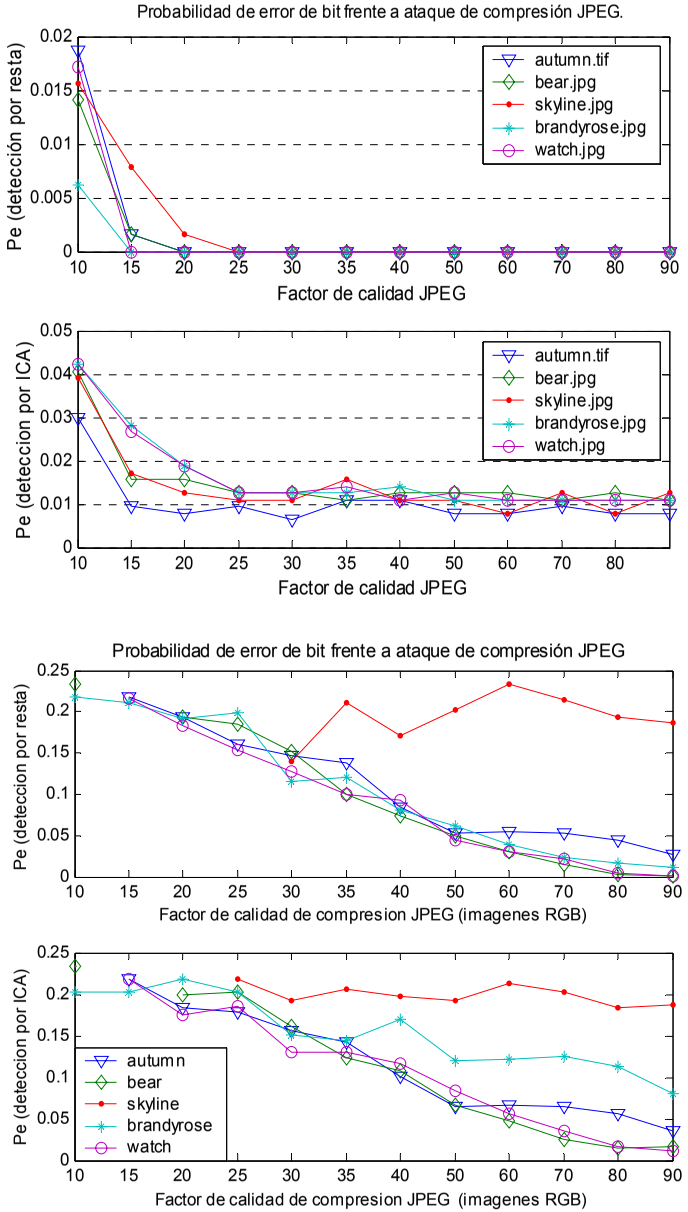


FIGURA V.13 (figura de la derecha). Probabilidad de error de bit obtenida para según tipo de imagen y factor de compresión. Para imágenes selladas y atacadas en escala de grises (gráfica superior derecha) y en color RGB (inferior derecha).

FIGURA V.14 (figura de la izquierda). Probabilidad de error de bit genérica en función del factor de compresión utilizado. Para imágenes en escala de grises (gráfica superior) y en color RGB (gráfica inferior) .



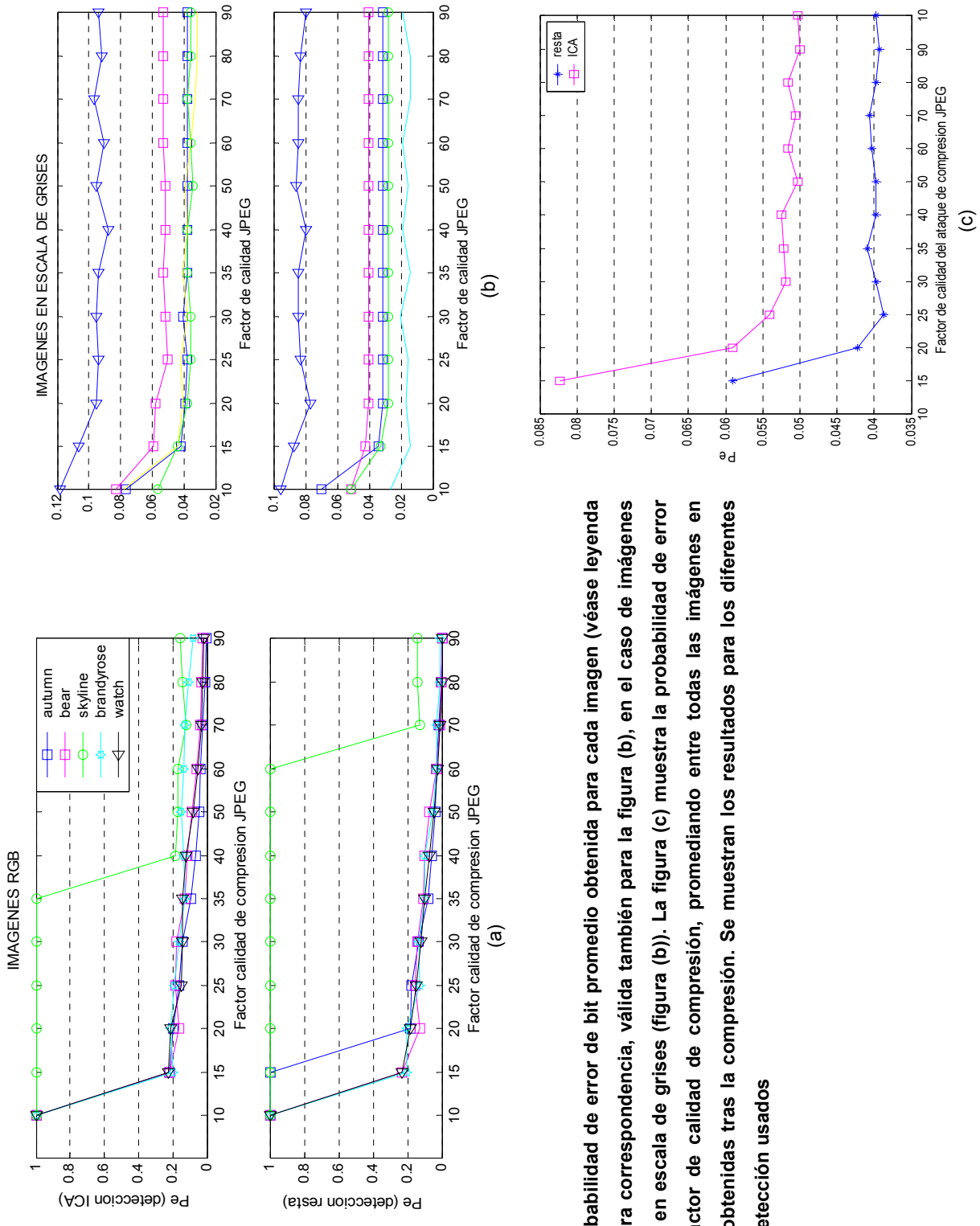


FIGURA V.15. Probabilidad de error de bit promedio obtenida para cada imagen (véase leyenda de la figura (a) para correspondencia, válida también para la figura (b), en el caso de imágenes RGB (figura (a)) y en escala de grises (figura (b)). La figura (c) muestra la probabilidad de error en función del factor de calidad de compresión, promediando entre todas las imágenes en escala de grises obtenidas tras la compresión. Se muestran los resultados para los diferentes mecanismos de detección usados

V.13 Ataque de cortado de parte de la imagen

Al igual que frente al ataque de escalado, antes de la detección de la marca de agua en la imagen atacada, se ajustan las dimensiones de ésta a las de la original mediante la adición de la zona eliminada de la imagen cortada a partir de la versión sin marcar. Un ejemplo del proceso puede verse en la figura V.16.

Los resultados obtenidos, (para las probabilidades de error de bit y de detección correcta) frente a los diferentes grados de dureza del ataque de cortado implementado se ilustran en las figuras que se adjuntan según el algoritmo de que se trate. En ellas se observan tendencias similares en los resultados obtenidos mediante los dos métodos de recuperación de marcas de agua estudiados (resta e ICA).

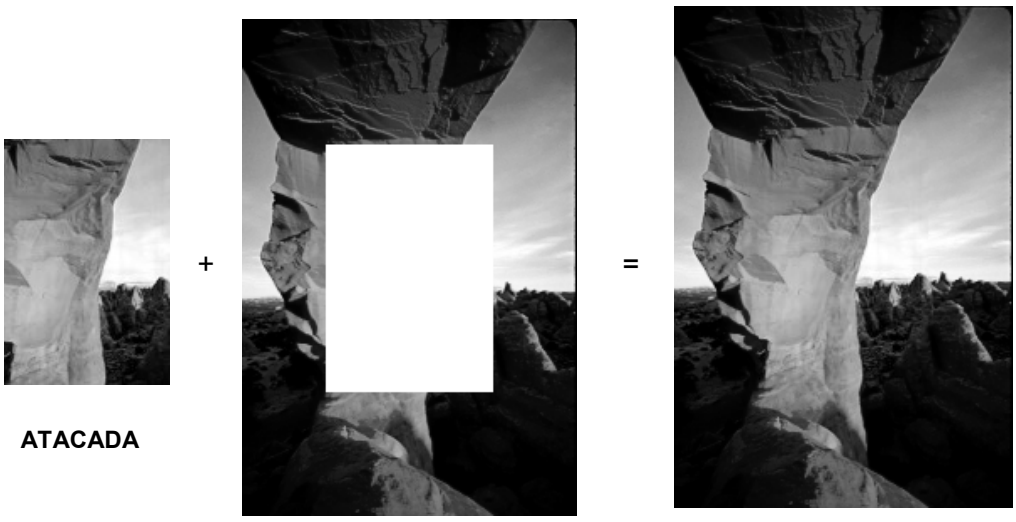


FIGURA V.16. Proceso de ajuste de dimensiones de la imagen cortada a partir de la imagen original.

V.13.1 Algoritmos 1 y 3

Mostramos los resultados obtenidos en los procesos de detección llevados a cabo en los algoritmos 1 y 3.

V.13.1.1 Algoritmo 1

Las figuras V.17 y V.18 muestran los resultados obtenidos de detección correcta y de probabilidad de error de bits en función de la imagen de que trate y del porcentaje de cortado de la imagen. Se observa que los valores de detección correcta son bastante buenos para porcentajes de cortado inferiores al cincuenta por ciento de la imagen, punto en el que empieza a degradarse de forma notoria la posibilidad de detectar correctamente la marca de agua. Asimismo se puede ver que las imágenes que mejor responden a este ataque de eliminación o borrado de la marca de agua son, por orden de mención, *brandyrose.jpg, watch.jpg, skyline.jpg y bear.jpg.* Notar además que se observan valores de detección correcta mejores en la detección por resta. La figura V.18 trata de ilustrar que los resultados obtenidos para las probabilidades de error de bits de las estimaciones por resta y por ICA son, prácticamente, idénticos.

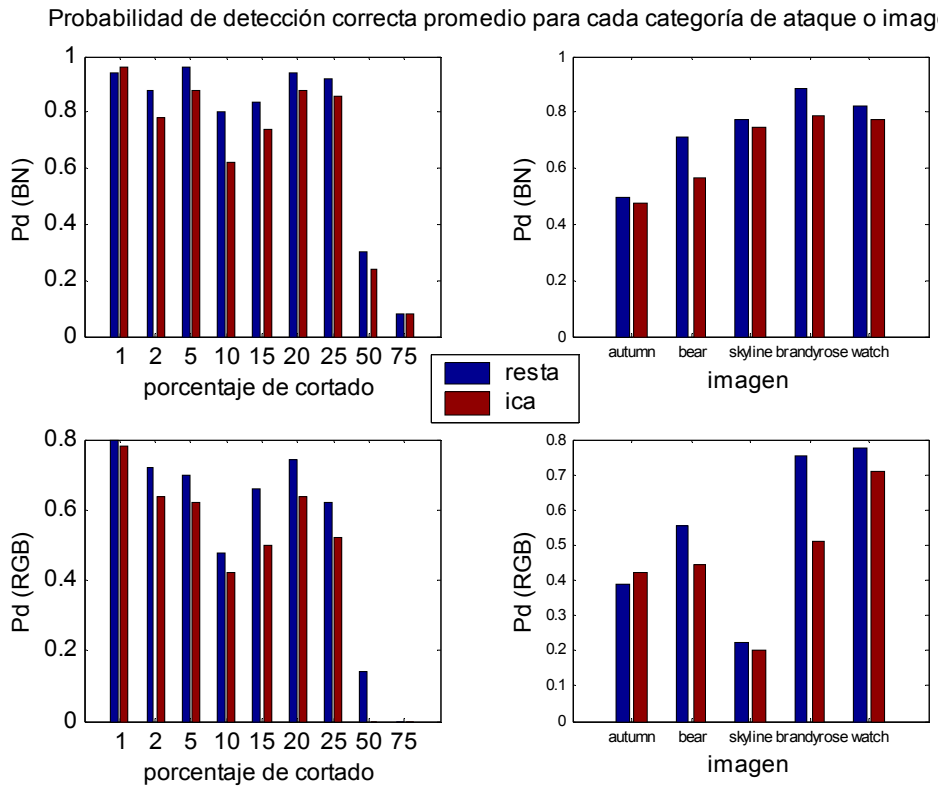


FIGURA V.17. Probabilidad de detección correcta promedio para imágenes en escala de intensidades (par de graficas superior) y de color RGB (par de gráficas inferior). Mostrada para los diferentes grados de severidad del ataque de cortado (figuras de la izquierda) o para las diferentes imágenes (gráficas de la derecha).

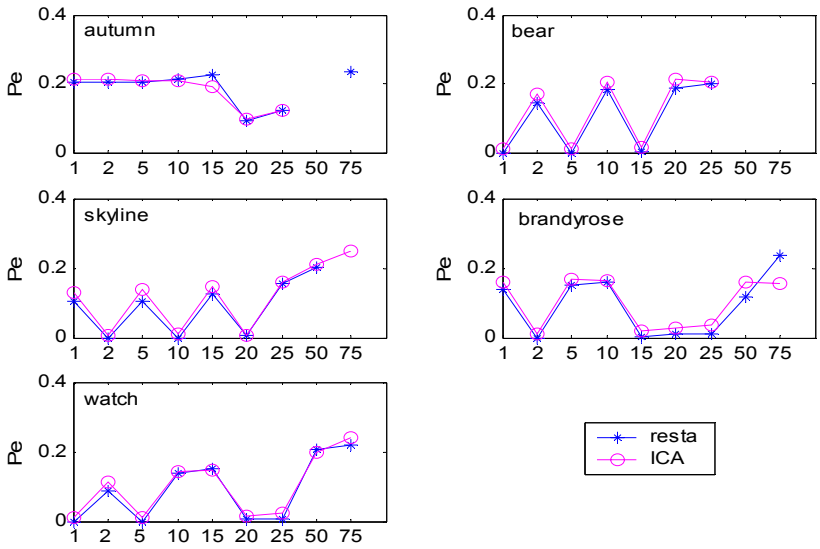


FIGURA V.18. Probabilidad de error de bit promedio para las diferentes imágenes bajo estudio y técnicas de detección empleadas, calculadas para imágenes en escala de grises.

V.13.1.2Algoritmo 3

Los resultados del algoritmo 3 se muestran en la figura siguiente, en la que se observan tendencias de comportamiento parecidas a las obtenidas en el algoritmo 1 (véase figura V.18), en el caso de que exista detección correcta, pues se observa una caída considerable de dicha magnitud con respecto al algoritmo anterior. La imagen que mejor responde a este ataque es la referida como *brandyrose.jpg* que es una imagen que presenta una reducida gama de color.

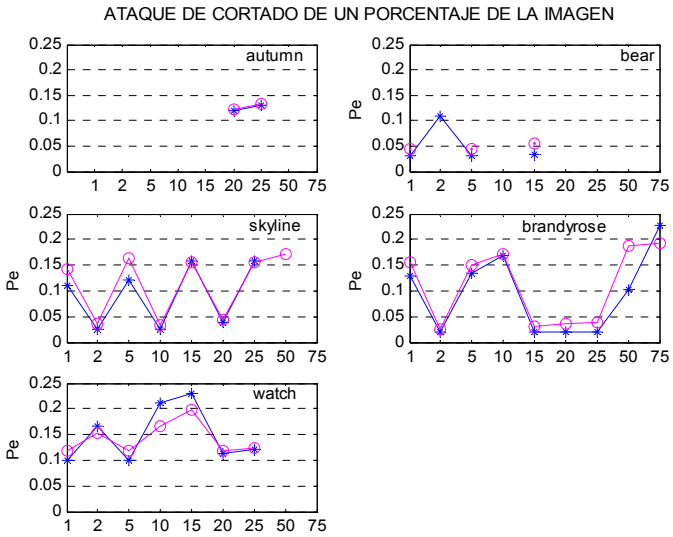


FIGURA V.19.

Probabilidad de error de bit promedio para las diferentes imágenes bajo estudio y técnicas de detección empleadas (en azul detección por resta y en magenta mediante ICA), calculadas para imágenes en escala de grises.

Los valores de probabilidad de detección correcta resultan inferiores a los obtenidos para el algoritmo 1(figura V.17), aunque se observa que la detección por ICA se hace más robusta frente a la detección por resta a medida que incrementamos el porcentaje de cortado, dándose situaciones en las que sólo se aprecia detección correcta mediante ICA para una misma modalidad de ataque (obsérvese el caso de la imagen *skyline.jpeg* para porcentaje de cortado del cincuenta por ciento en la figura V.19).

V.13.2 Algoritmos 2 y 4

Finalmente, se muestran los resultados relativos a probabilidad de detección correcta obtenidos en los algoritmos 2 y 4.

ALGORITMO 2 (DCT)

METODO DE DETECCIÓN	PORCENTAJE DE CORTADO DE LA IMAGEN									PROMEDIO
	1%	2%	5%	10%	15%	20%	25%	50%	75%	
RESTA	1	1	1	1	0.90	1	1	0.50	0.20	**0.84**
ICA	1	1	1	1	0.85	1	1	0.50	0.15	**0.82**

ALGORITMO 4 (DCT y DWT)

METODO DE DETECCIÓN	PORCENTAJE DE CORTADO DE LA IMAGEN									PROMEDIO
	1%	2%	5%	10%	15%	20%	25%	50%	75%	
RESTA	1	0.96	1	0.83	0.87	0.81	0.83	0.37	0	**0.74**
ICA	1	0.86	1	0.83	0.90	0.83	0.79	0.37	0	**0.73**

FIGURA V.19. Probabilidad de detección correcta en función del porcentaje de cortado aplicado a la imagen, para los dos métodos de detección indicados, en los algoritmos 2 y 4.