INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA
MECÁNICA Y ELÉCTRICA

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

MARCAS DE AGUA ROBUSTAS EN IMÁGENES DIGITALES CON FORMATO BMP

T E S I S

QUE PARA OBTENER EL GRADO DE
MAESTRO EN CIENCIAS EN INGENIERÍA DE TELECOMUNICACIONES

P R E S E N T A

IZLIAN YOLANDA OREA FLORES

ASESOR

M. en C. MARCO ANTONIO ACEVEDO MOSQUEDA

MÉXICO, D.F. JUNIO DE 2005

CGPI-14

INSTITUTO POLITÉCNICO NACIONAL

COORDINACIÓN GENERAL DE POSGRADO E INVESTIGACIÓN

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México, D. F. siendo las 11:00 horas del día 20 del mes de Junio del 2005 se reunieron los miembros de la Comisión Revisora de Tesis designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de la E. S. I. M. E. para examinar la tesis de grado titulada:

"MARCAS DE AGUA ROBUSTAS EN IMAGENES DIGITALES CON FORMATO BMP"

Presentada por el alumno:

OREA	**FLORES**	**IZLIAN YOLANDA**
Apellido paterno	materno	nombre(s)

Con registro:

B	0	3	1	4	7	6

Aspirante al grado de:

MAESTRO EN CIENCIAS

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***SU APROBACIÓN DE LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Director de tesis

M. EN C. MARCO ANTONIC ACEVEDO MOSQUEDA

José Luis López Bonilla

DR. JOSE LUIS LOPEZ BONILLA

DR. OLEKSIY POGREBNYAK

DR. FRANCISCO JAVIER GALLEGOS FUNES

DR. JAIR GARCIA LAMONT

M. EN C. MIGUEL SANCHEZ MERAZ

EL PRESIDENTE DEL COLEGIO

DR. JAIME ROBLES GARCIA

SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION

INSTITUTO POLITECNICO NACIONAL

COORDINACION GENERAL DE POSGRADO E INVESTIGACION

CARTA CESION DE DERECHOS

En la Ciudad de México, Distrito Federal, el día 2 del mes de agosto del año 2005, el (la) que suscribe Izlian Yolanda Orea Flores alumno(a) del Programa de Maestría en Ingeniería de Telecomunicaciones con número de registro B031476, adscrito a la Sección de Estudios de Posgrado e Investigación de la ESIME Unidad Zacatenco, manifiesta que es autor(a) intelectual del presente Trabajo de Tesis bajo la dirección del M. En C. Marco Antonio Acevedo Mosqueda y cede los derechos del trabajo intitulado: Marcas de agua robustas en imágenes digitales con formato bmp, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, graficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección: iorea@ipn.mx.

Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

IZLIAN YOLANDA OREA FLORES

Nombre y firma

OBJETIVO

El objetivo de esta tesis es proponer una técnica de inserción de marcas de agua robustas en imágenes digitales de formato BMP utilizando la Transformada Wavelet Discreta.

JUSTIFICACIÓN

Debido a la importancia que actualmente tienen las comunicaciones digitales pero sobre todo debido al aumento en la piratería y al espionaje, es que surge la idea de las marcas de agua digitales con el único fin de proteger la información. Pero las propias características de la información digital que parecieran ser ventajas, para muchos otros vienen a ser desventajas, es decir, los documentos digitales tienen por ejemplo, la facilidad de réplica, de transmisión y modificación, entre otras. Lo que hace necesaria la presencia de una técnica de protección robusta.

Entonces, las marcas de agua en imágenes digitales van a servir para darle el sello de propiedad y en un determinado momento poder comprobar a quién pertenece la información. Pero, a la par de las técnicas de inserción de marcas de agua surgen nuevas formas para tratar de eliminarlas por lo que se está proponiendo una técnica de inserción de marcas de agua robustas capaces de resistir a diferentes ataques.

RESUMEN

En este trabajo se emplea la Transformada Wavelet Discreta para aplicaciones de marcas de agua robustas en imágenes digitales BMP con el propósito de dar protección a los derechos de autor, y se compara con la técnica de la Transformada del Coseno Discreto para la misma aplicación. Se realizan las pruebas necesarias, tanto analíticas como no analíticas, para validar la seguridad y la robustez de la marca de agua principalmente, pero también para mostrar que la imagen original sufre una mínima variación después de la inserción de la marca de agua, también se indica cómo insertar la marca de agua, en qué parte y la capacidad de inserción de las imágenes.

ABSTRACT

In this work we use the Discrete Wavelet Transform in watermarking applications for digital BMP images. The objective is to guarantee some level of security for the copyright, additionally we compare the results with the Discrete Cosine Transform for the same application. Results are obtained from a number of tests, both analytic and not analytic, in order to validate the security level and the robustness of the watermark mostly, but also to prove that the original image suffers very small variations after the watermark is embedded. We also show how to embed the watermark, where to insert it and the capacity supported to insert an image.

CONTENIDO

OBJETIVO ..... **V**

JUSTIFICACIÓN ..... **VI**

RESUMEN ..... **VII**

ABSTRACT ..... **VIII**

ÍNDICE DE FIGURAS ……...… **XII**

ÍNDICE DE TABLAS ..……..... **XIV**

INTRODUCCIÓN ……..…. **1**

1 MARCAS DE AGUA ……..... **3**

1.1 Introducción a las Marcas de Agua ……..... 3

1.2 Aplicaciones de las Marcas de Agua ……... 4
1.2.1 Marcas de Agua como Firmas Digitales ……..... 4
1.2.2 Marcas de Agua Transaccionales (fingerprinting) ……..... 5
1.2.3 Marcas de Agua para Autenticación ……..... 6
1.2.4 Monitorizado de las Transmisiones de Radiodifusión ……..... 6
1.2.5 Control de Copias …….. 7
1.2.6 Comunicaciones Secretas …….. 7

1.3 Requerimientos de una Marca de Agua ……...……. 7
1.3.1 Legibilidad ……..…. 7
1.3.2 Seguridad (Imperceptibilidad e Indetectabilidad) ……..... 8
1.3.3 Robustez ……. 8

1.4 Técnicas de Inserción ……..... 9
1.4.1 Técnicas en el Dominio del Espacio ……... 10
1.4.2 Técnicas en el Dominio de la Frecuencia …….. 10

Referencias ……. 10

2 IMÁGENES DIGITALES 11

2.1 Introducción a las Imágenes Digitales 11
2.1.1 Imágenes en Escala de Grises 11
2.1.2 Imágenes a Color 13
2.1.3 Histogramas 16
2.1.4 Índice de Correlación y Energía 17

2.2 Formatos Gráficos 18
2.2.1 Clasificación 19
2.2.2 Formato BMP 20

Referencias 23

3 TRANSFORMADA DEL COSENO DISCRETO Y TRANSFORMADA WAVELET 24

3.1 Transformada del Coseno Discreto 24
3.1.1 TCD de una Dimensión 24
3.1.2 TCD de dos Dimensiones 25
3.1.3 TCD para Aplicaciones de Marcas de Agua 26

3.2 Transformada Wavelet 28
3.2.1 Transformada Wavelet Discreta 29
3.2.2 Transformada Haar 31
3.2.3 Transformada Wavelet Discreta en dos Dimensiones 31
3.2.4 TWD para Aplicaciones de Marcas de Agua 34

Referencias 34

4 ATAQUES 36

4.1 Ataques no Intencionados 36

4.2 Ataques Intencionados 36
4.2.1 Compresión 37
4.2.2 Distorsión de Brillo 38
4.2.3 Ruido 39
4.2.3.1 Ruido Multiplicativo 39
4.2.3.2 Ruido Impulsivo 41
4.2.3.3 Ruido Gaussiano 42

Referencias …… 44

5 IMPLEMENTACIÓN Y PRUEBAS 46

5.1 Capacidad de Inserción en una Imagen ……..... 46
5.1.1 Inserción Aplicando la TCD ……. 46
5.1.2 Inserción Aplicando la TWD ……... 49
5.1.3 Comparación de la TCD y la TWD en la Capacidad de Inserción …….. 51

5.2 Compresión en una Imagen …… 55
5.2.1 Compresión al Aplicar la TCD …… 56
5.2.2 Compresión al Aplicar la TWD …… 56
5.2.3 Comparación de la TCD y la TWD al recuperar la marca de agua después de una compresión ……..... 56

5.3 Distorsión de Brillo en la Imagen …….. 60

5.4 Añadiendo Ruido a la Imagen ……...……. 64
5.4.1 Ruido Multiplicativo en la Imagen ...…… 64
5.4.2 Ruido Impulsivo en la Imagen ...……. 70
5.4.3 Ruido Gaussiano en la Imagen ..……..... 76

5.5 Comparación General .....……... 81

CONCLUSIONES ……. 85

TRABAJO FUTURO ……. 86

ANEXOS …….. 87

INDICE DE FIGURAS

1.1 Documento oficial de E.U.A. 3
1.2 Marca de agua en billetes 4
1.3 Ejemplo gráfico de un sistema de marcas de agua estándar 9

2.1 Conversión de imagen de tono continuo a digital 11
2.2a Resolución 258 x 339 píxeles 12
2.2b Resolución 100 x 131 píxeles 12
2.2c Resolución 50 x 66 píxeles 12
2.3a Escala de grises a 3 bits 13
2.3b Escala de grises a 4 bits 13
2.3c Escala de grises a 8 bits 13
2.4 Descomposición de una imagen en sus planos R, G y B 14
2.5 Planos de una imagen 14
2.6 Píxel 14
2.7 Cubo de color RGB 15
2.8a Dibujo de 8 bits por píxel 16
2.8b Fotografía de 8 bits por píxel 16
2.9 Fotografía con dos intensidades de brillo 17
2.10 Clasificación de imágenes de acuerdo a la compresión 20

3.1 Posición de las frecuencias 26
3.2a Bloque de 8 x 8 píxeles de una imagen 27
3.2b Bloque después de aplicar la TCD 28
3.3 Algoritmo de codificación en sub-bandas 30
3.4 Transformada Wavelet de un nivel 33
3.5 Transformada Wavelet de dos niveles 33

4.1 Jinan.bmp 37

4.2 Jinan.jpg 37
4.3 Mujer China 38
4.4 Mujer China con Distorsión de Brillo 38
4.5 Tigre 40
4.6 Tigre afectado por ruido multiplicativo de varianza 0.05 40
4.7 Tigre afectado por ruido multiplicativo de varianza 0.2 40
4.8 Paisaje 41
4.9 Paisaje afectado por ruido impulsivo con densidad 0.05 41
4.10 Paisaje afectado por ruido impulsivo con densidad 0.1 42
4.11 Clavel 42
4.12 Clavel afectado por ruido gaussiano con varianza 0.01 media 0 42
4.13 Clavel afectado por ruido gaussiano con varianza 0.03 y media 0 43

5.1 Frecuencias usadas para insertar la información 47
5.2a Imagen original 48
5.2b Cuadro de 8x8 píxeles 48
5.2c Matriz de luminancia 48
5.2d Aplicando la TCD 48
5.2e Insertando la información 48
5.2f Armando la matriz de luminancia 48
5.2g Cuadro de 8x8 píxeles con información 48
5.2h Imagen con información 48
5.3a Imagen original en blanco y negro 49
5.3b Descomposición en frecuencias aplicando la TWD 50
5.3c Descomposición en frecuencias dela TWD después de haber insertado la información 50
5.3d Reconstrucción de la imagen con información 51

INDICE DE TABLAS

2.1 Formatos Gráficos 19
2.2 Estructura del archivo BMP 21

4.1 Generación de variables aleatorias 44

5.1 Ejemplo con histogramas de la capacidad de inserción aplicando la TCD y la TWD 52
5.2 Capacidad de inserción aplicando la TCD y la TWD 53
5.3 Comparación de los histogramas de una imagen después de una compresión 57
5.4 Comparación de la TCD y la TWD al recuperar la marca de agua después de una compresión 58
5.5 Fotografía “iglesia” con diferentes distorsiones de brillo al utilizar la TCD y la TWD 60
5.6 Fotografía “pez”, añadiéndole ruido multiplicativo con diferentes varianzas al utilizar la TCD y la TWD 65
5.7 Fotografía “circo”, añadiéndole ruido multiplicativo con diferentes varianzas al utilizar la TCD y la TWD 69
5.8 Fotografía “iglesia”, añadiéndole ruido multiplicativo con diferentes varianzas al utilizar la TCD y la TWD 70
5.9 Fotografía “pez”, añadiéndole ruido impulsivo con diferentes densidades al utilizar la TCD y la TWD 71
5.10 Fotografía “circo”, añadiéndole ruido impulsivo con diferentes densidades al utilizar la TCD y la TWD 75
5.11 Fotografía “iglesia”, añadiéndole ruido impulsivo con diferentes densidades al utilizar la TCD y la TWD 75
5.12 Fotografía “pez”, añadiéndole ruido gaussiano con diferentes densidades al utilizar la TCD y la TWD 76

5.13 Fotografía “circo”, añadiéndole ruido gaussiano con diferentes densidades al utilizar la TCD y la TWD 80
5.14 Fotografía “iglesia”, añadiéndole ruido gaussiano con diferentes densidades al utilizar la TCD y la TWD 81
5.15 Comparación de la TCD y la TWD en la capacidad de incrustación de marcas de agua robustas 82
5.16 Comparación de la TCD y la TWD en el índice de correlación entre la imagen y ésta después de la inserción de la marca de agua robusta .. 83
5.17 Comparación de la TCD y la TWD en la pérdida de energía entre la imagen y ésta después de la inserción de la marcas de agua robusta 84

INTRODUCCIÓN

El uso de las marcas de agua surge de la necesidad de proteger los derechos de autor en documentos digitales (texto, audio, imágenes y video), dado el incremento en la piratería, clonación de documentos y espionaje en los diferentes medios de comunicación. [1] Es necesario proteger los documentos para poder intercambiar información de manera confiable dentro de medios de comunicación inseguros.

Las características propias de la información digital (facilidad de réplica, facilidad de transmisión y uso múltiple, facilidad de tratamiento y modificación, equivalencia de las copias digitales, etc.) permiten la agresión contra los derechos de autor, lo que hace necesaria la existencia de un sistema de protección potente. Por esto, el concepto de marcas de aguas se ha expandido al mundo digital para autentificar la propiedad de una información digital y en la defensa de los intereses de dicha propiedad.

Las marcas de agua son parte de un campo aun más grande llamado esteganografía.[2] El propósito de la esteganografía es incluir cierta información dentro de otra -llamada portadora- con el único requerimiento de que la portadora se modifique en forma despreciable.[3] Las técnicas de esteganografía modifican de manera insignificante el dato original, siendo el cambio invisible perceptivamente.[4] Usualmente se transmiten entre dos partes, es decir, punto a punto. Además, su principal objetivo es comunicar un mensaje y no autentificar un trabajo -como la marca de agua. Las técnicas de estenografía no requieren una gran robustez o protección.

Por otro lado, una marca de agua es aún más compleja porque debe ser robusta contra ataques. Si la información oculta es descubierta debe ser difícil de modificar por el atacante y, en caso de ser modificada o removida, la portadora debe cambiar de forma completamente visible para indicar que la información ha sido alterada. Entonces, para ser aplicable, una marca de agua aparte de ser imperceptible debe cumplir también con los siguientes requerimientos: legibilidad, seguridad, y robustez. En el capítulo I se explica más detalladamente qué es una marca de agua, así como las características que requiere para ser más resistente a diferentes ataques, los cuales incluyen operaciones de procesamiento digital tales como compresión, distorsión de brillo y diferentes tipos de ruido,[2] mismos que se explican en el capítulo IV.

Aunque este trabajo está enfocado únicamente en imágenes digitales BMP, al principio se comentó que las marcas de agua digitales se pueden aplicar a diferentes tipos de documentos. Por eso se hizo necesario explicar en el capítulo II qué es una imagen digital y los diferentes tipos que existen.

Actualmente hay una técnica muy eficiente para insertar marcas de agua en archivos digitales, que es aplicando la Transformada del Coseno Discreto, pero en este

trabajo se propone una nueva técnica de inserción que utiliza la Transformada Wavelet Discreta. Ambas transformadas, al igual que sus técnicas respectivas, se exponen en el capítulo III. Todas las pruebas realizadas en la implementación de la técnica propuesta se comparan con la ya existente para resaltar las diferencias entre ambas. Los resultados se muestran en el último capítulo.

---

[1] J. J. K. Ò Ruanaidh, W. J. Dowling, y F. M. Boland. "Watermarking digital images for copyright protection", *IEEE Image and Signal Processing*, pp. 250-256, 1996.

[2] Arto Kaarna, Pekka Toivanen. "Digital Watermarking of spectral Images in PCA/Wavelet-transform Domain", *IEEE transactions on image processing*, pp. 220-224, 2003.

[3] D. Artz. "Digital Steganography, Hiding data within Data", *IEEE Internet Computing*, vol 5, Iss.3, pp. 75-80, May/Jun 2001.

[4] Stefan Katzenbeisser, Fabien A. P.,Petitcolas. "Information Hiding", *Principles of Steganography*, Artech House, 2000.

CAPÍTULO I

MARCAS DE AGUA

Antes de explicar la parte fundamental de este trabajo, es necesario definir algunos términos que se manejan a lo largo del mismo para su mejor comprensión.

1.1. INTRODUCCIÓN A LAS MARCAS DE AGUA

El uso de las marcas de agua como sistema de protección es casi tan antiguo como la fabricación del papel, teniendo sus primeros registros hace 700 años.[1] Durante cientos de años, cualquiera que poseyera o fabricase un documento u obra de arte valioso lo marcaba con un sello de identificación o marca de agua (visible o no), no sólo para establecer su propiedad, origen o autenticidad, sino para desalentar a aquellos que pudieran intentar robarlo.

Las técnicas de marcas de agua son utilizadas para la autenticación de la información (tanto del distribuidor o propietario legal), como de que el original no ha sido falsificado y para el seguimiento de copias, ya que permiten la identificación del autor, propietario, distribuidor y/o consumidor autorizado de un documento digital.[2]

Las figuras 1.1 y 1.2 muestran ejemplos de marcas de agua físicas: las primeras, en dos billetes de 100 dólares y 200 euros respectivamente; y la otra, en un documento oficial de EE.UU. Así, el mismo principio se aplica con las técnicas de marcas de agua digitales, pero con la gran diferencia de que éstas, en general, no son visibles, aunque son tan difíciles de copiar, cambiar o remover como las marcas de agua físicas.

Figura 1.1 Marcas de agua en billetes

Figura 1.2 Documento oficial de EE.UU.

La técnica de protección digital requiere básicamente dos procesos:

1. Introducción de la firma o marca en la información a proteger
2. Extracción e identificación de la marca

Una marca de agua es entonces un código de identificación, perceptible o preferiblemente imperceptible, que se encuentra permanentemente incrustado en la información (la cual no desaparece después del descifrado) y que puede contener –como ya se ha dicho- información acerca del propietario, los derechos de autor, el creador, el usuario autorizado, el número de copias o reproducciones autorizadas, etc.

1.2. APLICACIONES DE LAS MARCAS DE AGUA

Los requisitos que deben cumplir en la práctica los algoritmos de marcas de agua deben analizarse dentro del entorno de trabajo del sistema y de acuerdo con la aplicación donde éste será utilizado.[3] Dicho esto, las siguientes son algunas de las posibles aplicaciones de las marcas de agua y sus peculiaridades.

1.2.1. *MARCAS DE AGUA COMO FIRMAS DIGITALES*

Las marcas pueden utilizarse para firmar archivos multimedia. El propietario de uno de estos archivos insertará una marca de agua que lo identifique como tal. Esta aplicación puede verse en los siguientes escenarios:

- **Identificación del propietario**

La forma usual de informar sobre los derechos de propiedad intelectual, tanto en libros, fotografías o cualquier tipo de documentos, como en las cajas de CDs de música y los créditos de las películas, es una nota de copyright colocada en forma visible. Evidentemente estas notas no garantizan la protección de la autoría de tales materiales; baste sólo nombrar lo fácil que resulta borrar los créditos de una película, o tirar la envoltura de un CD de música. Como complemento de las notas de copyright, puede insertarse una marca de agua que formará parte del contenido del producto; por ejemplo, la información del copyright insertada dentro de una imagen fotográfica.

- **Prueba de propiedad**

Los propietarios de archivos multimedia pueden usar las marcas de agua no sólo para identificar sus derechos de autor, sino también para probar la propiedad que ejercen sobre estos archivos.

1.2.2. *MARCAS DE AGUA TRANSACCIONALES (FINGERPRINTING)*

Las marcas de agua también pueden utilizarse para identificar a los compradores de archivos multimedia, lo cual puede servir para buscar al infractor en caso de que se distribuyan copias ilegales de un archivo dado. [3]

En este caso, la marca de agua transaccional se incrusta de manera adicional (o efectuando una nueva copia de los archivos originales) y lleva los datos tanto del propietario como del comprador. Además de usar la marca de agua (firma), para demostrar la propiedad de sus datos multimedia, el propietario podría identificar al responsable de la distribución ilegal de las copias que ha vendido.

Es importante recalcar que dentro de los requisitos de esta aplicación, el sistema ha de tener capacidad y permiso para insertar varias marcas de agua en un mismo archivo.

Uno de los escenarios donde estas marcas de agua pueden ser utilizadas es durante el rodaje de una película: el resultado diario de las tomas de fotografía de una película se distribuye a todas las personas involucradas en su realización. Estas tomas tienen un carácter altamente confidencial y los originales de las mismas se guardan celosamente. En caso de que se filtre la copia de una toma dada, los estudios cinematográficos necesitan identificar con prontitud al infractor; si cada copia distribuida contiene una marca que identifica a su poseedor, se descubre al culpable. En este entorno las marcas de agua no necesitan ser totalmente imperceptibles, ya que lo que se precisa es identificar a quién se le ha dado cada copia.

La vulnerabilidad de un sistema de este tipo a un posible ataque por confabulación debe estudiarse cuidadosamente y tenerse en cuenta en su diseño e implementación.

1.2.3. *MARCAS DE AGUA PARA AUTENTICACIÓN*

Existen muchas aplicaciones donde la veracidad de una imagen es crucial; tal es el caso de imágenes médicas y muchas otras. Las marcas utilizadas para la autenticación contendrán la información requerida que determinará la integridad de un archivo multimedia. La marca debe ser invisible y frágil (cualquier modificación de la imagen debe alterar la marca) y es muy deseable que pueda ofrecer información sobre los cambios ocurridos en las imágenes.[4]

Supongamos otro escenario: una agencia de prensa que recibe imágenes capturadas por un reportero con una cámara digital; antes de usar las imágenes la agencia querrá tener la seguridad de que las mismas no han sido alteradas o editadas tras su captura.

Una de las primeras ideas aportadas para la creación de una cámara digital confiable fue Friedman.[5] Su sistema añadiría una firma criptográfica asociada con la imagen captada, que formara parte de los datos localizados en la cabecera del formato de la misma, lo que supone el inconveniente de que dicha firma desaparece cuando la imagen se pasa a otro formato que no contenga este campo de cabecera.

Para resolver este problema y volviendo al ejemplo inicial, se incrusta durante la captura de la imagen una marca de agua invisible. Esta marca llevará información acerca del número de serie de la cámara digital, de manera que, al detectarla, la agencia de prensa determinará la veracidad de la imagen. Aquí el uso de la marca posibilitará la detección de las manipulaciones, ya que cualquier alteración aparecerá también en la marca.

1.2.4. *MONITOREO DE LAS TRANSMISIONES DE RADIODIFUSIÓN*

Al igual que en las firmas y las marcas transaccionales, las marcas de agua identificarán al propietario de los archivos multimedia y/o al comprador de una copia determinada de los mismos y serán detectadas por sistemas automatizados que rastrean las transmisiones de televisión y radiodifusión, las redes de computadoras y otros canales de distribución para estar al tanto de cuándo y dónde se ha utilizado un archivo multimedia. [4]

Muchas comunidades están interesadas en la supervisión de las transmisiones de radiodifusión, cada una de ellas por diferentes motivos. Por ejemplo, los músicos y actores cuyas obras son retransmitidas en diversas cadenas de radio y televisión, así como los agentes publicitarios, desean asegurarse de que el tiempo que realmente están al aire, sea el que han pagado. En este contexto, la marca de agua insertada en cada video clip debe ser irremplazable.

1.2.5. *CONTROL DE COPIAS*

Las marcas de agua diseñadas para el control de copias contendrán la información determinada por su propietario, acerca de las reglas de uso y copiado de los archivos en los que se insertan. A diferencia de las marcas de agua transaccionales y de las marcas de aguas usadas para el monitorizado, identificación y pruebas de propiedad, que sólo sirven como herramienta para investigar a los transgresores del sistema, las marcas de agua usadas en el control de copias restringen la utilización de los archivos de acuerdo con las reglas de uso y copiado que porten.

Actualmente, esta aplicación está evolucionando continuamente. En los DVD de video, uno de los sistemas implantados fue el DIVX con características del tipo pago por evento; sin embargo, esta iniciativa ha sucumbido ante la inconformidad de la mayoría de sus consumidores potenciales.

Muchas compañías se han asociado en la búsqueda de métodos más apropiados para los DVD, las corporaciones Macrovision, Philips y Digimarc se agruparon en el llamado Millennium Group Watermarking para desarrollar un sistema que combina un procedimiento de marcas de agua con un sistema de control de reproducción de pistas y autenticación, con vistas a la protección de los contenidos de video grabados en videocasetes y DVDs y de las transmisiones hechas por cable o satélite. También se incluía dentro del hardware el diseño de módulos de las computadoras que garanticen esta protección.[4]

1.2.6. *COMUNICACIONES SECRETAS*

En esta aplicación, la marca incrustada en los archivos multimedia es utilizada por dos o más personas para comunicarse secretamente sin levantar la sospecha de terceros. Es la aplicación clásica de la esteganografía (ocultamiento de una información dentro de otra): la comunicación a través de canales subliminales.[2]

1.3. REQUERIMIENTOS DE UNA MARCA DE AGUA

Existe un gran número de publicaciones en las que se discuten los requisitos que deben cumplir las marcas de agua.[6] Es bueno destacar que la seguridad de estos sistemas no debe radicar en el ocultamiento de los algoritmos utilizados, sino en la fortaleza de los mismos.

Por orden de efectividad, una marca de agua debe ser *legible*, *segura* y *robusta*.[7]

1.3.1. *LEGIBILIDAD*

Que una marca de agua digital sea legible significa que se pueda detectar correctamente la información contenida cuando se necesite extraerla, sin modificaciones ni alteraciones.

1.3.2. *SEGURIDAD (IMPERCEPTIBILIDAD E INDETECTABILIDAD)*

La imperceptibilidad y la indetectabilidad de las marcas de agua son dos conceptos que tienden a confundirse frecuentemente, aunque son muy distintos y no están relacionados entre sí.

La imperceptibilidad o transparencia de la marca tiene como base el comportamiento del sistema perceptivo humano. Una marca de agua es imperceptible (transparente), si la degradación que causa en los archivos donde se ha insertado es muy difícil de apreciar. Este concepto se contrapone al de la robustez, si tenemos en cuenta que un sistema robusto debe insertar la marca en las regiones perceptiblemente significativas del archivo. En algunas aplicaciones se puede aceptar una pequeña degradación de los datos, a cambio de lograr mayor robustez o menor costo del sistema.

La indetectabilidad está relacionada con el modelo estadístico del archivo antes y después de ser marcado. Se dice que la marca es indetectable si después de haberla insertado, el archivo marcado conserva las mismas propiedades estadísticas que su original. Lo que quiere decir que una persona no autorizada no podrá detectar la presencia de la marca utilizando métodos estadísticos. Esta propiedad es muy deseable en el caso de las comunicaciones encubiertas en las que el principal objetivo es ocultar la presencia del mensaje incrustado en el archivo.

1.3.3. *ROBUSTEZ*

Una marca de agua se considera robusta si perdura en la imagen aún después de sufrir diferentes ataques tales como: distorsión de brillo, la compresión y ruido.[8] Para consolidar su robustez, los sistemas de marcas de agua deben insertar la marca en las regiones perceptiblemente significativas de los archivos (véase Cox et al [4]).

La robustez no debe exigirse incondicionalmente, ya que un sistema de marcas de agua puede necesitar ser robusto respecto a determinados procesos y frágil respecto a otros. Cuando un sistema de marcas de agua requiere que ciertas modificaciones de los archivos dañen la marca se le denomina sistema de marcas de agua frágiles y es muy importante en determinadas aplicaciones.

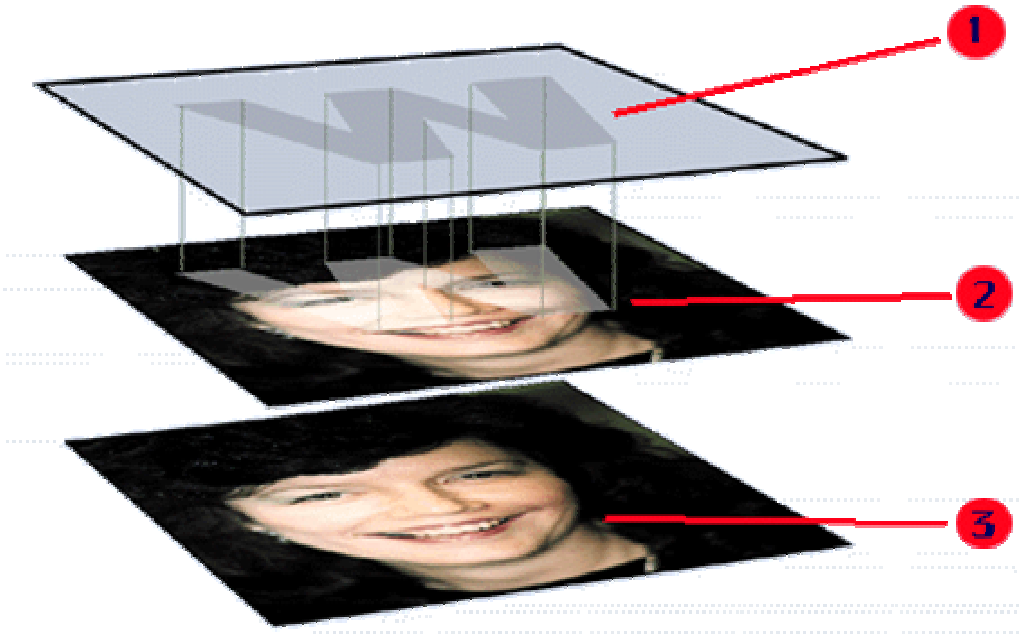


Figura 1.3 Ejemplo gráfico de un sistema de marcas de agua estándar

La mayoría de los sistemas de marcas de aguas digitales actuales se basan en la introducción de la marca en las componentes espectrales perceptiblemente significativas de una imagen, que son las frecuencias bajas. Ahora bien, la modificación de dichas componentes ha de ser lo suficientemente pequeña como para que no se pueda percibir a simple vista.

Un sistema de marcas de agua estándar está compuesto por dos módulos principales, que realizan los procesos de codificación (o inserción) de la marca y decodificación (o extracción e identificación) de la misma.

En la figura 1.3, el módulo codificador realiza la inserción de la marca de agua 1 en la información original 2 para crear la información marcada 3, que en este caso debe ser visualmente 2.

1.4. TÉCNICAS DE INSERCIÓN

Las técnicas de inserción existentes se pueden clasificar en dos grupos, en función del tipo de elemento de la imagen al que la marca de agua afecta de manera directa.[2]

1.4.1. *TÉCNICAS EN EL DOMINIO DEL ESPACIO*

La inserción de la marca de agua va a modificar directamente el valor de luminancia y/o cromancia de los píxeles.

1.4.2. *TÉCNICAS EN EL DOMINIO DE LA FRECUENCIA*

La marca modifica directamente el valor de los coeficientes espectrales de la imagen. La mayor parte de las técnicas desarrolladas en este dominio están inspiradas en métodos de codificación y compresión.

---

[1] Simon Singh, "Los Códigos Secretos", la evolución de la escritura secreta, Debate, 2000.

[2] Stefan Katzenbeisser, Fabien A. P.,Petitcolas. "Information Hiding", Principles of Steganography, Artech House, 2000.

[3] I.J. Cox, M. L. Miller, J. A. Bloom. "Digital Watermarking", Morgan Kaufman Publishers, 2003.

[4] J. J. Eggers, B. Girod. "Blind Watermarking Applied to Image Authentication", Utah, USA, 2001.

[5] L. Friedman. "The trustworthy digital camera: restoring credibility to the photographic image", *IEEE Trans. On Consumer Electronics*, vol.39, pp 905-910, November 1993.

[6] I. J. Cox, J. Kilian, T. Leighton, T. Shamoon. "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.

A. Piva, M. Barni, F. Bartolini. "Copyright protection of digital images by means of frequency domain watermarking. Mathematics of Data/Image Coding, Compression, and Encryption", Proceedings of SPIE Vol. 3456, pp. 25-35, 1998

[7] J. J. K. Ò Ruanaidh, W. J. Dowling, and F. M. Boland. "Watermarking digital images for copyright protection", IEEE Image and Signal Processing, pp. 250-256, 1996.

[8] 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.

CAPÍTULO II

IMÁGENES DIGITALES

2.1. INTRODUCCIÓN A LAS IMÁGENES DIGITALES

Una imagen natural comienza como una sucesión continua de variaciones de color y sombras. En el caso de una fotografía las sombras varían de claras a oscuras y los colores varían de rojos a azules, pasando por los amarillos. A una imagen de esta naturaleza se le conoce como de tono continuo,[1] lo cual quiere decir que los colores y sombras variantes se mezclan sin interrupción abrupta, describiendo fielmente la escena original.

2.1.1. *IMÁGENES EN ESCALA DE GRISES*

Una imagen digital en tonos de gris está compuesta por un valor finito de puntos de tonalidad que varían dentro de un rango que va del negro al blanco, pasando por una gran gama de grises. Para fabricar una imagen digital a partir de una imagen de tono continuo, la imagen debe dividirse en puntos individuales de brillo (muestreo). Adicionalmente, cada punto de brillo debe ser descrito por un valor digital (cuantificador), la figura 2.1 da un ejemplo de este proceso.

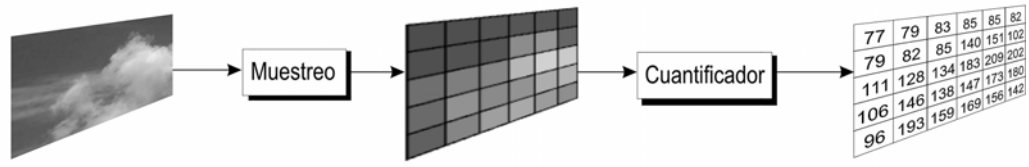


Figura 2.1 Conversión de imagen de tono continuo a digital.

A cada muestra obtenida se le denomina píxel y representa un elemento discreto de la imagen digital. Una imagen generalmente se muestrea en un arreglo rectangular de píxeles, es decir una matriz, por lo que cada píxel tiene una coordenada (x, y) que corresponde a su ubicación dentro de la imagen. En la mayoría de los casos la coordenada (0,0) se refiere a la esquina superior izquierda de la imagen, siendo la x la localidad horizontal y la y la localidad vertical.

La calidad de la imagen digital está directamente relacionada con el número de píxeles que tenga y con el rango disponible de valores de brillo. A estos aspectos se les conoce como resolución de la imagen. Se usa el término resolución espacial para describir cuántos píxeles componen una imagen. A mayor número de píxeles, mayor resolución espacial. La figura 2.2 muestra una misma fotografía a diferentes resoluciones espaciales.

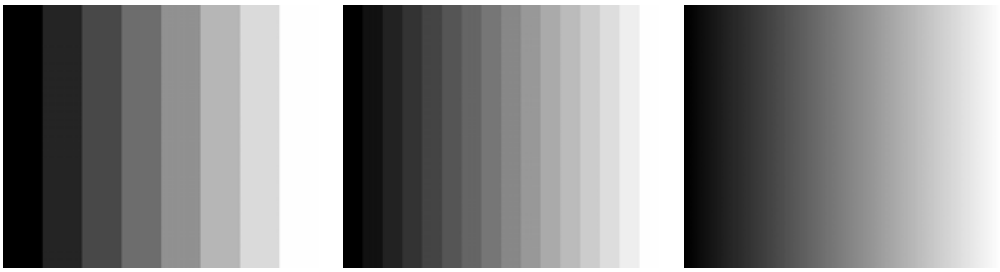
a) b) c)

Figura 2.2 Diferentes resoluciones en una imagen, a) 258 x 339 píxeles , b) 100 x 131 píxeles, c) 50 x 66 píxeles

Los requerimientos de resolución espacial para una imagen están determinados por la aplicación que se le quiera dar a la imagen. En el ejemplo de la figura 2.2 vemos que la resolución de 258 x 339 píxeles fue adecuada para ese tamaño de impresión, pero la de 50 x 66 píxeles ya no es suficiente. Si la intención es enviar las imágenes por correo electrónico, una resolución comúnmente empleada es la denominada VGA, que consiste en 640 x 480 píxeles. Otros estándares comunes son SVGA a 800 x 600 píxeles y UVGA a 1024 x 768 píxeles.

Por otro lado, se tiene la resolución de brillo. Cada píxel representa la intensidad de brillo de la imagen original en la ubicación espacial donde fue muestreado. El concepto de resolución de brillo considera con qué precisión puede el brillo de un píxel representar la intensidad de brillo de la imagen original. Si se aumenta el rango numérico posible de brillo para cada píxel, se incrementa así mismo la resolución de brillo.

Después del proceso de muestreo, cada muestra se cuantifica. El proceso de cuantificación convierte la intensidad de tono continuo en el punto de muestreo a un valor digital de brillo. La precisión del valor digital depende directamente de cuántos bits se usen en el cuantificador. Si se usan 3 bits, el brillo se puede convertir en uno de ocho niveles disponibles de gris. En este caso el nivel “0” de gris representa al color negro y el nivel “7” de gris representa al color blanco; los niveles de gris “1” a “6” representan una escala descendente de tonalidades de gris, entre el negro y el blanco.



a) b) c)

Figura 2.3 Diferentes escalas de grises en una imagen a) 3 bits, b) 4 bits y c) 8 bits

Si se usan 4 bits para representar el brillo, cada píxel es representado por uno de 16 niveles de gris. Análogamente, un valor de brillo de 8 bits permite un rango de 256 tonalidades distintas. Vea la figura 2.3 y compruebe cómo la suavidad de la escala de grises mejora conforme más bits se usan en el cuantificador.

2.1.2. IMÁGENES A COLOR

Cuando trabajamos con imágenes a color, los mismos conceptos de muestreo, cuantificación, resolución espacial y resolución de brillo son válidos. Pero, en lugar de usar un solo valor para representar el brillo, las imágenes digitales a color generalmente son cuantificadas empleando tres componentes de brillo. Al desplegar color, se usan tres emisores independientes de color, que emiten cada uno una banda única de luz para generar en conjunto todos los colores del espectro.

Si miramos muy de cerca la pantalla de una computadora, descubriremos puntos individuales de colores sólidos. Esos puntos pueden emitir luz en los colores rojo, verde o azul. Conforme nos alejamos de la pantalla los puntos tienden a mezclarse hasta el grado en que ya no se distinguen los puntos individuales. En lugar de eso, ahora se percibe la combinación de color y se percibe como si fuera un solo color, producto de esos tres colores. Esto es debido a que todos los colores del espectro se pueden generar a partir de los llamados colores primarios: rojo, verde y azul.

A esto se le conoce como la propiedad aditiva del color.[2] Si sólo se enciende el color rojo, el color que se percibe naturalmente es rojo. Pero, conforme el rojo varía de oscuro a más iluminado, se podrán observar los distintos brillos del rojo. Así mismo ocurrirá con el verde y con el azul. Ahora bien, si se encienden los componentes rojo y verde, entonces se percibirá un amarillo. Si se varía la intensidad de brillo, entonces se percibirán los colores desde café oscuro hasta amarillo brillante.

Entonces, una imagen digital a color es una matriz tridimensional, que se compone por tres planos conocidos como R, G y B (Red, Green, Blue) como se muestra en la figura 2.4, donde R contiene el componente de rojo de cada píxel; G, el verde y B,

el azul. Con la combinación de estos tres elementos en las proporciones correspondientes se puede formar cualquier otro color.[2]

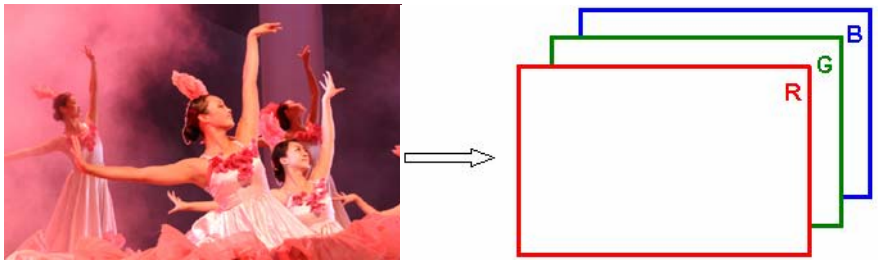


Figura 2.4 Descomposición de una imagen en sus planos R, G y B

Si tomamos un pequeño rectángulo de una fotografía y descomponemos sus planos podremos ver los valores digitales que la forman, tal como lo muestra la figura 2.5.

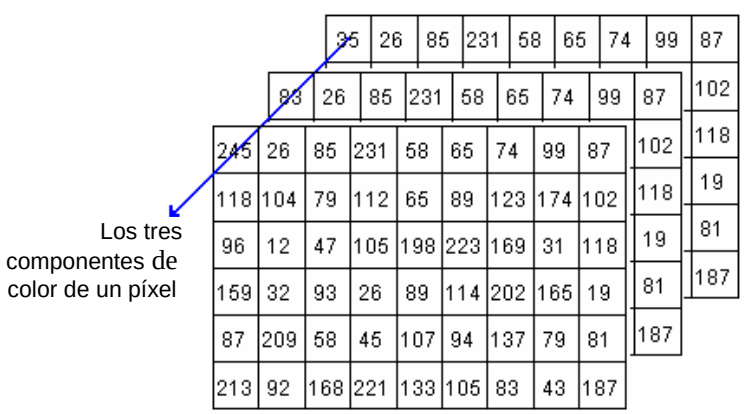


Figura 2.5 Planos de una imagen

Entonces el color correspondiente al primer píxel de la imagen estaría formado por la combinación de los elementos: (0,0,1), (0,0,2) y (0,0,3), como se ve en la figura 2.6.

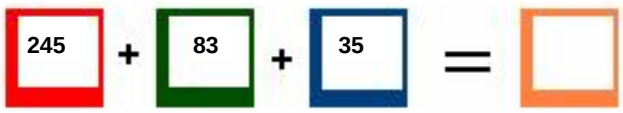


Figura 2.6 Píxel

El espacio de color RGB usualmente se muestra gráficamente como un cubo de color igual al indicado en la figura 2.7. Los vértices del cubo son los colores primarios (rojo, verde y azul) y secundarios (cyan, magenta y amarillo), colores de la luz.[3]

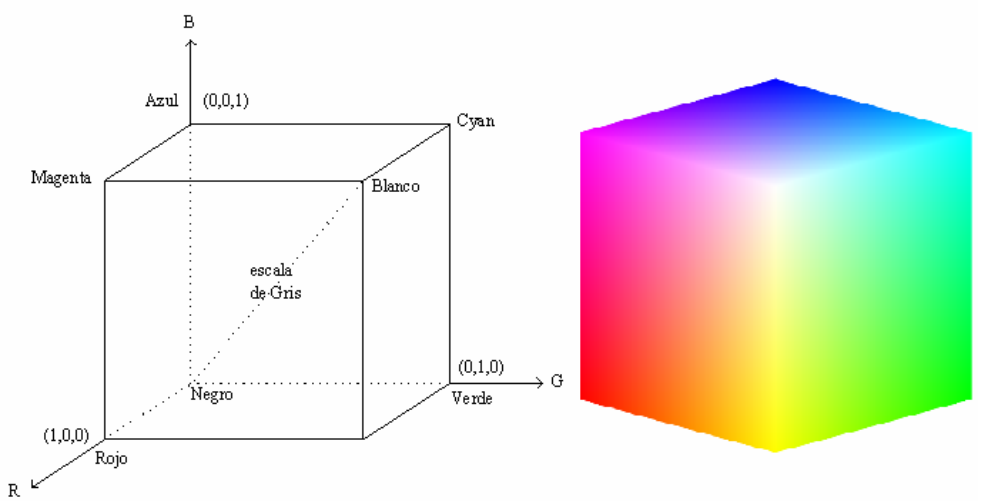


Figura 2.7 Cubo de color RGB

El espacio de color más conocido es el RGB pero existe otro espacio conocido como YCbCr, formado por una componente de luminancia (Y) y dos de crominancia (Cb y Cr). La luminancia indica el brillo del color y la crominancia distingue los grados de color. Un vector de color en RGB puede convertirse a YCbCr usando la siguiente transformación:[4]

$$Y = 0.99R + 0.587G + 0.114B$$

$$Cb = 0.5 + \frac{B - Y}{2}$$

$$Cr = 0.5 + \frac{R - Y}{1.6}$$

¿Cómo se almacenan las imágenes a color? Será fácil comprenderlo recordando los conceptos presentados anteriormente. Si para una imagen en tonos de gris a 8 bits se requiere un byte (ya que un byte puede almacenar uno de 28 valores en el rango de 0 a 28-1) para almacenar cada píxel, entonces en las imágenes a color que requieran la posibilidad de guardar 3 valores de intensidad (rojo, verde y azul) para cada píxel, se requerirán 3 bytes por píxel. Un byte almacenará la intensidad del rojo, otro la intensidad del verde y otro más la intensidad del azul. A este arreglo se le conoce como imágenes a color de 24 bits o de color verdadero.

Cabe mencionar que también existen imágenes a color de 8 bits, siendo su aplicación más importante los dibujos estilo historieta. Esas imágenes son muy populares en los iconos usados en las páginas de Internet. Se les puede encontrar en forma de botones, separadores, animaciones (que son una secuencia de varias imágenes de 8 bits), menús, etc. Se ahorra espacio usando solamente 8 bits y aunque se tienen disponibles sólo 256 colores, eso ha demostrado ser suficiente. Pero si el interés es mostrar fotografías de escenarios naturales, entonces 8 bits a menudo no serán suficientes, por lo que se recurre a 24 bits que proveen un rango aproximado de 16 millones de colores. No obstante, habrá algunos tipos de fotografías que a pesar de representar escenarios naturales puedan ser aceptablemente almacenadas con 8 bits. La figura 2.8a muestra un dibujo típico que se almacena con 8 bits y la figura 2.8b muestra un atardecer que, de manera excepcional, también está almacenado en 8 bits sin perder gran fidelidad.

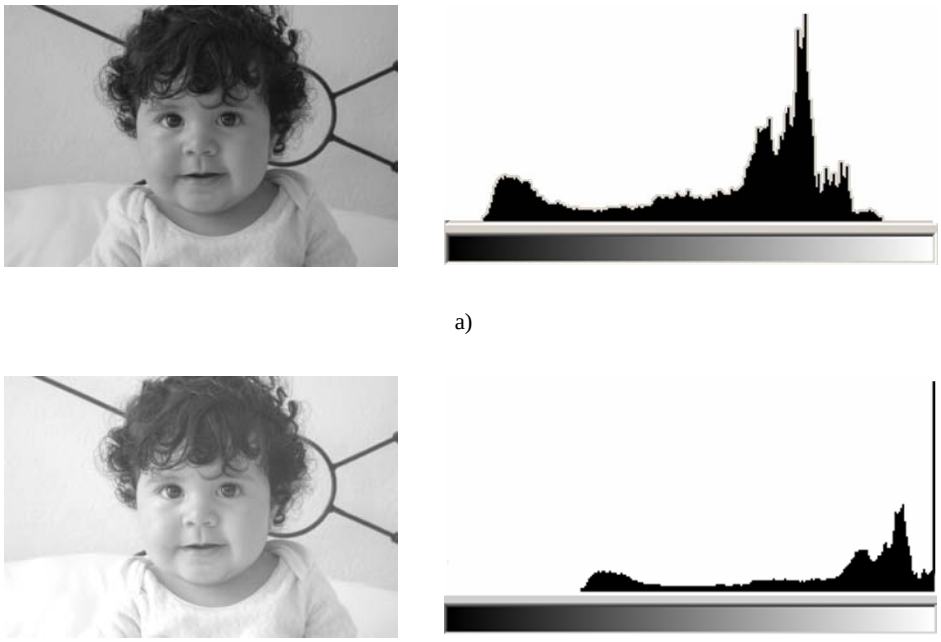
a) b)

Figura 2.8 Imágenes a 8 bits por píxel

2.1.3. *HISTOGRAMAS*

Los histogramas para una imagen a color son una versión triple del histograma de brillo de una imagen de tonos de gris. Se calculan tres histogramas, uno para cada componente de color. Cada histograma nos puede ayudar a determinar la distribución de brillo, el contraste y los rangos dinámicos para cada componente de color. Otra posibilidad es primero convertir la imagen a color a una imagen de tonos de gris y entonces calcular un solo histograma que represente toda la imagen.

Sirva como ejemplo la figura 2.9 que muestra dos versiones de la misma fotografía. La figura 2.9a es más oscura y por lo tanto su histograma tiene más componentes del lado izquierdo, es decir, del lado de los tonos más oscuros, tendientes al negro (valor cero). La figura 2.9b se produjo aumentándole brillo a la imagen original. Su histograma presenta una gráfica corrida hacia la derecha, mostrando así que son más abundantes los tonos claros y más escasos los tonos negros. Se observa también una fuerte presencia de color blanco (barra vertical en el extremo derecho del histograma, valor 255).



a)

b)

Figura 2.9 Fotografía con dos intensidades de brillo y sus respectivos histogramas.

En todos los histogramas que se muestran en este trabajo, La escala horizontal representa los posibles valores de 0 a 255 de tonos de gris, correspondiéndole el 0 al color negro y el 255 al color blanco. La escala vertical representa el número de píxeles que aparecen para cada tonalidad.

2.1.4. *ÍNDICE DE CORRELACIÓN Y ENERGÍA*

Cuando los cambios en una imagen no llegan a ser notorios ni visual ni gráficamente, se debe tener una manera de saber si una fotografía ha sido modificada por mínimo que esto sea. El análisis matemático es la única forma exacta de saber qué tanto cambió una señal con respecto a la original.[5] Dos formas de ver este análisis es el índice de correlación y la energía.

- **Índice de Correlación**

Indica qué tan diferentes son dos señales, si el índice de correlación es 1, las señales son exactamente iguales, y si es 0, son completamente diferentes.[5]

$$\rho_{xy}[l] = \frac{r_{xy}[l]}{\sqrt{r_{xx}[0]\ r_{yy}[0]}} \qquad l = 0, \pm 1, \pm 2 \ldots$$

donde:

ρ_{xy}[l] es el índice de correlación

r_{xy}[l] es la correlación cruzada entre la imagen original y la imagen modificada.

r_{xx}[0] es la autocorrelación de la imagen original.

r_{yy}[0] es la autocorrelación de la imagen modificada.

- **Energía**

La medición de la energía es importante porque si se ha perdido una cantidad considerable de energía en una señal significa que se ha perdido información fundamental de la misma. En todas las señales, incluyendo las imágenes, un gran porcentaje de energía se alberga en las frecuencias bajas. La energía de una señal $x[n]$ se calcula de la siguiente manera.[5]

$$E_x = \sum_{n=-\infty}^{\infty} |\, x[n] \,|^2$$

2.2. FORMATOS GRÁFICOS

Ya hemos revisado que se pueden asignar más o menos bytes para almacenar cada píxel. Pero esto es sólo la punta del iceberg que representa la estructura de datos encargada de almacenar físicamente el archivo en una computadora. La estructura empleada puede ser tan distinta como diseñadores y programadores hay. No obstante, existe una serie de formatos gráficos que son muy populares debido a que sus aplicaciones son bastante conocidas en el mundo. En la tabla 2.1 se presenta una lista alfabética de los formatos gráficos más comunes y sus respectivas aplicaciones.[6] Los acrónimos en inglés sin traducción conocida, se han dejado entre comillas en el idioma original.

Tabla 2.1 Formatos gráficos

Formato de archivo	Descripción
BIFF	Formato XITE (3D)
BMP	Mapa de bits (MS-Windows)
BW	Formato SGI para blanco y negro
CGM	“Computer Graphics Metafile”
DRAW	Formato basado en vectores de Acorn
DWG	Archivo de AutoCAD
FAX	Estándar del Grupo 3 de faxes
DCX	Formato gráfico para fax
EPSF	Archivo encapsulado Postscript
FIG	Formato empleado por la utilería “xfig”
FITS	Sistema de transporte flexible de imagen
GIF	Formato de intercambio gráfico
GL	Formato para animaciones
ICC	Formato de impresión Kodak
IFF	Formato de intercambio de archivos
JPEG	“Joint Photographic Experts Group”
MIFF	Formato independiente de la máquina
NAP	Formato orientado a objetos
PIX	Usado por SGI
PCX	Usado por Microsoft Paintbrush
PNG	“Portable Network Graphics Specification”
PBM+	Mapa de bits portátil mejorado
PBM	Mapa de bits monocromático
PGM	Formato para escala de grises
PPM	Imágenes a todo color
PNM	Formato general de imágenes
RLE	“Run length encoded”
RAS	“Sun Raster File”
RGB	Formato de color para SGI
SLD	Transparencias de AutoDesk
SPRITE	Mapa de bits para el sistema operativo RISC de Acorn
TGA	Formato llamado “Targa”
TIFF	“Tagg Image File Format”

2.2.1. *CLASIFICACIÓN*

Una manera de clasificar los distintos formatos gráficos es en base a la compresión. La compresión de una imagen es una operación para reducir el espacio de almacenamiento de la misma. El objetivo es representar una imagen con un determinado nivel de calidad requerido, pero de forma más compacta. El proceso de compresión busca extraer la información esencial de modo que la imagen pueda ser reconstruida con precisión. La información no esencial a menudo se descarta.

La compresión de imágenes generalmente se efectúa como antecedente al almacenamiento o transporte de las mismas. Esto es debido a que ambas situaciones son sensibles al tamaño de la imagen. Si se puede reducir la cantidad de datos que representan a una imagen, entonces tanto el tiempo de transferencia como el espacio de almacenamiento se reducirán. De este modo, la compresión de imágenes puede representar un gran ahorro de recursos.

Dentro de la compresión de imágenes existen dos tipos: compresión sin pérdida (por ejemplo, el formato BMP) y compresión con pérdida (por ejemplo, el formato JPG). La figura 2.10 muestra esta clasificación.

Figura 2.10 Clasificación de imágenes de acuerdo a la compresión

Como ya se mencionó, cada formato gráfico está determinado por una definición de estructura interna. En este capítulo, se presenta la descripción del formato BMP por ser éste el que se utilizó para la inserción de las marcas de agua.

2.2.2. *FORMATO BMP*

El formato BMP es el formato estándar de MS-Windows.[6] Los archivos BMP se almacenan en un formato independiente del dispositivo. Esto quiere decir que el mapa de bits especifica el color del píxel en forma independiente al método usado para desplegar el color.

Estructura del archivo BMP. Cada archivo BMP contiene un encabezado, información del encabezado, una tabla de color (opcional) y un arreglo de bytes que

definen los bits de la imagen, como se puede ver en la tabla 2.2. El encabezado contiene información acerca del tipo, tamaño y estructura del archivo. La información del encabezado especifica las dimensiones, tipo de compresión y formato de color del mapa de bits. La tabla de color contiene tantos elementos como colores tenga el mapa de bits. No existe tabla de color para mapas de bits de 24 bits puesto que cada píxel es representado directamente por valores rojo-verde-azul de 24 bits en el área de datos (al final del archivo). Si existe una tabla, los colores deben aparecer ordenados por grado de importancia. Esto ayuda al manejador de video a desplegar un mapa de bits en un dispositivo que no cuente con todos los colores presentes en la imagen.

La estructura BITMAPINFO se puede usar para representar la información combinada de encabezado y tabla de color. Los bits de datos, que aparecen enseguida de la tabla de color, consisten en un arreglo de bytes que representan filas consecutivas de la imagen. Cada fila (o renglón) consiste de bytes que representan los píxeles en ese renglón de la imagen, de izquierda a derecha. El número de bytes que representan un renglón depende del formato de color y el ancho de la imagen (en píxeles). En caso necesario, el renglón debe completarse con ceros para obtener un tamaño en múltiplos de 32 bits.

Tabla 2.2 Estructura del archivo BMP

Nombre		Tamaño	Descripción
Encabezado		14 bytes	Estructura de Windows: BITMAPFILEHEADER
	Firma	2 bytes	'BM'
	Tamaño archivo	4 bytes	Tamaño de archivo en bytes
	Reservado	4 bytes	no usado (=0)
	Offset de datos	4 bytes	Offset del archivo para inicio de datos
Información-Encabezado		40 bytes	Estructura de Windows: BITMAPINFOHEADER
	Tamaño	4 bytes	Tamaño de Inf-Encabezado =40
	Ancho	4 bytes	Ancho de la imagen (en píxeles)
	Altura	4 bytes	Altura de la imagen (en píxeles)
	Planos	2 bytes	Número de planos (=1)
	Código	2 bytes	Bits por píxel 1 = paleta monocroma. NumColors = 1 4 = 4bit con paleta. NumColors = 16 8 = 8bit con paleta. NumColors = 256 16 = 16bit RGB. NumColors = 65,536 24 = 24bit RGB. NumColors = $16x10^6$
	Compresión	4 bytes	Tipo de Compresión 0 = BI_RGB sin compresión 1 = BI_RLE8 compresión RLE de 8 bits 2 = BI_RLE4 compresión RLE de 4 bits

	Tamaño de imagen	4 bytes	(comprimida) Tamaño de imagen Válido poner 0 si no hay compresión
	Xpixels	4 bytes	resolución horizontal: píxeles/metro
	Ypixels	4 bytes	resolución vertical: píxeles/metro
	Colores usados	4 bytes	Número de colores usados
	Colores Importantes	4 bytes	Número de colores importantes 0 = todos
Tabla de color		4 bytes * Colores usados	Presente sólo si Código <= 8 Los colores deben ordenarse por importancia
	Rojo	1 byte	Intensidad de rojo
	Verde	1 byte	Intensidad de verde
	Azul	1 byte	Intensidad de azul
	Reservado	1 byte	no usado (=0)
	repetir “Colores Usados” veces		
Datos de la imagen		3 bytes por píxel	Datos de cada píxel

El miembro que llamamos “código” en la tabla de color determina el número de bits que definen cada píxel y el número máximo de colores en la imagen. Código puede tener los siguientes valores:

Valor	Significado
1	El mapa de bits es monocromático y la tabla de colores tiene dos entradas. Cada bit en el arreglo representa un píxel. Si el bit es cero, el píxel se despliega con el color señalado en la primer entrada de la tabla de color. Si el bit es uno, el píxel adquiere el color señalado en el segundo registro de la tabla.
4	El mapa de bits tiene un máximo de 16 colores. Cada píxel en el mapa de bits se representa por un índice de 4 bits en la tabla de colores.
8	El mapa de bits tiene un máximo de 256 colores. Cada píxel en el mapa de bits se representa por un índice de 1 byte en la tabla de colores.
24	El mapa de bits tiene un máximo de 16,777,216 colores. Cada secuencia de 3 bytes en el mapa de bits representa las intensidades relativas de rojo, verde y azul, respectivamente, para cada píxel.

Portabilidad del formato BMP. Aunque el formato BMP fue inventado para la plataforma MS-DOS, muchos programas de otras plataformas también pueden leerlo y escribirlo.

Derechos de autor. Finalmente debe notarse que el formato BMP no causa cargos por su uso. Este dato es de suma importancia cuando se desea diseñar aplicaciones que produzcan archivos gráficos, a fin de no caer en una violación a los derechos de autor de alguien más.

---

[1] Gabriel Orea. "Diseño de un sistema de Esteganografía: Incrustación y Extracción de Información Privada en Imágenes Digitales no Comprimidas", UNAM, 2003

[2] J. Foley. "Computer Graphics", *Principles and Practice, Reading,* Addison Wesley, New York, 1990.

[3] R. Woods, S. Eddins, R. Gonzalez. "Digital Image Processing", Prentice Hall, New Jersey, 2004.

[4] Stefan Katzenbeisser, Fabien A. P.,Petitcolas. "Information Hiding", *Principles of Steganography,* Artech House, London, 2000.

[5] Sanjit K. Mitra. "Digital Signal Processing", McGraw-Hill, New York, 2001.

[6] Baxes Gregory. "Digital Image Processing", *Principles and Applications,* Wiley, 1994.

CAPÍTULO III

TRANSFORMADA DEL COSENO DISCRETO Y TRANSFORMADA WAVELET

Actualmente las técnicas de cambio de dominio son más empleadas que las técnicas en el dominio del espacio, debido a que muestran las características de frecuencia de una imagen espacial y así lograr una amplia manipulación de la información y en este caso de la imagen, lo cual permite dar mayor seguridad y robustez a las marcas de agua.[1]

3.1. TRANSFORMADA DEL COSENO DISCRETO

La *transformada del coseno discreto* (TCD) es uno de los dominios más populares para marcas de agua[2] y la *transformada wavelet discreta* (TWD) es la técnica que se propone en este trabajo, por lo que en este capítulo se explican ambas herramientas, para compararlas posteriormente entre sí en el capítulo cinco.

3.1.1. *TCD DE UNA DIMENSIÓN*

La transformada del coseno discreto consiste en mapear uno a uno una serie de valores de los píxeles de la imagen en el dominio del tiempo a una serie de valores en el dominio de la frecuencia. Sujeta a los efectos aritméticos, la transformación es reversible.

Suponiendo que se necesita una imagen de una dimensión, que consiste en una serie lineal de N pixeles, donde cada uno se encuentra dentro de una escala de gris $p(x)$ $(0 \le x < N)$, donde, $p(x)$ es una función que varía en el espacio.[3] Esta imagen puede ser representada como la suma de las componentes espectrales f con un rango de frecuencias de 0 a N-1:

$$\begin{aligned} p(x) &= \sqrt{\frac{2}{N}} \sum_{f=0}^{N-1} C(f) S(f) \cos\left[\frac{(2x+1)\pi f}{2N} \right] \\ &= \frac{S(0)}{\sqrt{N}} + \sqrt{\frac{2}{N}} \sum_{f=1}^{N-1} S(f) \cos\left[\frac{(2x+1)\pi f}{2N} \right] \end{aligned} \tag{3.1}$$

donde:

$$C(f) = \begin{cases} 1/\sqrt{2} & f = 0 \\ 1 & f > 0 \end{cases}$$

Para llegar a la formulación de la ecuación (3.1), se necesita calcular los coeficientes:

$$\{S(f), \quad 0 \le f < N\}$$

El primer término de la ecuación (3.1) es la componente constante, o componente de frecuencia cero. Este término puede ser igual al valor aproximado de *p(x)*, de tal forma que:

$$S(0) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} p(x)$$

La ecuación general para *S(f)* es:

$$S(f) = \sqrt{\frac{2}{N}} C(f) \sum_{x=0}^{N-1} p(x) \cos\left[\frac{(2x+1)\pi f}{2N}\right] \qquad (3.2)$$

La ecuación (3.2) es llamada TCD de una dimensión de *p(x)*, y la ecuación (3.1) es el inverso TCD de *S(f)*.

3.1.2. *TCD DE DOS DIMENSIONES*

Una matriz de *N*x*N* píxeles pueden ser representados por una suma de *N*x*N* funciones coseno. Esta relación es:

$$p(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)S(u,v) \cdot \cos\left[\frac{(2x+1)\pi u}{2N}\right] \cos\left[\frac{(2y+1)\pi v}{2N}\right] \qquad (3.3)$$

donde:

$$S(0,0) = \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} p(x.y)$$

La ecuación general para *S(f)* es:

$$S(u,v) = \frac{2}{N}C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} p(x,y)\cdot \cos\left[\frac{(2x+1)\pi u}{2N}\right]\cos\left[\frac{(2y+1)\pi v}{2N}\right] \qquad (3.4)$$

La ecuación (3.4) es llamada TCD bidimensional de *p(x,y)*.

Las frecuencias se van colocando en orden de zig-zag como lo muestra la figura 3.1 quedando en la posición (1,1) la frecuencia más baja y en la posición (8,8) la más alta.[4]

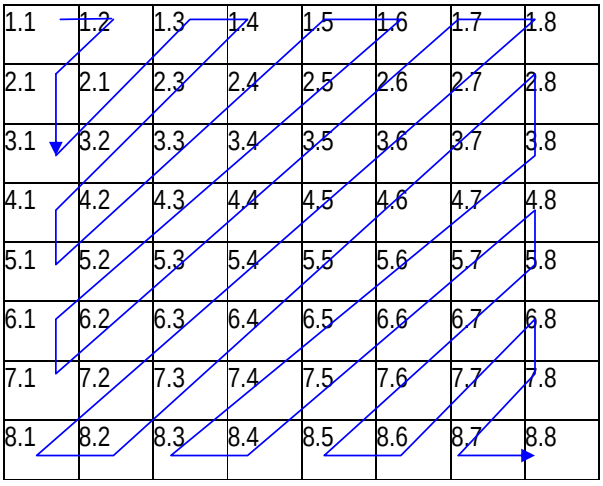


Figura 3.1. Posición de las frecuencias

3.1.3. *TCD PARA APLICACIONES DE MARCAS DE AGUA*

Los métodos de transformación del dominio ocultan el mensaje en áreas significativas de la imagen de cobertura, lo cual hace que éste sea más robusto ante ataques como lo es una compresión, permitiendo tener una marca de agua más resistente.[5]

Durante el proceso de codificación, se divide la imagen de cobertura en bloques de 8x8 píxeles; en cada bloque se recomienda codificar no más de 3 bits del mensaje. El proceso de inserción comienza seleccionado un bloque pseudoaleatorio *Bi* el cual puede ser usado para codificar el *i-ésimo* bit del mensaje. Siendo el bloque de la imagen transformado con la TCD.

Se localizan dos coeficientes del bloque, los cuales serán usados en el proceso de inserción; quedando denotados ambos índices por *(u1 ,v1)* y *(u2 , v2)*, ambos coeficientes corresponden a las frecuencias medias bajas; esto asegura que la información sea almacenada en una parte significante de la señal. Además, se puede asumir que el proceso de inserción no degenerará la cobertura, porque los valores de los coeficientes en las frecuencias medias tienen magnitudes similares.[1]

Un bloque codifica un "1" si $Bi\ (u1\ ,v1) \geq Bi\ (u2\ ,\ v2)$, de lo contrario codifica un "0". Al aplicar una compresión puede que ésta modifique el tamaño de los coeficientes, por lo que es recomendable que $|Bi\ (u1\ ,v1) - Bi\ (u2\ ,\ v2)| > x$ para cualquier $x > 0$, lo cual puede ser sumando valores aleatorios a ambos coeficientes. Entre más grande sea el valor que se escoja para *x*, más grande es el grado de robustez con respecto a la compresión, como quiera que sea afectará a la calidad de la imagen. Después se ejecuta la DCT inversa para regresar los coeficientes al dominio del espacio.

Por ejemplo la figura 3.2a muestra el primer bloque de 8x8 píxeles de una imagen que al aplicarle la TCD de dos dimensiones se obtiene la figura 3.2b, donde se van acomodando las frecuencias en forma de zig-zag.

116	106	91	81	79	76	73	69
109	116	114	98	107	103	97	88
131	129	134	130	121	117	111	105
144	127	123	113	110	108	104	101
134	120	115	89	75	73	68	65
126	115	119	94	92	86	77	68
121	109	128	121	128	119	105	89
118	122	125	126	121	113	105	99

a)

849.5	100.4	-4.39	10.7	-7.5	3.671	9.664	10.17
-27.9	-0.21	19.45	1.241	-1.89	-4.48	-4.87	-3.09
-8.21	-27.2	-17.2	2.772	0.208	-4.77	-6.01	-1.04
-85.6	31.47	17.15	4.919	-3.22	-0.4	3.988	4.59
-27.3	16.25	21.51	-0.84	5.25	0.797	-2.96	-6.07
26.89	-11.4	-4.96	8.717	7.749	5.269	2.079	1.085
-2.82	10.34	4.241	-5.64	1.808	1.585	-1.6	-4.17
-3.14	6.532	-3.92	-3.63	1.17	4.014	1.07	-1.98

b)

Figura 3.2 a)Bloque de 8x8 píxeles de una imagen, b) Bloque después de aplicar la TCD

3.2. TRANSFORMADA WAVELET

Las wavelets proveen un poderoso y muy variado grupo de herramientas para enfrentar problemas fundamentales en la ciencia y la ingeniería. Para ejemplificar tan solo algunos de los problemas que han logrado ser resueltos aplicando wavelets, se muestra la siguiente lista.

- Eliminación de ruido en audio
- Eliminación de ruido en imágenes
- Compresión de señales
- Reconocimiento de patrones

Y ahora se propone con este trabajo la aplicación de wavelets para inserción de marcas de agua robustas en imágenes.

El análisis de tiempo-frecuencia se puede ver y entender de dos formas distintas: física y matemáticamente, siendo la última la que nos permite ver cómo es que las propiedades espectrales de la señal cambian con el tiempo.[6] Las wavelets son una técnica que permite estudiar la estructura tiempo-frecuencia de las señales.

El análisis wavelet es un desarrollo reciente en el análisis matemático que tiene numerosas aplicaciones en matemáticas, física e ingeniería.[7] Las wavelets son funciones de la forma:

$$\psi_{j,k}(x) = a^{j/2}\psi\left(a^{j}x - kb\right) \tag{3.5}$$

Donde $\psi \in L^2(R)$, $a > 0$, $b \in R$, y j,k son enteros. Esto es, las wavelets son funciones generadas por una sola función ψ (la wavelet madre). El estándar propone que a y b sean $a = 2$ y $b = 1$.

Los coeficientes de la wavelet de $f \in L^2(R)$ son definidos como:

$$\tilde{f}(j,k) = \int_{-\infty}^{\infty} f(x)\overline{\psi}_{j,k}(x)dx \tag{3.6}$$

y la serie $\sum_{j,k=-\infty}^{\infty} \tilde{f}(j,k)\psi_{j,k}(x)$ es llamada la serie wavelet asociada con f.

3.2.1. *TRANSFORMADA WAVELET DISCRETA (TWD)*

La señal *x[n]* se pasa a través de un banco de filtros espejo en cuadratura.[8] La señal resultante de cada filtro es diezmada por un factor de 2.

La resolución de la señal, la cual es una medida de la cantidad detallada de la información dentro de la señal, se modifica por la acción de filtrado y la escala se modifica por la operación de diezmado. El diezmado de una señal corresponde a la reducción de la velocidad de muestreo, o a la eliminación de algunas de las muestras de la señal. A este proceso de filtrado y diezmado sucesivo se le conoce como codificación en sub-bandas como se muestra en la figura 3.3.

Este procedimiento puede expresarse como:

$$y_{alto}[k] = \sum_{n} x[n] \cdot g[2k - n] \tag{3.7}$$

y

$$y_{bajo}[k] = \sum_{n} x[n] \cdot h[2k - n] \tag{3.8}$$

donde $y_{alto}[k]$ y $y_{bajo}[k]$ son las salidas de los filtros pasa altas y pasa bajas respectivamente, después del diezmado por 2.

De este modo opera la transformada wavelet discreta (TWD), esta acción analiza la señal en diferentes bandas de frecuencia con diferentes resoluciones mediante la descomposición de la señal en componentes de mayor y menor energía. La descomposición de la señal en diferentes bandas de frecuencia se obtiene mediante el filtrado sucesivo de la señal como se muestra en la figura 3.3. La secuencia original *x[n]* se pasa por un filtro pasa altas *g[n]* y uno pasa bajas *h[n]*.

La codificación en sub-bandas puede repetirse cuantas veces sea necesario para una mayor descomposición. Cada nivel de filtrado y diezmado resultará en la mitad del número de muestras y por lo tanto, en la mitad de la resolución en el tiempo. Dependiendo de la wavelet elegida, los coeficientes de *g[n]* y *h[n]* cambiarán.

Existen diferentes tipos de transformadas wavelets, pero en este trabajo solo se menciona la transformada wavelet Haar, puesto que después de varias pruebas realizadas con ataques, ésta fue la que conservó más integra la marca de agua (debido a la forma en que distribuye la energía) por lo que es la más apropiada para la aplicación, y sólo se aplicará la transformada al primer nivel.[9]

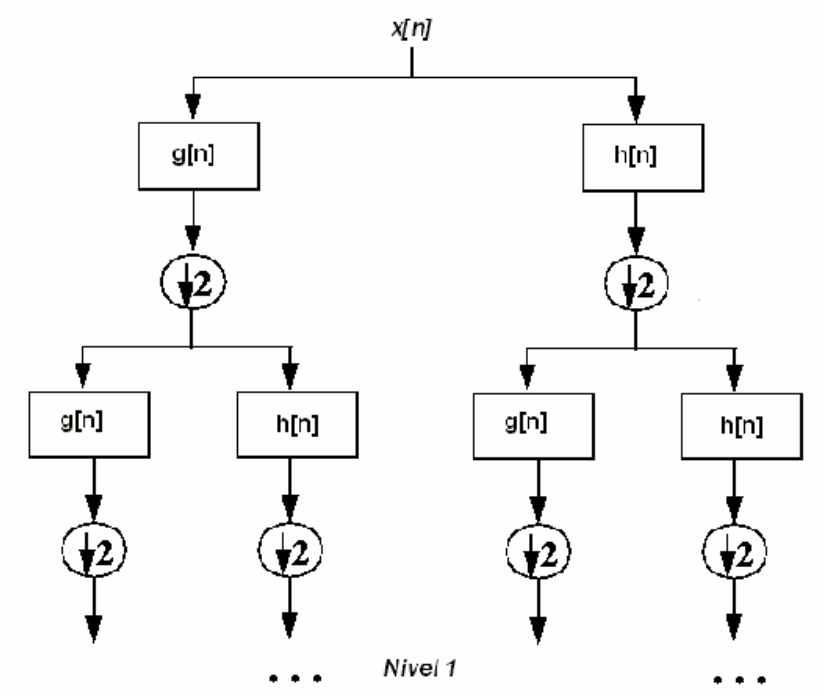


Fig. 3.3 Algoritmo de codificación en sub-bandas

3.2.2. *TRANSFORMADA HAAR*

Al igual que todas las demás transformadas wavelets, la *transformada Haar* descompone una señal discreta en dos sub-señales de la mitad de longitud. La sub-señal a es conocida como el promedio y la otra sub-señal d como la diferencia. Entonces se tiene una señal discreta de la forma $f = (f_1, f_2, ..., f_N)$, donde N es un entero positivo la sub-señal promedio es calculada con la siguiente fórmula:

$$a_m = \frac{x_{2m-1} + x_{2m}}{\sqrt{2}} \tag{3.9}$$

para $m = 1,2,3,..., N/2$

Continuando de la misma forma la sub-señal diferencia se obtienen con la siguiente fórmula:

$$d_m = \frac{x_{2m-1} - x_{2m}}{\sqrt{2}} \tag{3.10}$$

para $m = 1,2,3,..., N/2$

Quedando las frecuencias bajas en a y las altas en d.

3.2.3. *TRANSFORMADA WAVELET DISCRETA EN DOS DIMENSIONES*

Una imagen discreta X es una matiz de M renglones por N columnas de números reales, donde M y N deben ser pares:

$$x = \begin{pmatrix} x_{1,M} & x_{2,M} & \cdots & x_{N,M} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,2} & x_{2,2} & \cdots & x_{N,2} \\ x_{1,1} & x_{2,1} & \cdots & x_{N,1} \end{pmatrix}$$

La transformada wavelet de dos dimensiones, se obtiene con las mismas fórmulas que para las de una dimensión, realizando los dos pasos siguientes:

a) Aplicar la transformada wavelet a cada fila de *X*, lo cual producirá una nueva matriz.

b) A esta nueva matriz obtenida en el paso anterior, aplicar nuevamente la transformada wavelet, pero esta vez a cada columna.

Quedando cuatro sub-imágenes de *M*/2 filas y *N*/2 columnas:

$$f \rightarrow \begin{pmatrix} a^1 & | & h^1 \\ - & & - \\ v^1 & | & d^1 \end{pmatrix} \tag{3.11}$$

$\boldsymbol{a^1}$ se calcula con el promedio de las filas seguido por el promedio de las columnas, quedando en esta sub-imagen una compresión de la original, albergando las frecuencias bajas.

$\boldsymbol{h^1}$ es calculada con el promedio de las filas y la diferencia de las columnas; aquí se conservan los detalles horizontales de la imagen, y contiene las frecuencias medias-bajas.

$\boldsymbol{v^1}$ es similar a h^1, excepto que los roles de vertical y horizontal son cambiados, esta sub-imagen contiene los detalles verticales, conservando las frecuencias medias-altas.

$\boldsymbol{d^1}$ va a contener los detalles diagonales, porque se obtiene de la diferencia tanto de filas como de columnas y conserva las frecuencias altas.

La figura 3.4 muestra de manera visual la descomposición en frecuencias de una imagen aplicando la transformada Wavelet a un nivel, si a esta misma imagen aplicamos la transformada wavelet en dos niveles, tenemos como resultado la figura 3.5.

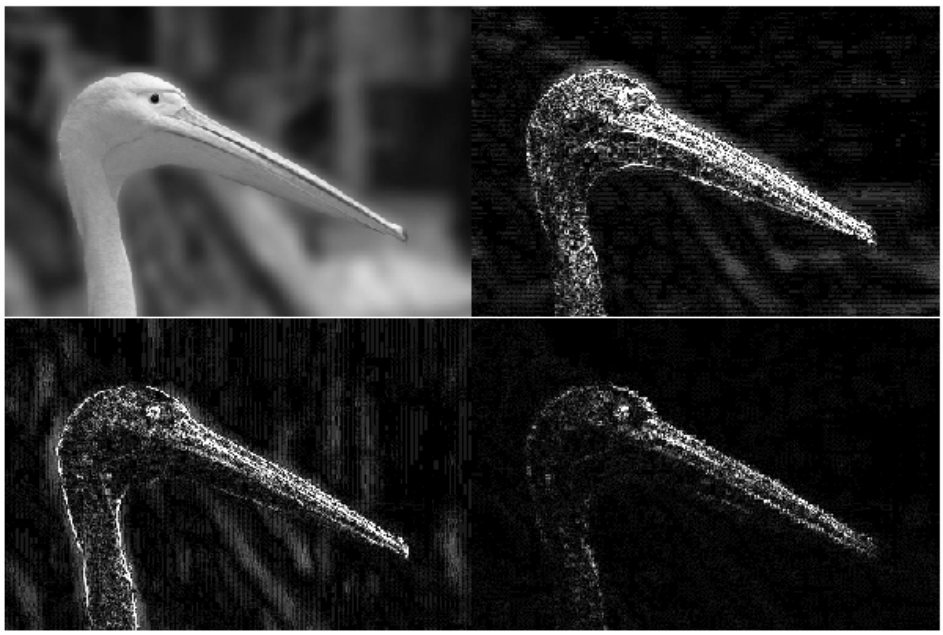


Figura 3.4 Transformada Wavelet de un nivel

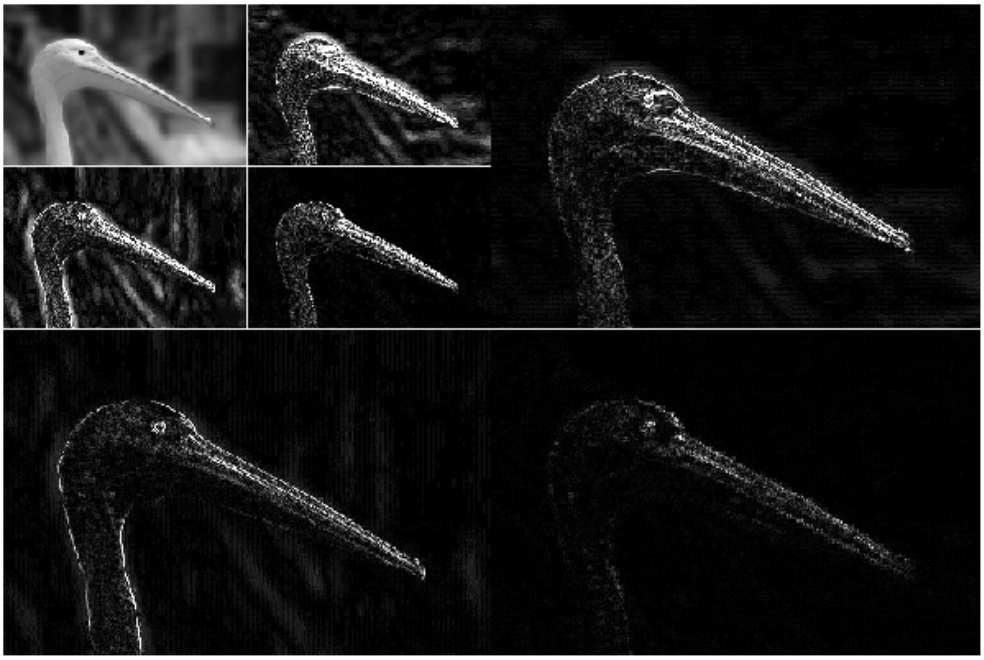


Figura 3.5 Transformada Wavelet de dos niveles

3.2.4. *TWD PARA APLICACIONES DE MARCAS DE AGUA*

Una vez que se tienen las sub-matrices a^1, h^1 ,v^1 y d^1, la matriz a^1 se conserva intacta porque aquí se concentran las frecuencias bajas; alterar estas frecuencias podría ser visualmente perceptible por lo que no es recomendable,[10] y las matrices v^1 y d^1 tampoco se utilizan para insertar la marca de agua ya que son frecuencias medias altas y altas respectivamente, siendo las más vulnerables a cualquier tipo de ataque. Queda entonces únicamente la sub-matriz h^1 que contiene las frecuencias medias bajas, siendo la parte más robusta a los ataques después de las frecuencias bajas, y con la diferencia de que los cambios que se realicen no son perceptibles.

Se inserta la marca de agua de la siguiente manera: se va a ir recorriendo la matriz y se van a comparar el primer par de elementos, si el primero es mayor al segundo se considera como un valor 1, de lo contrario como un 0, después se compara el siguiente par y se realiza el mismo criterio de inserción hasta recorrer toda la matriz. Se pueden manipular los elementos para incrustar el valor deseado, por ejemplo si el primer valor es menor que el segundo y se quiere que sea mayor, se va incrementado hasta que sea mayor que el segundo o simplemente se intercambian.

Esta es la mejor manera de incrustar la marca de agua debido a que están concentradas todas las frecuencias medias bajas en forma consecutiva en esta matriz, entonces los elementos tienen valores muy cercanos unos con otros y al ser intercambiados o manipulados los cambios afectan de modo despreciable a la imagen, esto lo podremos comprobar en el capítulo 5, al realizar las pruebas. Otra ventaja de insertar la información de esta manera es que siempre será resistente a la distorsión de brillo, ventaja que también se demuestra en las pruebas en el último capítulo.

---

[1] Stefan Katzenbeisser, Fabien A. P.,Petitcolas. “Information Hiding”, *Principles of Steganography*, Artech House, London, 2000.

[2] Patrick Loo, Nick Kingsbury. “Digital Watermarking with Complex Wavelets”, IEE Proc. Colloquium on Secure Images and Images Authentication, London, 2000.

[3] D. Knuth. “The Art of Computer Programming”, Vol. 2, Seminumerical Algorithms, 2a ed., Addison - Wesley, 1981.

[4] Izlian Orea. “Intercambio de información utilizando protocolos de canal subliminal”, UPIITA-IPN, 2002.

[5] Bruce Schneirer. “Applied Cryptography”, John Wiley and Sons, Inc., 1994.

[6] Lokenath Debnath. “Wavelets and Signal Processing”, Birkhäuser, 2002,pp. 106.

[7] John J. Benedetto. Ahmed I. Zayed, "Sampling, Wavelets, and Tomography", Birkhäuser, 2003, pp. 11-17.

[8] Sanjit K. Mitra. "Digital Signal Processing: a computer based approach", Ed. McGraw-Hill International, 2a ed., pp. 88-94, 2003.

[9] M. A. Acevedo, I. Orea-Flores, J. López-Bonilla, "Wavelets and Discrete Cosine Transform for Hidden Information into Images", Sampling Theory in Signal and Image Processing (STSIP Journal), New York, 4, No.2, pp.141-150, May 2005.

James S. Walter. "A Primer on WAVELETS and their Scientific Applications", Chapman & Hall/CRC Press, London, 1999.

Martin Vetterli, Jelena Kovacevic. "WAVELETS and sub-band coding", Prentice Hall, New Jersey, 1995.

[10] M. A. Acevedo, I. Orea-Flores, J. López-Bonilla, "Wavelet Transform for Watermarks in Digital Images", Proceeding of the Pakistan Academy of Sciences, 42, No.2, June 2005, in print..

CAPÍTULO IV

ATAQUES

Una vez que la marca de agua ha sido introducida en un documento digital es susceptible a un amplio abanico de ataques que, según la causa y objetivo que los originan, se pueden agrupar en ataques *intencionados* y *no intencionados*.[1] Los ataques intencionados pretenden eliminar la imagen o al menos distorsionarla, pero teniendo cuidado de no modificarla de forma visible.

A lo largo de este capítulo se explican las características y se dan ejemplos de ambos tipos de ataques, pero se da un peso mayor a la parte sobre ataques intencionados.

4.1. ATAQUES NO INTENCIONADOS

Los ataques no intencionados son aquellos a los que la marca de agua está sometida de manera casi inevitable.

Ejemplos claros son:

- El propio proceso de recuantificación del documento marcado antes de ser expedido.
- El ruido introducido por el canal de transmisión por el que se envía dicho documento marcado.

A menos que se esté transmitiendo por un canal muy ruidoso las marcas de agua van a sobrevivir en general a este tipo de ataques, por lo que la atención de los creadores de las mismas está enfocada en el otro tipo de ataques, los intencionados.

4.2. ATAQUES INTENCIONADOS

Existen varios tipos de ataques para tratar de eliminar una marca de agua. Pero cabe mencionar que **para que un ataque sea efectivo, debe eliminar la marca de agua sin modificar de manera visible a la imagen**.[2]

Hay una gran variedad de ataques intencionados, pero solo se analizarán los tres más agresivos: compresión, distorsión de brillo y ruido.

Primero es necesario aclarar que los histogramas de todas las fotografías se realizaron para el equivalente en niveles de gris de las imágenes, porque para las fotografías a color se tendrían que hacer tres histogramas -uno para cada plano-.

4.2.1. *COMPRESIÓN*

Es cuando se aplica cualquier método de compresión a la imagen para tratar de eliminar la marca de agua y luego se regresa al formato original. Lo anterior es muy claro por lo que no es necesario ahondar más, pero veamos un ejemplo. Las dos siguientes figuras muestran del lado izquierdo una fotografía y del lado derecho su histograma, con la diferencia de que la figura 4.1 es la foto original (archivo BMP) y la 4.2 es la foto comprimida (archivo JPG).

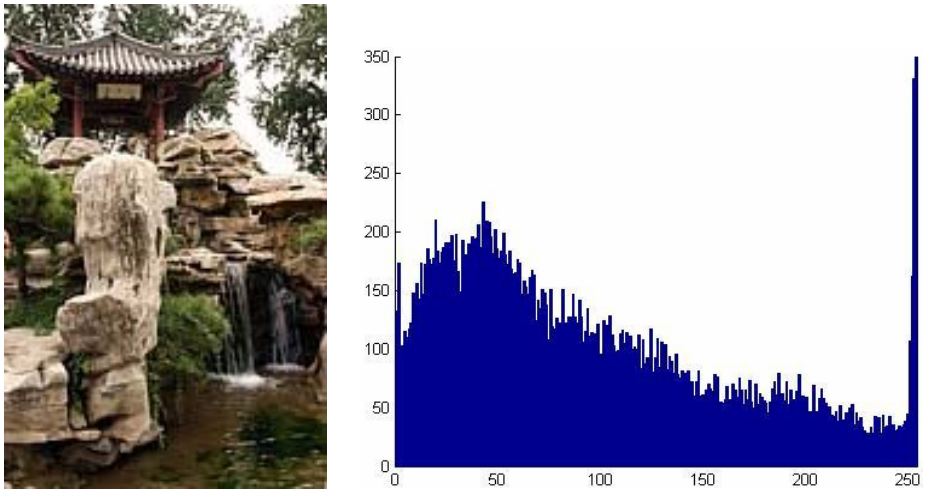


Figura 4.1 Jinan.bmp

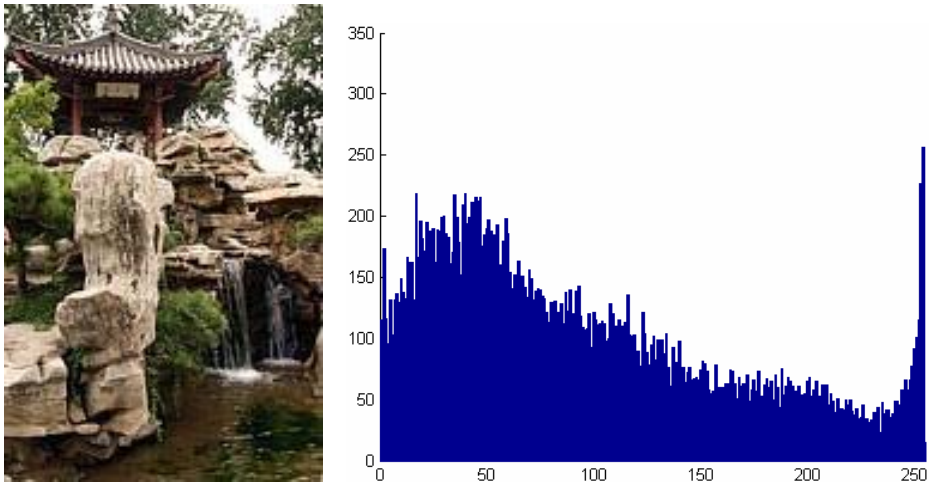


Figura 4.2 Jinan.jpg

Podríamos pasar horas tratando de encontrar la diferencia entre ambas imágenes y nunca lo lograríamos, y más asombroso resulta ver que aún sus respectivos histogramas son casi iguales. Esto muestra lo efectivo que puede resultar este tipo de ataque.

4.2.2. *DISTORSIÓN DE BRILLO*

Este tipo de ataque consiste en sumarle a cada píxel de la imagen un valor pequeño para modificarla completamente sin que se note visualmente. La modificación se realiza de manera uniforme.[3]

Entonces, lo que pasa con la fotografía es que se va a cambiar su intensidad de brillo.

Vamos a ver un ejemplo que es con un valor mucho muy grande sólo para mostrar visualmente el efecto provocado. Obviamente, para llevar a cabo un ataque se tendrá que realizar con un valor más pequeño, para no provocar alteraciones visibles.

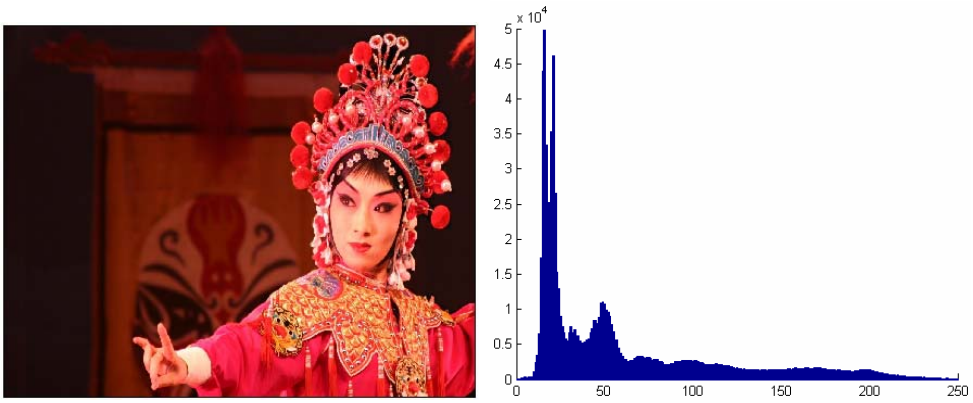


Figura 4.3 Mujer China

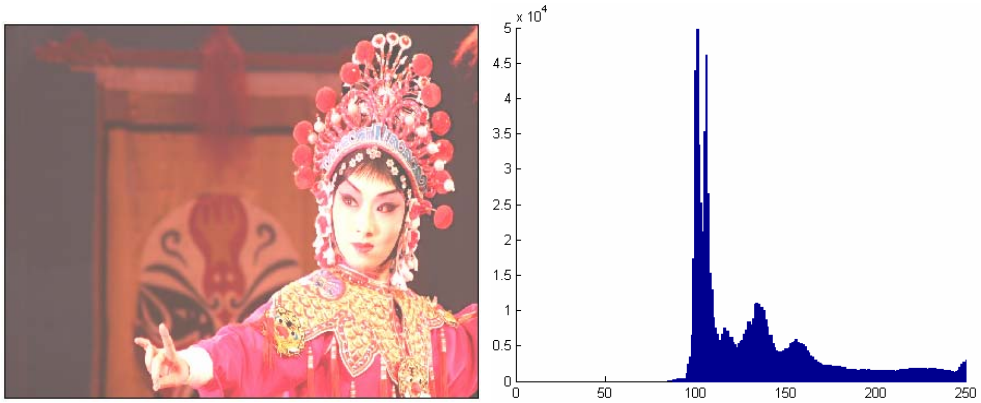


Figura 4.4 Mujer China con Distorsión de Brillo

La figura (4.3) ilustra la fotografía antes de ser alterada, mientras que la figura (4.4) muestra la imagen con un incremento uniforme con valor de 80, el cual sumamos a cada elemento. Vemos que la imagen pierde color porque, con el incremento, movemos todos los valores en dirección al blanco (255). Esto se comprende mejor si comparamos los histogramas correspondientes.

4.2.3. RUIDO

Existen diferentes tipos de ruido que se pueden añadir a la imagen para alterarla con el fin de modificar la marca de agua, dejarla ilegible o incluso eliminarla.

Es necesario mencionar que todas las pruebas fueron hechas en Matlab y ésta herramienta normaliza los parámetros numéricos; los parámetros correspondientes a las operaciones con imágenes se encuentran en un rango de intensidad de 0 a 1, por lo cual al sumarle algún tipo de ruido a la imagen con varianzas o densidades muy pequeñas el cambio será más notorio. Los valores presentados en todos los ejemplos con ruido son los que se usaron en Matlab, pero para conocer el valor real se tendría que hacer el escalamiento. Por ejemplo, para añadir ruido gaussiano con una media de 36 y una varianza de 65 a una imagen, se escala la media con la operación 36/255 y la varianza con $65/(255)^2$. Entonces si un ejemplo dice que es una imagen afectada con ruido con una varianza de 0.001, el valor real será $0.001x(255)^2 = 65.025$.

4.2.3.1 Ruido multiplicativo

El principio de este ruido es muy similar al de la distorsión de brillo. Se utiliza la ecuación 4.1 para sumar ruido a la imagen.

$$g = f + (nf) \tag{4.1}$$

Siendo f la imagen y n una distribución uniforme aleatoria con una media cero y una varianza *v*. El rango en el que n toma valores va a depender de *v*.

Este ruido suaviza la imagen de manera no uniforme, pero con una varianza pequeña suele ser muy sutil.

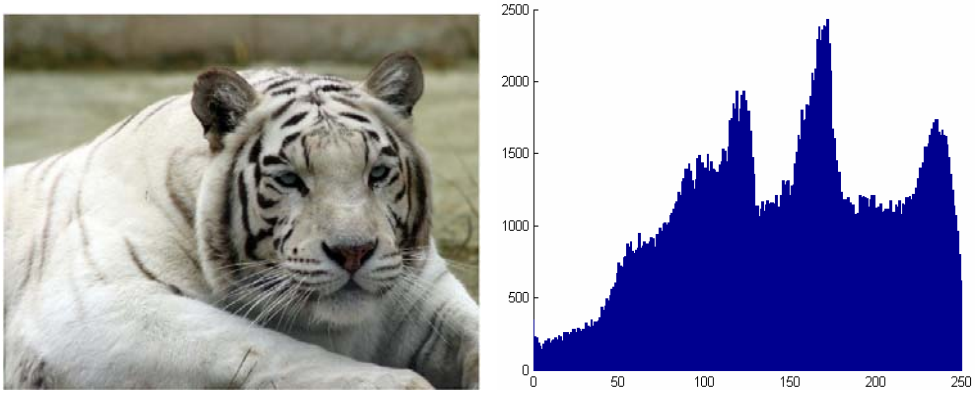


Figura 4.5 Tigre

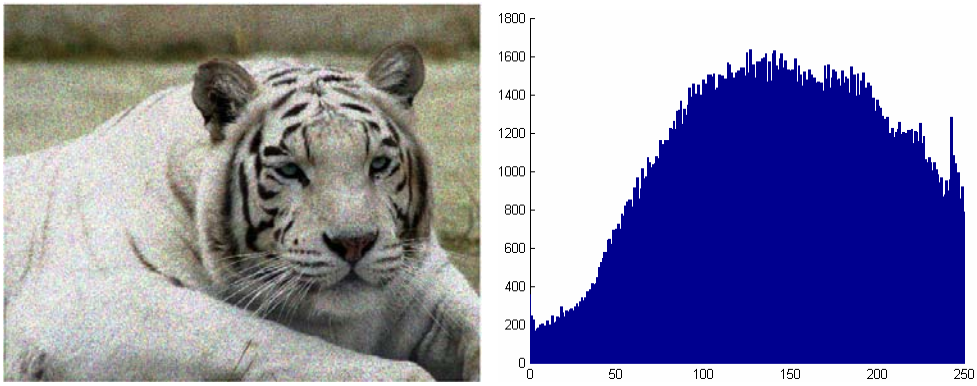


Figura 4.6 Tigre afectado por ruido multiplicativo de varianza 0.05

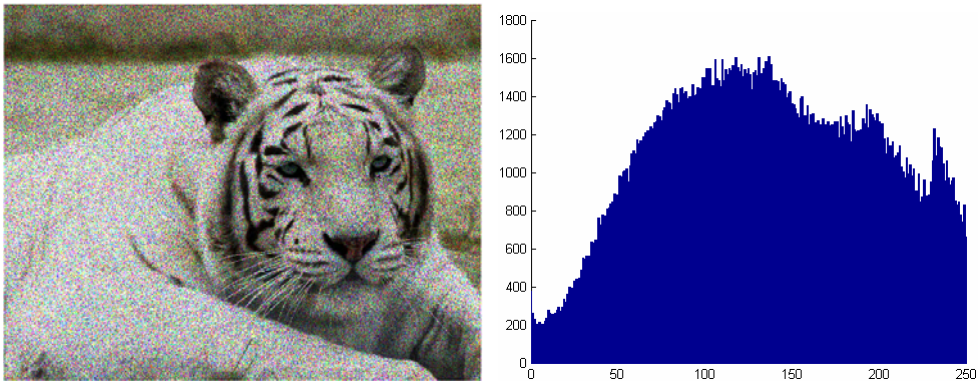


Figura 4.7 Tigre afectado por ruido multiplicativo de varianza 0.2

Las figuras 4.5, 4.6, y 4.7 son ejemplos de una fotografía afectada con diferentes varianzas para mostrar cómo el ruido multiplicativo las modifica de forma visual. Sus respectivos histogramas muestran los cambios.

4.2.3.2 Ruido Impulsivo

El ruido impulsivo es muy agresivo[4], suma diferentes valores a algunos píxeles de la imagen que selecciona de manera aleatoria. La cantidad de píxeles afectados está relacionada con la densidad de ruido, con la siguiente fórmula, *d* x *numel(f)*, siendo *d* la densidad dada y *numel(f)* el número de píxeles de la imagen *f*.[5] Los elementos alterados por este tipo de ruido son generalmente muy notorios en la imagen.

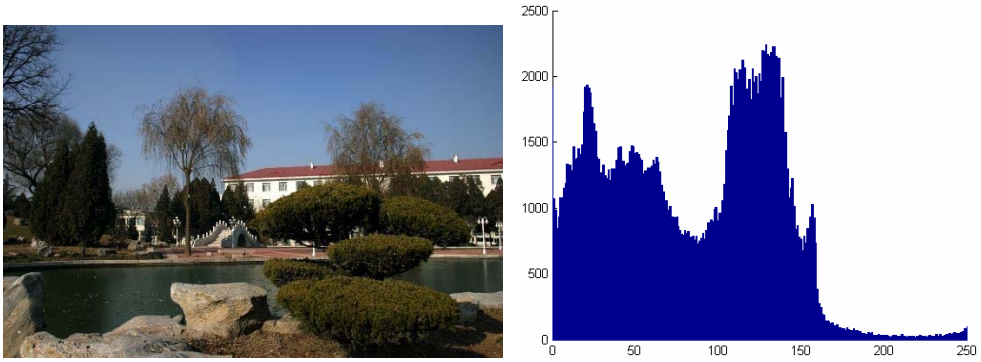


Figura 4.8 Paisaje

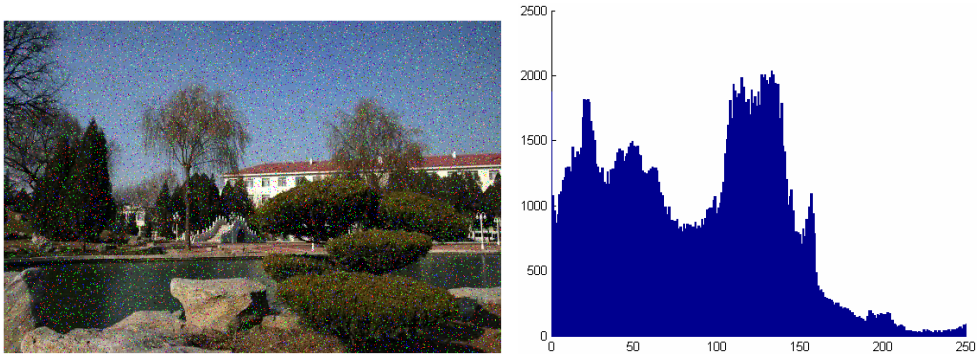


Figura 4.9 Paisaje afectado por ruido impulsivo con densidad 0.05

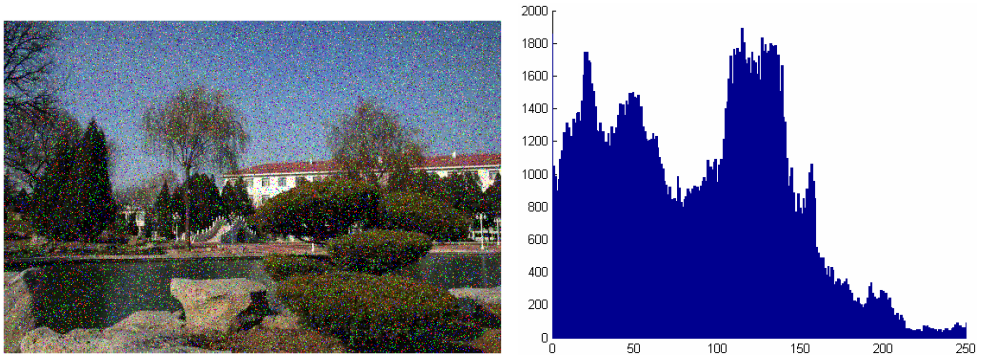


Figura 4.10 Paisaje afectado por ruido impulsivo con densidad 0.1

4.2.3.3 Ruido Gaussiano

Suma ruido con una distribución de probabilidad gaussiana (ver tabla 1), con media *m* y varianza *v*. Este ruido modifica toda la imagen.

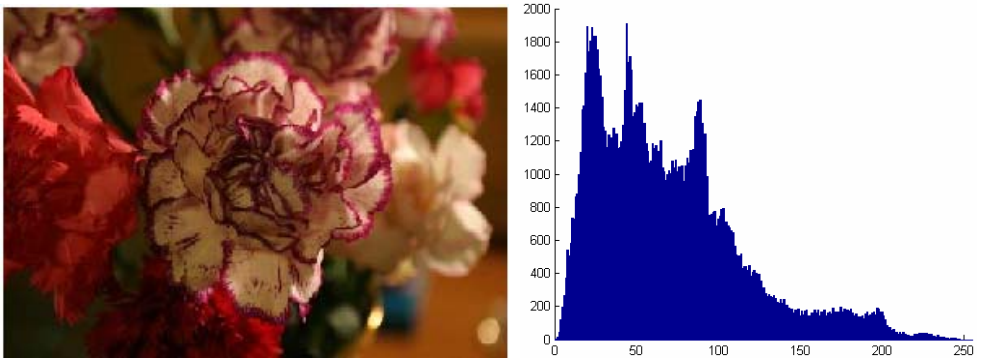


Figura 4.11 Clavel

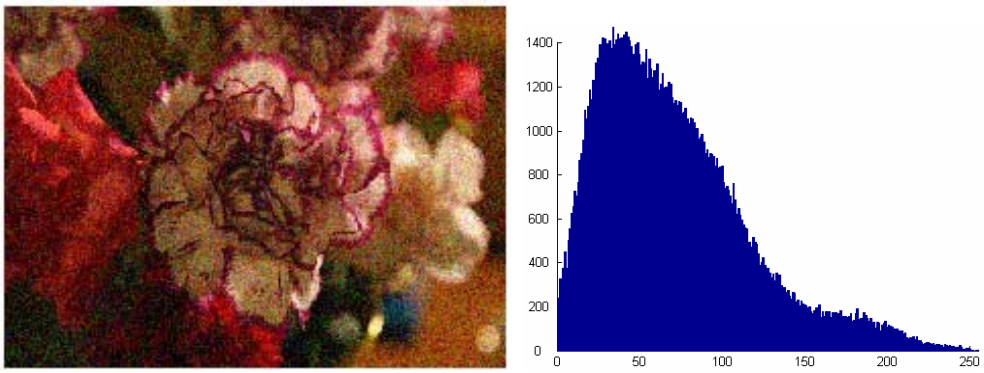


Figura 4.12 Clavel afectado por ruido gaussiano con varianza 0.01 y media 0

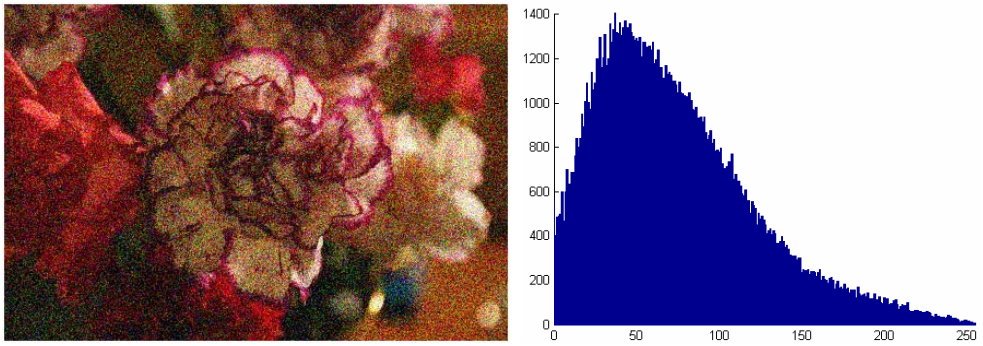


Figura 4.13 Clavel afectado por ruido gaussiano con varianza 0.03 y media 0

La figura 4.11 muestra la imagen original y su respectivo histograma, mientras que las figuras 4.12 y 4.13 dejan ver los cambios visuales de las imágenes después de afectarlas con ruido gaussiano, pero lo más sobresalientes de estas dos figuras son los histogramas que permiten ver claramente como cambió la distribución de probabilidad de la imagen hacia una distribución de probabilidad gaussiana.

Los modelos anteriores de ruido se consideran ruido en el dominio espacial. Los valores del ruido espacial son números aleatorios caracterizados por la función de densidad de probabilidad (FDP), o bien por la correspondiente función de distribución acumulativa (FDA). Los números aleatorios generados por los tipos de distribuciones siguen algunas reglas simples de la teoría de probabilidad. [5]

Los generadores de números aleatorios casi siempre se basan en la generación de números aleatorios con una FDA uniforme en el intervalo (0,1).

Ahora bien, si *w* es una variable aleatoria uniformemente distribuida en el intervalo (0,1), entonces se puede obtener una variable aleatoria *z* con una específica FDA, $F_{z,}$ que satisface la ecuación:

$$z = F_z^{-1}(w) \tag{4.2}$$

Y esto es equivalente a encontrar la solución de la ecuación:

$$F_z(z) = w \tag{4.3}$$

La tabla 4.1 muestra las ecuaciones generadoras de los números aleatorios para los modelos de ruido Gaussiano e Impulsivo.

Tabla 1. Generación de variables aleatorias

	Gaussiano	**Impulsivo**
FDP	$p_z(z) = \frac{1}{\sqrt{2\pi}b} e^{-(z-a)^2/2b^2}$ $-\infty < z < \infty$	$p_z(z) = \begin{cases} P_a & z = a \\ P_b & z = b \\ 0 & \text{otro caso} \end{cases}$ $b > a$
media y varianza	$m = a$ $\sigma^2 = b^2$	$m = aP_a + bP_b$ $\sigma^2 = (a-m)^2 P_a + (b-m)^2 P_b$
FDA	$F_z(z) = \int_{-\infty}^{z} p_z(v)dv$	$F_z(z) = \begin{cases} 0 & z < a \\ P_a & a \le z < b \\ P_a + P_b & b \le z \end{cases}$
Generador	Función aleatoria	Función aleatoria

[1] J.K. Su, J.J. Eggers, y B. Girod. "Capacity of Digital Watermarks Subjected to an Optimal Collusion Attack", *European Signal Processing Conference* (EUSIPCO 2000), Tampere, Finlandia, Sep/2000.

[2] S. Voloshynovskiy, S Pereira, T. Pun, JJ. Eggers and J. K. Su. "Attacks on Digital Watermarks: Classification, Estimation-based attacks and Benchmarks submitted", IEEE Communication Magazine, 2001.

[3] F. A. P. Petitcolas, R. J. Anderson, M. Kuhn, "Attacks on copyright marking systems", Artech House Publishers, 1998.

[4] S. Voloshynovskiy, S Pereira, V. Iquise, T. Pun "Towards a second generation watermarking benchmark Signal Processing", Special Issue on Information Theoretic Issues in Digital Watermarking, 2001.

[5] R. Woods, S. Eddins, R. Gonzalez, "Digital Image Procesing", Prentice Hall, 2004.

CAPÍTULO V
IMPLEMENTACIÓN Y PRUEBAS

El objetivo de esta tesis no es únicamente proponer una aplicación de inserción de marcas de agua robustas en imágenes aplicando la transformada wavelet discreta, sino también realizar una comparación con otra técnica para marcas de agua que utiliza la transformada del coseno discreto, técnica muy utilizada en el procesamiento digital de imágenes.

Este capítulo está dedicado a mostrar de manera analítica y no analítica los resultados obtenidos en diferentes pruebas de comparación de ambas técnicas, tales como la capacidad de inserción y el porcentaje de recuperación de la marca de agua al ser sometida a diferentes ataques.

5.1 CAPACIDAD DE INSERCIÓN EN UNA IMAGEN

Como se vio en el capítulo 3, las frecuencias bajas son las que almacenan la mayor cantidad de energía en una señal en general y en este caso en una imagen. Esto indica que se deben conservar estas frecuencias intactas porque de lo contrario los cambios que se realicen al insertar la información serán muy obvios pues distorsionarán la imagen de forma visible. Por lo tanto, podremos trabajar con las frecuencias medias – bajas, medias – altas y altas.

5.1.1. *INSERCIÓN APLICANDO LA TCD*

Ya se sabe que para realizar el cambio de dominio, la TCD lo realiza por bloques de 8x8 elementos, acomodando las frecuencias en forma de zig-zag yendo de la más baja a la más alta.

Entonces, respetaremos las frecuencias más bajas, área oscura de la figura 5.1, y usaremos las restantes para insertar información, tomando parejas y comparándolas para introducir los bits como se explica en el capítulo tres.

El proceso anterior se realiza en cada plano de la imagen, tanto en el de luminancia como en los dos de crominancia. Tanto en esta técnica como en la de la TWD fue necesario pasar del espacio RGB al YCbCr antes de realizar el cambio de dominio, debido a que las pruebas mostraron que se recuperaba mejor la marca de agua en este espacio de color.

1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8
2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8
3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8
4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8
5.1	5.2	5.3	5.4	5.5	5.6	5.7	5.8
6.1	6.2	6.3	6.4	6.5	6.6	6.7	6.8
7.1	7.2	7.3	7.4	7.5	7.6	7.7	7.8
8.1	8.2	8.3	8.4	8.5	8.6	8.7	8.8

Figura 5.1 Frecuencias usadas para insertar la información

Para mostrar más claramente esta técnica de inserción, en las figuras 5.2a a la 5.2h se puede ver el proceso realizado paso a paso, con la transformación del dominio ilustrada en un bloque de 8x8 píxeles.

Primero se muestra la imagen original en la figura 5.2a, donde está marcado en azul un cuadro que contiene 8x8 píxeles en una zona muy variada en color, el cual se crece en la figura 5.2b lo suficiente como para distinguir perfectamente los límites y el color de cada píxel con el único propósito de poder ver los cambios del mismo después de haber insertado la información.

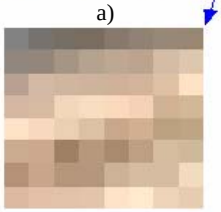
Siguiendo con el proceso, el paso siguiente es pasar la imagen a su equivalente de luminancia y crominancia, la figura 5.2c muestra únicamente los valores correspondientes a la matriz de luminancia del bloque seleccionado.

Después se va recorriendo la imagen por bloques de 8x8, para aplicar a cada bloque la TCD, quedando el bloque con el que se está ilustrando tal como se muestra en la figura 5.2d.

Ahora el paso que sigue es el de inserción de la información que se realiza como se explica en el capítulo 3, al ir comparando pares de valores que dependiendo si uno es mayor que el otro dará un uno ó un cero. En la figura 5.2e se puede ver cómo han cambiado los valores después de insertar la información.

Una vez que ya se ha insertado toda la información, se regresa nuevamente al dominio del espacio. En la figura 5.2f se ven los cambios sufridos en la matriz de luminancia y en la figura 5.2e se observa el cambio de tono de los píxeles al regresar al formato RGB y por último la figura 5.2e muestra la imagen con la información.

a)



b)

127	115	112	112	122	130	136	135
134	134	147	159	164	161	182	190
159	180	177	175	174	176	187	214
179	181	205	210	208	203	174	177
215	208	199	186	165	173	158	161
169	167	131	152	140	158	182	178
148	165	150	151	173	181	181	208
182	188	188	190	215	220	201	195

c)

1365	-44.4	14.14	-0.46	2.125	-10.3	0.501	-7.98
-96.2	-8.41	-2.42	-16	6.918	11.44	2.539	7.38
-77	-57.5	6.293	14.98	-0.4	-6.28	-4.36	9.871
-119	22.91	39.51	12.51	-0.38	12.97	-9.58	-7.08
27.88	58.18	-35.6	19.15	-5.13	4.201	17.03	3.565
-26.8	-19.1	-6.35	-1.35	1.568	-12.2	4.306	-0.01
-14.5	4.394	19.39	4.632	-4.57	4.073	-9.79	-5.82
-0.13	22.06	21.9	-11	-5.01	-11.8	4.418	-0.86

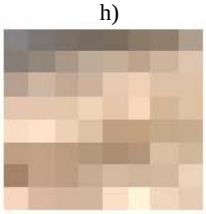
d)

1365	-44.4	14.14	-0.46	2.125	-10.3	0.501	-7.98
-96.2	-8.41	-2.42	-16	6.918	-0.4	2.539	-4.36
-77	-57.5	6.293	14.98	11.44	-6.28	7.38	9.871
-119	22.91	39.51	-35.6	-0.38	12.97	-9.58	3.565
27.88	58.18	12.51	19.15	-0.38	4.201	17.03	-7.08
-26.8	-19.1	-6.35	-1.35	1.568	-12.2	4.306	-9.79
-14.5	4.394	19.39	21.9	-11	4.073	-0.01	4.418
-0.13	22.06	4.632	-4.57	-5.01	-11.8	-5.82	-0.86

e)

129	119	115	111	111	123	128	154
126	134	149	166	170	161	175	189
158	177	166	174	194	200	187	187
191	192	191	202	191	207	177	186
211	216	200	187	159	159	166	167
158	160	155	150	143	149	184	177
135	161	156	168	180	176	179	201
206	180	177	177	212	228	204	196

f)



g)

h)

Figura 5.2 Proceso de la TCD, a) Imagen original, b) Cuadro de 8x8 píxeles, c) Matriz de luminancia, d) Aplicando la TCD, e) Insertando la información, f) regresando a la matriz de luminancia, g) Cuadro de 8x8 píxeles con información, h) Imagen con información

5.1.2. *INSERCIÓN APLICANDO LA TWD*

La transformada wavelet discreta se aplica directamente a cada plano de la imagen. Si recordamos, la TWD, al ser aplicada a una matriz o un plano de MxN, dará como resultado cuatro sub-matrices de M/2 x N/2. Cada una de las cuatro sub-matrices contendrá un tipo distinto de frecuencias, a saber: las bajas, las medias bajas, las medias altas y las altas.

Siguiendo el mismo criterio, se aplicará la TWD a cada plano de la imagen, y se conservarán intactas las frecuencias bajas, insertando la información en las restantes. El proceso de inserción será el propuesto en el capítulo III.

Las figuras 5.3a a la 5.3d muestran el proceso de inserción de la información aplicando la TWD. Se utiliza la misma imagen que en el ejemplo de la TCD, aunque para poder observar gráficamente las frecuencias por separado se necesita que la matriz sea bidimensional y no tridimensional como lo es una imagen a color, por lo tanto se convirtió a su equivalente en niveles de gris para el ejemplo. Primero se muestra la imagen en blanco y negro en la figura 5.3a, después la figura 5.3b consta de cuatro imágenes que están formadas por la descomposición de frecuencias que se obtiene al aplicar la TWD, ya que tenemos separadas las frecuencia entonces insertamos la información en las frecuencias medias bajas, medias altas y altas, figura 5.3c, y por último se reconstruye la imagen que es la figura 5.3d.

Figura 5.3a Imagen original en blanco y negro

Figura 5.3b Descomposición en frecuencias aplicando la TWD

Figura 5.3c Descomposición en frecuencias por la TWD después de haber insertado la información

Figura 5.3d Reconstrucción de la imagen con información

COMPARACIÓN DE LA TCD Y LA TWD EN LA CAPACIDAD DE INSERCIÓN

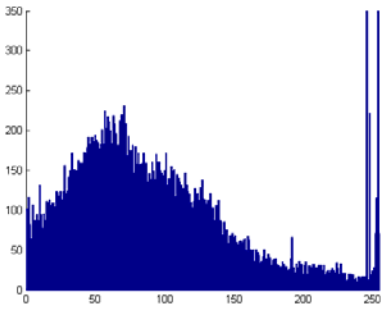
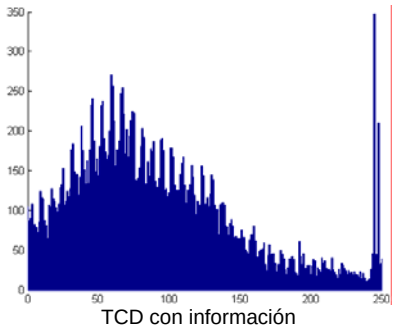
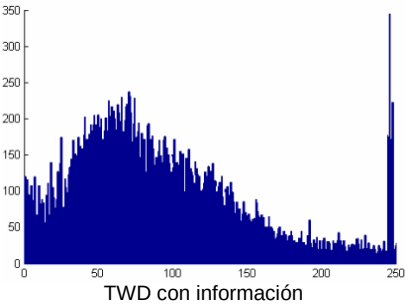
La comparación se va a realizar por medio de una tabla donde se indica la capacidad de inserción medida en relación con el tamaño de la imagen portadora, además de otros factores que se consideran importantes para medir cuánto modifica cada técnica a la imagen original.

Los siguientes son los significados de las siglas utilizadas en las tablas de este capítulo:

TI	Tamaño de la Imagen
MII	Máxima Información Insertada
EIO	Energía de la Imagen Original
EII	Energía de la Imagen con información
IC	Índice de Correlación
PI	Porcentaje de Inserción
PMAR	Porcentaje de Marca de Agua Recuperada

La tabla 5.1 tiene un ejemplo con las imágenes y sus histogramas para observar el cambio que sufren las imágenes después de insertar la información.

Tabla 5.1 Ejemplo con histogramas de la capacidad de inserción aplicando la TCD y la TWD

Imagen original e histograma	Imagen con información e histograma
  Imagen original	  TCD con información
	  TWD con información

Como se puede ver en los histogramas de la tabla anterior la TCD modifica más drásticamente a la imagen que la TWD. La tabla 5.2 tiene diez ejemplos diferentes para comparar la capacidad de inserción que tiene cada técnica, así como la energía que se pierde al insertar la información y el índice de correlación entre la imagen original y la imagen con información.

Tabla 5.2 Capacidad de inserción aplicando la TCD y la TWD

Imagen original	Técnica de inserción de M. A.	Capacidad de inserción %	% de Energía perdida	Índice de Correlación
Pez	TCD	TI = 77.3KB MII = 4.17KB PI = 5.39%	EIO = 921571582 EII = 913840231 % = 0.8389	IC = 0.994896
	TWD	TI = 77.3KB MII = 39.6KB PI = 51.22%	EIO= 921571582 EII= 920437230 % = 0.1230	IC = 0.998945
Lago	TCD	TI = 132KB MII = 7.3KB PI = 5.53%	EIO= 1856775512 EII= 1835943120 % = 1.1219	IC = 0.989753
	TWD	TI = 132KB MII = 67.3KB PI = 50.98%	EIO= 1856775512 EII= 1854943120 % = 0.0986	IC = 0.998934
Mujer	TCD	TI = 177KB MII = 9.21KB PI = 5.20%	EIO= 2606306287 EII= 2581971758 % = 0.9336	IC = 0.991257
	TWD	TI = 177KB MII = 90.3KB PI = 51.01%	EIO= 2606306287 EII= 2602571602 % = 0.1432	IC = 0.998963
Iglesia	TCD	TI = 115KB MII = 6.52KB PI = 5.66%	EIO= 1652016249 EII= 1638144942 % = 0.8396	IC = 0.993804
	TWD	TI = 115KB MII = 58.7KB PI = 51.04%	EIO= 1652016249 EII= 1650144942 % = 0.1132	IC = 0.999202
Histograma Imagen original	Técnica de inserción de M. A.	Capacidad de inserción %	% de Energía perdida	Índice de Correlación
Flor	TCD	TI = 141KB MII = 7.89KB PI = 5.59%	EIO= 2404392884 EII= 2384705822 % = 0.8187	IC = 0.995670
	TWD	TI = 141KB MII = 73KB PI = 51.77%	EIO= 2404392884 EII= 2400205482 % = 0.1741	IC = 0.998775
Circo	TCD	TI = 102KB MII = 5.78KB PI = 5.66%	EIO= 974714905 EII= 963950983 % = 1.1043	IC = 0.989926
	TWD	TI = 102KB MII = 52KB PI =50.98%	EIO= 974714905 EII= 973659869 % = 0.1082	IC = 0.999270

Casa	TCD	TI = 80KB MII = 4.4KB PI = 5.50%	EIO= 963159812 EII= 952120627 % = 1.1461	IC = 0.989559
	TWD	TI = 80KB MII = 39.8KB PI = 51.09%	EIO= 963159812 EII= 962230743 % = 0.0965	IC = 0.999019
Canoa	TCD	TI = 90.5KB MII = 4.99KB PI = 5.51%	EIO= 520532110 EII= 514597261 % = 1.1401	IC = 0.989686
	TWD	TI = 90.5KB MII = 46.1KB PI = 50.93%	EIO= 520532110 EII= 520086070 % = 0.0856	IC = 0.999404
Ciudad	TCD	TI = 165KB MII = 9.5KB PI = 5.75%	EIO= 3382985193 EII= 3418738374 % = 1.0568	IC = 0.990545
	TWD	TI = 165KB MII = 84.2KB PI = 51.03%	EIO= 3382985193 EII= 3379838374 % = 0.0930	IC = 0.999345

Histograma Imagen original	Técnica de inserción de M. A.	Capacidad de inserción %	% de Energía perdida	Índice de Correlación
Playa	TCD	TI = 225KB MII = 12.78KB PI = 5.68%	EIO= 4878953936 EII= 4828242081 % = 1.0394	IC = 0.990791
	TWD	TI = 225KB MII = 114.8KB PI = 51.02%	EIO= 4878953936 EII= 4871242081 % = 0.1580	IC = 0.999079

Después de analizar los resultados de la tabla 5.2, vemos que la capacidad de inserción aplicando la TCD es en promedio de 5.5%, mientras que la capacidad de inserción al aplicar la TWD es del 51%.

Por lo tanto, podemos decir que la técnica de la TWD supera por mucho a la TCD en capacidad de almacenamiento, y no sólo permite insertar más del 50% de información en la imagen, sino que también conserva la mayor cantidad de energía y es la que menos modifica a la imagen original, tal como lo muestran el índice de correlación y los histogramas.

5.2. COMPRESIÓN EN UNA IMAGEN

Comencemos con el ataque más discreto: la compresión. Es el más discreto porque es casi imposible notar visualmente los cambios en una fotografía después de haber realizado una compresión. Incluso, si recordamos el ejemplo del capítulo anterior, vemos que los histogramas de la imagen original y la comprimida son casi iguales. Pero esto no significa que no sea un ataque agresivo, sino todo lo contrario.

Se realizaron varias pruebas para identificar en qué parte de la imagen la marca de agua es resistente a una compresión. Se pudo comprobar que al distribuir la información uniformemente en las matrices de luminancia y crominancia se generan pérdidas. La información que se había insertado en las matrices de crominancia, se perdió casi por completo al pasar la imagen por un proceso de compresión.

Ahora, también hubo pérdidas en la parte que se introdujo en la matriz de luminancia, pero si analizamos la forma en que trabajan los formatos de compresión, será más fácil saber en qué parte la marca de agua será más resistente.

El principio básico de la compresión es conservar la mayor parte de la energía, y sabemos que ésta se encuentra en las frecuencias bajas. Por lo tanto, para empezar, debemos descartar las frecuencias altas porque seguramente serán eliminadas en el proceso de compresión. Luego, por las pruebas realizadas, tenemos que el mayor porcentaje de energía se encuentra en la matriz de luminancia. Entonces, insertar parte de la marca de agua en las matrices de crominancia también será inseguro.

Pero, dentro de las frecuencias bajas, únicamente podemos utilizar las medias bajas, respetando siempre las más bajas para no alterar la imagen de forma visible.

5.2.1. *COMPRESIÓN AL APLICAR LA TCD*

Después de introducir la marca de agua (MA) únicamente en la matriz de luminancia y en las frecuencias medias bajas, comprobamos que aún después de realizar una compresión a la imagen, la información puede recuperarse íntegramente con el método de TCD.

La tablas 5.3 y 5.4 muestran los resultados de las pruebas al comparar el histograma de la imagen original y el histograma de la imagen con la marca de agua después de una compresión, la cantidad de información insertada, el porcentaje de información recuperada después de la compresión, y la correlación entre la imagen con la marca de agua y la misma después de una compresión.

5.2.2. *COMPRESIÓN AL APLICAR LA TWD*

Bajo el criterio anterior, al utilizar la transformada wavelet, se insertó la marca de agua únicamente en las frecuencias medias-bajas, es decir en la subseñal *h*, sólo en la matriz de luminancia.

En la tabla 5.4 vemos resultados satisfactorios al recuperar por completo la información oculta después de una compresión en las imágenes portadoras. También se indica el tamaño que puede tener la marca de agua y el índice de correlación de la imagen con la marca de agua con respecto de la misma después de una compresión.

COMPARACIÓN DE LA TCD Y LA TWD AL RECUPERAR LA MARCA DE AGUA DESPUÉS DE UNA COMPRESIÓN

Si se incrusta la marca de agua en la zona de las frecuencias medias bajas para ambas técnicas, se puede asegurar que la información no será alterada si la imagen portadora sufre una compresión.

La tabla 5.3 muestra las imágenes y sus histogramas de la imagen original y de la misma después de incrustarle la marca de agua y pasarla por un proceso de compresión. Y la tabla 5.4 indica el porcentaje de inserción de marca agua de cada técnica, el índice de correlación entre la imagen original y la comprimida y el porcentaje de marca de agua recuperada.

Tabla 5.3 Comparación de los histogramas de una imagen después de una compresión

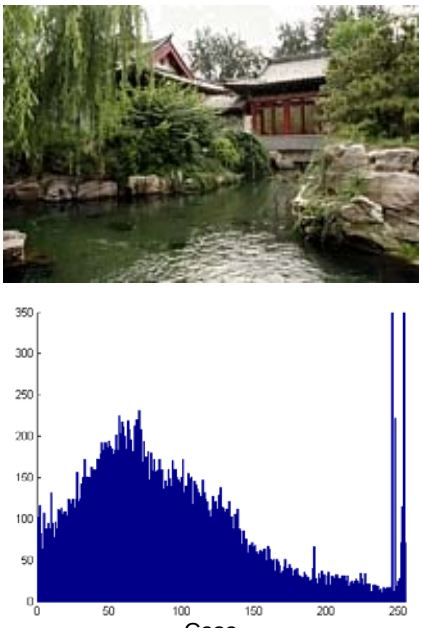
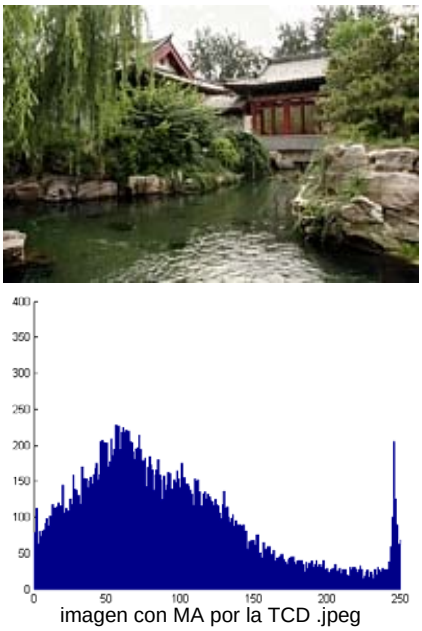
Imagen original e histograma	Imagen con información e histograma después de una compresión
	

	  imagen con MA por la TWD .jpeg

Tabla 5.4 Comparación de la TCD y la TWD al recuperar la marca de agua después de una compresión

Imagen original	Técnica de inserción de M. A.	% de inserción	Índice de Correlación	% MA recuperada
Pez	TCD	TI = 77.3KB MII = 0.45KB PI = 0.57%	IC = 0.999006	PMAR = 100%
	TWD	TI = 77.3KB MII = 3.32KB PI = 4.29%	IC = 0.999188	PMAR = 100%
Lago	TCD	TI = 132KB MII = 0.72KB PI = 0.54%	IC = 0.998516	PMAR = 100%
	TWD	TI = 132KB MII = 5.63KB PI = 4.26%	IC = 0.998156	PMAR = 100%
Mujer	TCD	TI = 177KB MII = 1KB PI = 0.56%	IC = 0.998877	PMAR = 100%
	TWD	TI = 177KB MII = 7.55KB PI = 4.26%	IC = 0.998890	PMAR = 100%
Iglesia	TCD	TI = 115KB MII = 0.64KB PI = 0.53%	IC = 0.999183	PMAR = 100%
	TWD	TI = 115KB MII = 4.91KB PI = 4.27%	IC = 0.999186	PMAR = 100%
Flor	TCD	TI = 141KB MII = 0.77KB PI = 0.54%	IC = 0.999538	PMAR = 100%
	TWD	TI = 141KB MII = 6.05KB PI = 4.28%	IC = 0.999539	PMAR = 100%
Imagen original	**Técnica de inserción de M. A.**	**% de inserción**	**Índice de Correlación**	**% MA recuperada**
Circo	TCD	TI = 102KB MII = 0.56KB PI =0.55%	IC = 0.998621	PMAR = 100%
	TWD	TI = 102KB MII = 4.36KB PI =4.27 %	IC = 0.998632	PMAR = 100%
Casa	TCD	TI = 80KB MII = 0.43KB PI = 0.53%	IC = 0.997835	PMAR = 100%
	TWD	TI = 80KB MII = 3.6KB PI = 4.3%	IC = 0.997869	PMAR = 100%

Canoa	TCD	TI = 90.5KB MII = 0.48KB PI = 0.53%	IC = 0.996936	PMAR = 100%
	TWD	TI = 90.5KB MII = 3.82KB PI = 4.22%	IC = 0.998042	PMAR = 100%
Ciudad	TCD	TI = 165KB MII = .9KB PI = 0.55%	IC = 0.998934	PMAR = 100%
	TWD	TI = 165KB MII = 7.05KB PI = 4.27%	IC = 0.998992	PMAR = 100%
Playa	TCD	TI = 225KB MII = 1.23KB PI = 0.55%	IC = 0.999146	PMAR = 100%
	TWD	TI = 225KB MII = 9.6KB PI = 4.26%	IC = 0.999156	PMAR = 100%

Ahora, si revisamos los resultados mostrados en la tabla 5.4, veremos que la capacidad de inserción se reduce drásticamente para ambas técnicas, situación que es necesaria si queremos marcas de agua robustas que sobrevivan a este ataque.

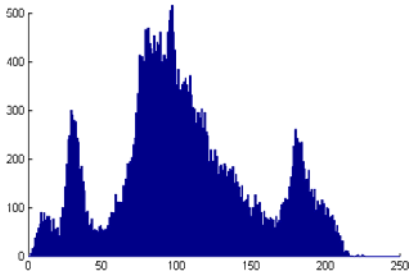
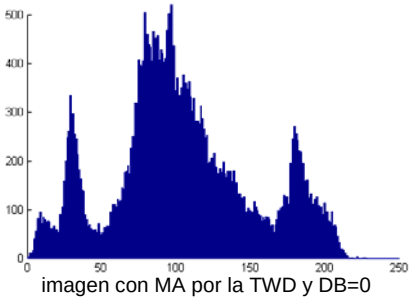
Entonces, la capacidad de almacenamiento cambia, de manera que la TCD permite insertar marcas de agua robustas del 0.55% con respecto al tamaño de la imagen portadora, mientras que en la TWD es de 4.27%. Este resultado coloca la técnica de la TWD por encima de la de TCD.

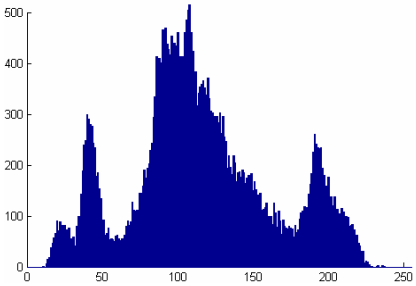
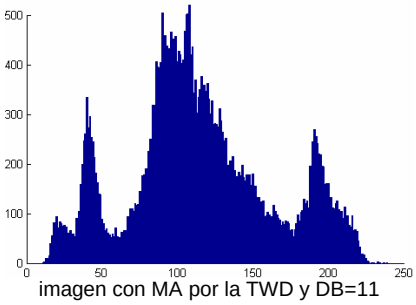
5.3. DISTORSIÓN DE BRILLO EN LA IMAGEN

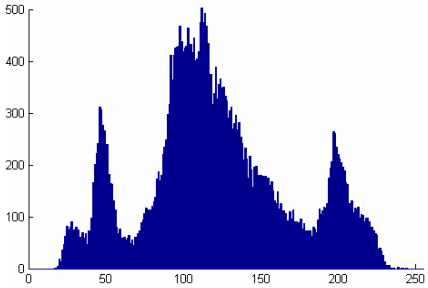
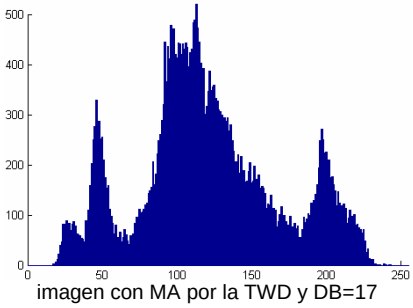
Ya se sabe que la distorsión de brillo aclara la fotografía si se le suma la misma cantidad a toda la imagen o la oscurece si se le resta. Siempre y cuando ese número no sea muy grande, los cambios no serán notorios visualmente. Pero a pesar de su sencillez, éste esta considerado dentro de los ataques más efectivos para eliminar marcas de agua.

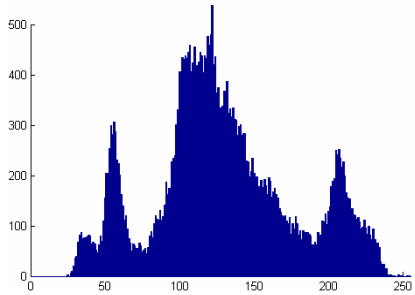
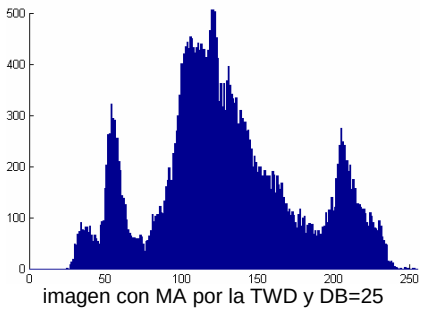
La tabla 5.5 muestra ejemplos de pruebas realizadas a una fotografía con tres diferentes niveles de distorsión de brillo (DB), sus respectivos histogramas, el índice de correlación de la imagen con la marca de agua con respecto a ésta después de ser alterada por distorsión de brillo, y finalmente el porcentaje de la marca de agua (MA) recuperada. Los ejemplos en general están realizados con marcas de agua diferentes.

Tabla 5.5 Imagen “iglesia” con diferentes distorsiones de brillo al utilizar la TCD y la TWD

Distorsión de Brillo	Imagen con M. A. E histograma	Índice de Correlación	% MA recuperada
0	  imagen con MA por la TCD y DB=0	IC =1.000	PMAR = 100%
	  imagen con MA por la TWD y DB=0	IC =1.000	PMAR = 100%

+11	  imagen con MA por la TCD y DB=11	IC = 0.999318	PMAR = 100%
	  imagen con MA por la TWD y DB=11	IC = 0.999325	PMAR = 100%

+17	  imagen con MA por la TCD y DB=17	IC = 0.998507	PMAR = 100%
	  imagen con MA por la TWD y DB=17	IC = 0.998523	PMAR = 100%

+ 25	  imagen con MA por la TCD y DB=25	IC = 0.997112	PMAR = 100%
	  imagen con MA por la TWD y DB=25	IC = 0.997139	PMAR = 100%

Después de analizar los ejemplos anteriores vemos que la distorsión de brillo nunca eliminará la marca de agua y esto se debe a la forma en la que estamos insertándola. Ya sabemos que para ambas técnicas se comparan dos elementos y dependiendo de que si uno es mayor o menor significa un “uno” o un “cero”. Entonces,

sumar una cantidad -cualquiera que esta sea- a todos los elementos de la imagen no alterará la relación entre los elementos.

Pero ¿qué pasa cuando tenemos elementos muy cercanos o iguales a 255, como en el caso de la imagen de "circo"? Nunca podremos tener valores mayores a ése. Por ejemplo, si sumamos el valor de 10 al siguiente vector [251 245 249 253 250 248] tendríamos como resultado lo siguiente [255 255 255 255 255 255]. Entonces, considerando esta posibilidad, lo que se propuso fue que la condición sea "mayor o igual", es decir que $(u1,v1) \geq (u2,v2)$.

Comentario [MSOffice1]: En plural o singular?

5.4. AÑADIENDO RUIDO A LA IMAGEN

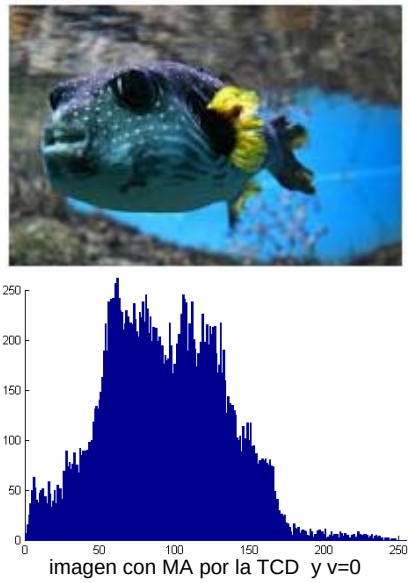
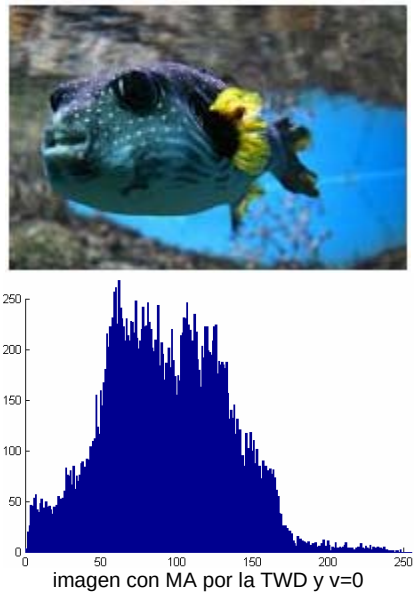
Como vimos en el capítulo anterior, el ruido también es una forma muy efectiva para modificar o eliminar una marca de agua, siempre y cuando sea con la "dosis apropiada", es decir, no se puede abusar porque entonces se modifica la imagen de forma visible y será obvio que fue alterada.

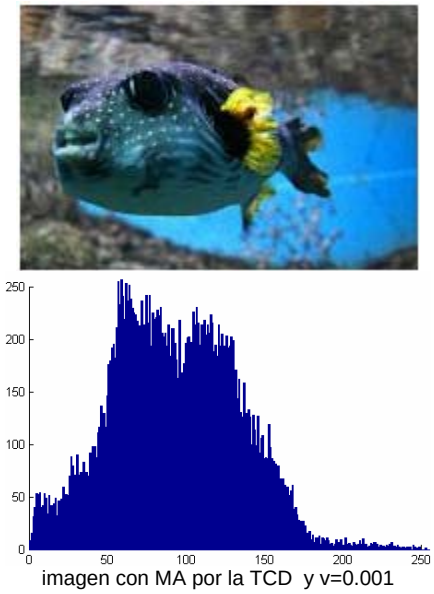
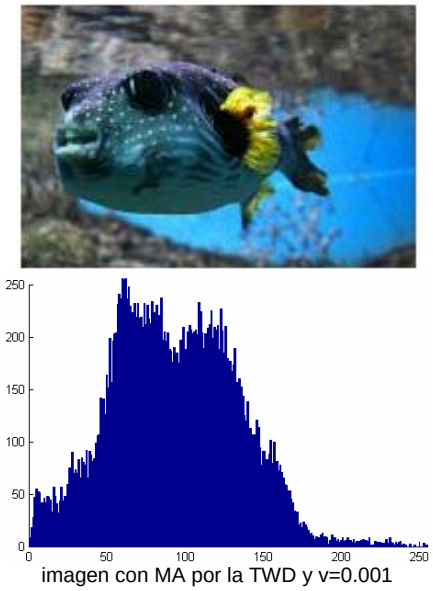
5.4.1. *RUIDO MULTIPLICATIVO EN LA IMAGEN*

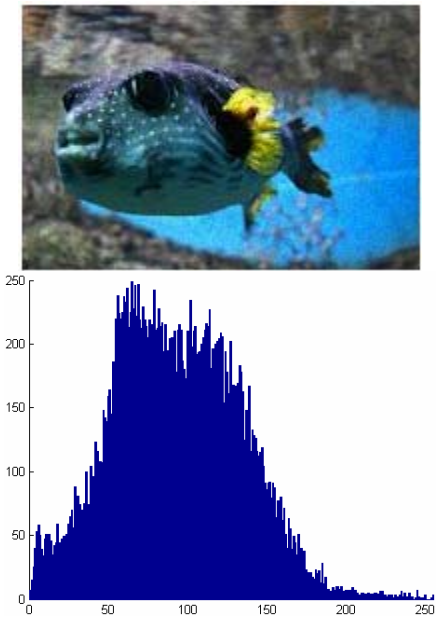
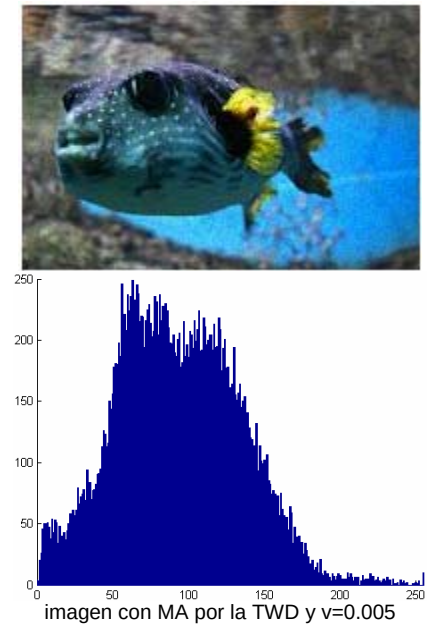
En el capítulo IV tenemos un par de ejemplos que muestran el efecto causado a la imagen cuando se le suma ruido multiplicativo. El cambio fue visiblemente obvio cuando se añadió a la imagen ruido multiplicativo con una varianza 0.05, por lo que las varianzas (v) que se usan para los siguientes ejemplos serán menores.

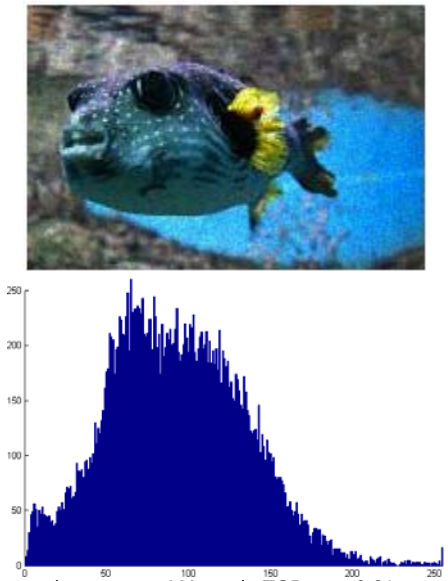
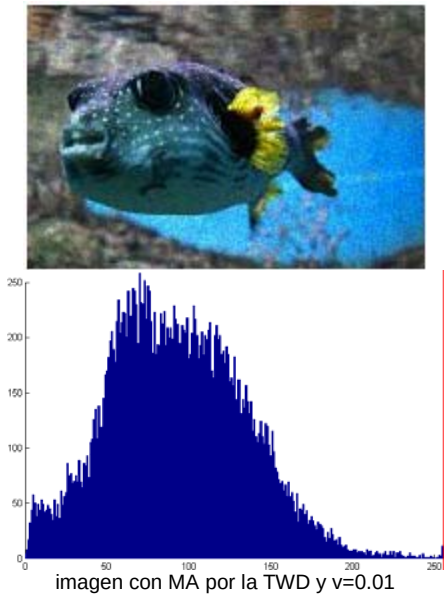
En la tabla 5.6 se muestran tres ejemplo realizados a una imagen con diferentes varianzas de ruido multiplicativo, se muestran las imágenes con sus respectivos histogramas, el índice de correlación entre la imagen con marca de agua y la misma después de alterarla con ruido multiplicativo y el porcentaje de marca de agua recuperada.

Tabla 5.6 Imagen “pez”, con diferentes varianzas de ruido multiplicativo utilizando la TCD y la TWD

Ruido Multiplicativo	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
varianza = 0	 imagen con MA por la TCD y v=0	IC = 1.000	PMAR = 100%
Ruido Multiplicativo	**Imagen con M.A. e histogramas**	**Índice de Correlación**	**% de MA recuperada**
	 imagen con MA por la TWD y v=0	IC = 1.000	PMAR = 100%

varianza = 0.001	 imagen con MA por la TCD y v=0.001	IC = 0.999491	PMAR = 100%
Ruido Multiplicativo	**Imagen con M.A. e histogramas**	**Índice de Correlación**	**% de MA recuperada**
	 imagen con MA por la TWD y v=0.001	IC =0.999500	PMAR = 100%

varianza = 0.005	 imagen con MA por la TCD y v=0.005	IC = 0.997511	PMAR = 96%
Ruido Multiplicativo	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
	 imagen con MA por la TWD y v=0.005	IC = 0.997579	PMAR = 98%

varianza = 0.01	 imagen con MA por la TCD y v=0.01	IC = 0.995044	PMAR = 83%
Ruido Multiplicativo	**Imagen con M.A. e histogramas**	**Índice de Correlación**	**% de MA recuperada**
	 imagen con MA por la TWD y v=0.01	IC = 0.995117	PMAR = 86%

Las tablas 5.7 y 5.8 son dos ejemplos más de imágenes con marcas de agua a las que se les sumó ruido multiplicativo con diferentes varianzas, en las que se muestra el

índice de correlación y el porcentaje de marca de agua recuperada después de haber alterado la imagen con el ruido.

Tabla 5.7 Imagen "circo", con diferentes varianzas de ruido multiplicativo utilizando la TCD y la TWD

Ruido Multiplicativo	Técnica de inserción de M. A.	Índice de Correlación	% de MA recuperada
varianza = 0	TCD	IC =1.000	PMAR = 100%
	TWD	IC =1.000	PMAR = 100%
varianza = 0.002	TCD	IC = 0.998999	PMAR = 99%
	TWD	IC = 0.999021	PMAR = 100%
varianza = 0.008	TCD	IC = 0.996136	PMAR = 86%
	TWD	IC = 0.996142	PMAR = 87%
varianza = 0.015	TCD	IC = 0.992780	PMAR = 71%
	TWD	IC = 0.992881	PMAR = 75%

Tabla 5.8 Imagen "iglesia", con diferentes varianzas de ruido multiplicativo utilizando la TCD y la TWD

Ruido Multiplicativo	Técnica de inserción de M. A.	Índice de Correlación	% de MA recuperada
varianza = 0	TCD	IC =1.000	PMAR = 100%
	TWD	IC =1.000	PMAR = 100%
varianza = 0.0015	TCD	IC = 0.999245	PMAR = 100%
	TWD	IC = 0.999288	PMAR = 100%
varianza = 0.007	TCD	IC = 0.996522	PMAR = 91%
	TWD	IC = 0.996856	PMAR = 97%
varianza = 0.012	TCD	IC = 0.994050	PMAR = 77%
	TWD	IC = 0.994985	PMAR = 82%

Por los resultados que arrojan las tablas anteriores y otros ejemplos realizados, se señala que la TCD es más susceptible a este ataque que la TWD. Por otro lado, el ataque será efectivo siempre y cuando tenga una varianza menor a 0.005 aproximadamente, porque con varianzas mayores modifica de forma visible a la imagen como lo muestra la tabla 5.6.

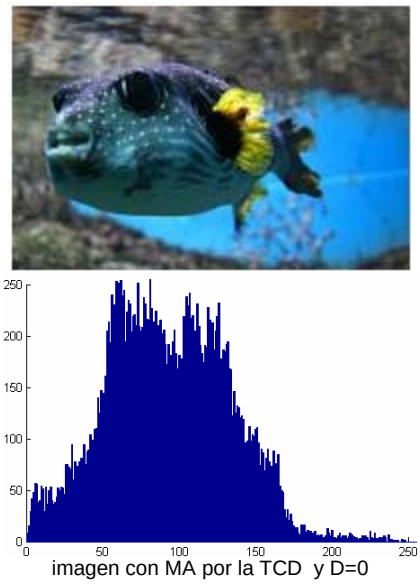
Finalmente, si se agrega ruido multiplicativo a la imagen con una varianza menor a 0.005, lo más probable es que los cambios no resalten y que el máximo porcentaje de pérdida de la marca de agua sea del 2% para la TWD y del 4% para el TCD.

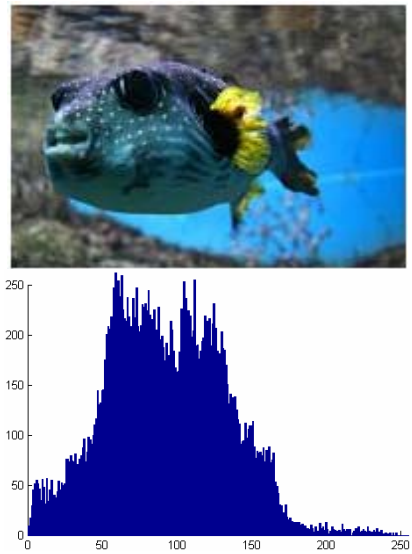
5.4.2. *RUIDO IMPULSIVO EN LA IMAGEN*

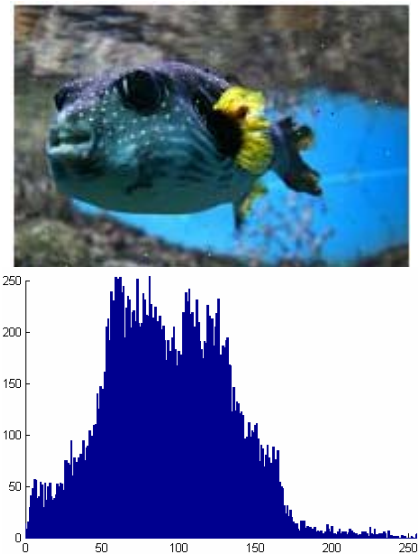
Como el ruido impulsivo suma valores aleatorios a píxeles que también elige de manera aleatoria, los cambios en la imagen son muy sobresalientes. En el capítulo anterior vimos que el porcentaje de píxeles afectados va a depender de la densidad del ruido (D). En las tablas 5.9 a la 5.11 se muestran las pruebas realizadas a imágenes afectadas con este ruido.

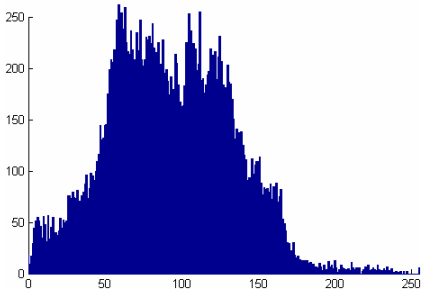
Primero en tabla 5.9 ilustra imágenes con marcas de agua que se alteraron con ruido impulsivo y sus histogramas, también el índice de correlación y el porcentaje de marca de agua recuperado.

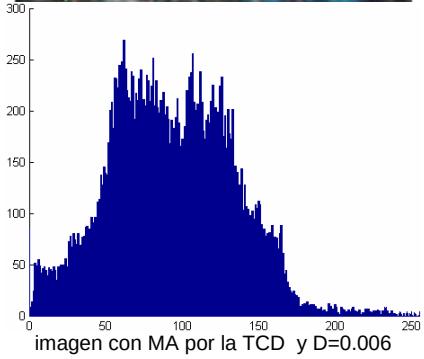
Tabla 5.9 Imagen “pez”, con diferentes densidades de ruido impulsivo utilizando la TCD y la TWD

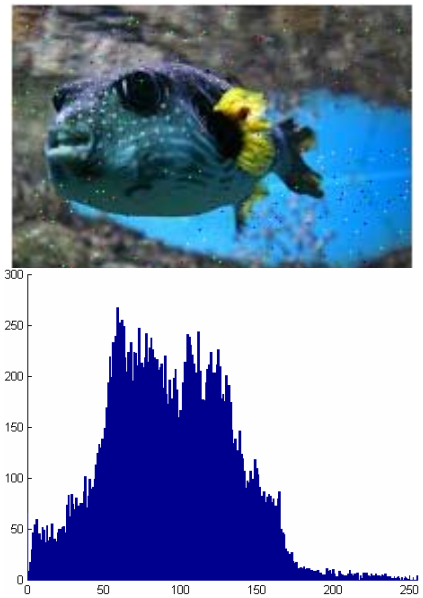
Ruido Impulsivo	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
Densidad = 0	 imagen con MA por la TCD y D=0	IC =1.000	PMAR = 100%

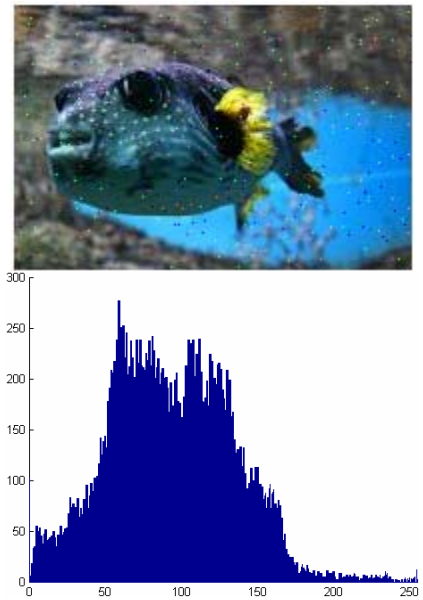
	 imagen con MA por la TWD y D=0	IC =1.000	PMAR = 100%

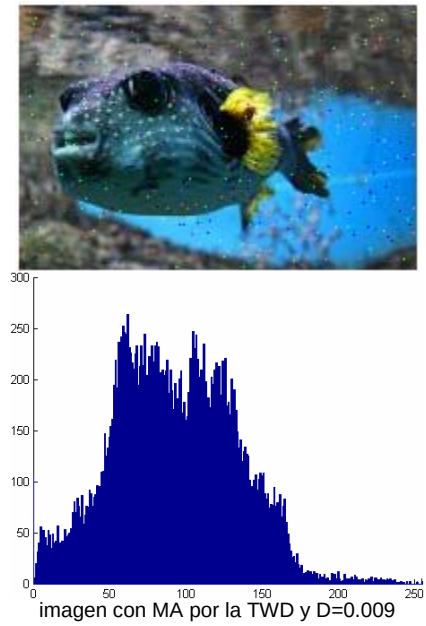
Ruido Impulsivo	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
Densidad = 0.001	 imagen con MA por la TCD y D=0.001	IC = 0.999138	PMAR = 85%

	  imagen con MA por la TWD y D=0.001	IC = 0.999237	PMAR = 88%

Ruido Impulsivo	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
Densidad = 0.006	  imagen con MA por la TCD y D=0.006	IC=0.993928	PMAR = 76%

	 imagen con MA por la TWD y D=0.006	IC = 0.993868	PMAR = 79%

Ruido Impulsivo	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
Densidad = 0.009	 imagen con MA por la TCD y D=0.009	IC = 0.991574	PMAR = 69%

	 imagen con MA por la TWD y D=0.009	IC = 0.992589	PMAR = 73%

Las siguientes dos tablas únicamente registran el índice de correlación y el porcentaje de marca de agua recuperado, para así poder comparar los resultados de ambas técnicas.

Tabla 5.10 Imagen “circo”, con diferentes densidades de ruido impulsivo utilizando la TCD y la TWD

Ruido Impulsivo	Técnica de inserción de M. A.	Índice de Correlación	% de MA recuperada
Densidad = 0	TCD	IC =1.000	PMAR = 100%
	TWD	IC =1.000	PMAR = 100%
Densidad = 0.0015	TCD	IC = 0.998451	PMAR = 83%
	TWD	IC=0.998686	PMAR = 85%
Densidad = 0.005	TCD	IC=0.994332	PMAR = 79%
	TWD	IC=0.994595	PMAR = 81%
Densidad = 0.01	TCD	IC = 0.987648	PMAR = 64%
	TWD	IC = 0.988559	PMAR = 69%

Tabla 5.11 Imagen “iglesia”, con diferentes densidades de ruido impulsivo utilizando la TCD y la TWD

Ruido Impulsivo	Técnica de inserción de M. A.	Índice de Correlación	% de MA recuperada
Densidad = 0	TCD	IC =1.000	PMAR = 100%
	TWD	IC =1.000	PMAR = 100%
Densidad = 0.003	TCD	IC = 0.997409	PMAR = 81%
	TWD	IC = 0.997658	PMAR = 84%
Densidad = 0.008	TCD	IC = 0.994430	PMAR = 70%
	TWD	IC = 0.994492	PMAR = 73%
Densidad = 0.012	TCD	IC = 0.991372	PMAR = 65%
	TWD	IC = 0.991552	PMAR = 68%

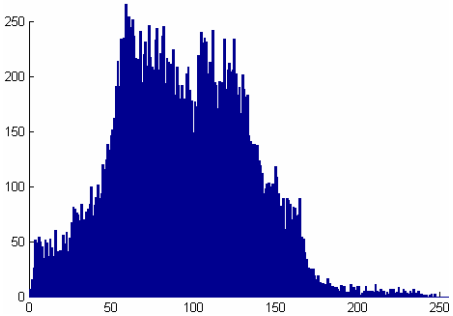
Si se observan los resultados de las tablas de la 5.9 a la 5.11 resalta el hecho de que la marca de agua definitivamente no resiste a este ataque por muy pequeña que sea la densidad del ruido, pero también sobresale el hecho de que el ruido impulsivo siempre es visible en las imágenes, lo que lo convierte en un ataque poco efectivo. Por otro lado el porcentaje de la marca de agua recuperado es mayor cuando se utiliza la técnica de la TWD.

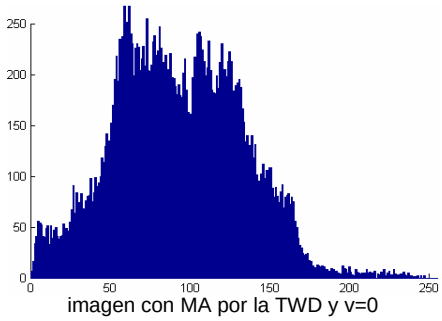
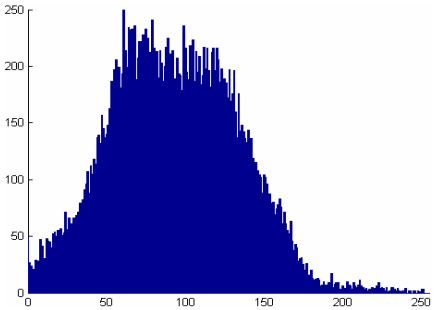
5.4.3. *RUIDO GAUSSIANO EN LA IMAGEN*

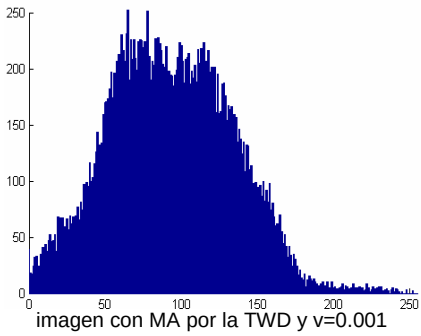
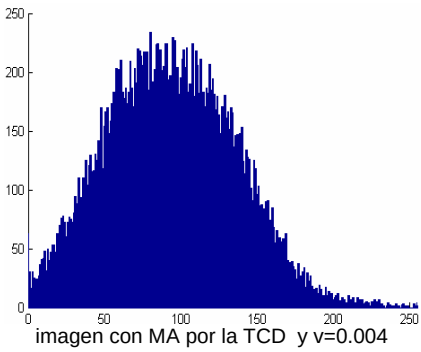
Al igual que el ruido multiplicativo, el ruido gaussiano modifica a todo la imagen pero éste lo hace con una distribución de probabilidad gaussiana. Para los ejemplos de las siguientes tres tablas la media va a ser cero y se irá modificando la varianza (v).

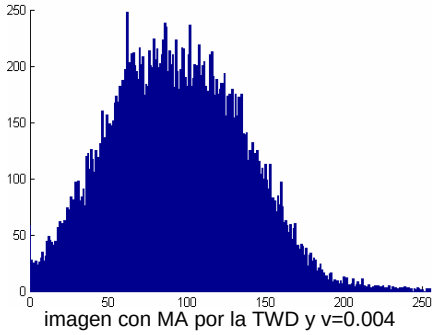
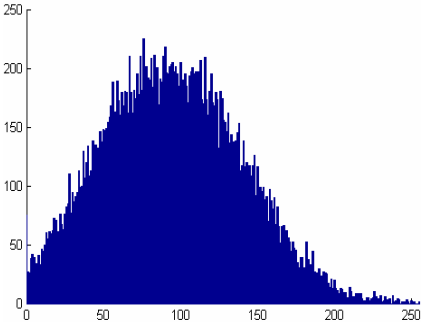
La tabla 5.12 va a mostrar una imagen a la que se le hicieron tres pruebas con diferentes varianzas de ruido multiplicativo. Serán pruebas visuales de las imágenes y sus histogramas.

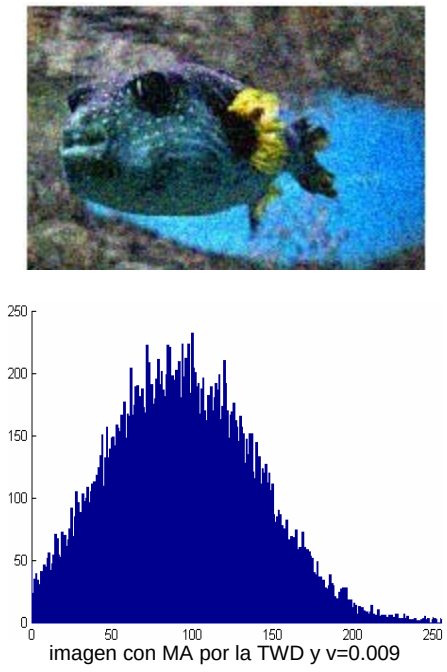
Tabla 5.12 Imagen “pez”, con diferentes densidades de ruido gaussiano utilizando la TCD y la TWD

Ruido Gaussiano	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
varianza = 0	  imagen con MA por la TCD y v=0	IC =1.000	PMAR = 100%

Ruido Gaussiano	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
	  imagen con MA por la TWD y v=0	IC =1.000	PMAR = 100%
varianza = 0.001	  imagen con MA por la TCD y v =0.001	IC = 0.996874	PMAR = 83%

Ruido Gaussiano	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
	  imagen con MA por la TWD y v=0.001	IC = 0.996935	PMAR = 84%
varianza = 0.004	  imagen con MA por la TCD y v=0.004	IC = 0.987764	PMAR = 80%

Ruido Gaussiano	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
	  imagen con MA por la TWD y v=0.004	IC = 0.987481	PMAR = 80%
varianza = 0.009	  imagen con MA por la TCD y v=0.009	IC = 0.973482	PMAR = 66%

Ruido Gaussiano	Imagen con M.A. e histogramas	Índice de Correlación	% de MA recuperada
	 imagen con MA por la TWD y v=0.009	IC = 0.973715	PMAR = 68%

Las tablas 5.13 y 5.14 también son ejemplos de imágenes con marcas de agua afectadas con ruido gaussiano donde se muestra el índice de correlación entre la imagen con marca de agua y la misma afectada con el ruido, y el porcentaje que se recuperó de la marca de agua después de haberle añadido el ruido gaussiano.

Tabla 5.13 Imagen “circo”, con diferentes densidades de ruido gaussiano utilizando la TCD y la TWD

Ruido Gaussiano	Técnica de inserción de M. A.	Índice de Correlación	% de MA recuperada
Varianza = 0	TCD	IC =1.000	PMAR = 100%
	TWD	IC =1.000	PMAR = 100%
Varianza = 0.003	TCD	IC = 0.988971	PMAR = 81%
	TWD	IC = 0.989188	PMAR = 82%
Varianza = 0.005	TCD	IC = 0.982278	PMAR = 78%
	TWD	IC = 0.982309	PMAR = 79%
Varianza = 0.01	TCD	IC = 0.966320	PMAR = 64%
	TWD	IC = 0.966575	PMAR = 66%

Tabla 5.14 Imagen “iglesia”, con diferentes densidades de ruido gaussiano utilizando la TCD y la TWD

Ruido Gaussiano	Técnica de inserción de M. A.	Índice de Correlación	% de MA recuperada
Varianza = 0	TCD	IC =1.000	100%
	TWD	IC =1.000	100%
Varianza = 0.002	TCD	IC = 0.995169	81%
	TWD	IC = 0.995098	82%
Varianza = 0.006	TCD	IC = 0.994492	75%
	TWD	IC = 0.994430	77%
Varianza = 0.012	TCD	IC = 0.972644	63%
	TWD	IC = 0.972407	66%

Según los resultados de las tablas 5.12 a la 5.14, al igual que en el caso del ruido impulsivo, al agregarle ruido gaussiano a la imagen la marca de agua es modificada, por mínima que sea la varianza del ruido. Pero también es un ruido cuya presencia se nota fácilmente, lo que significa que no será un ataque tan efectivo. Por otro lado, los histogramas reflejan drásticamente la evidencia de un cambio.

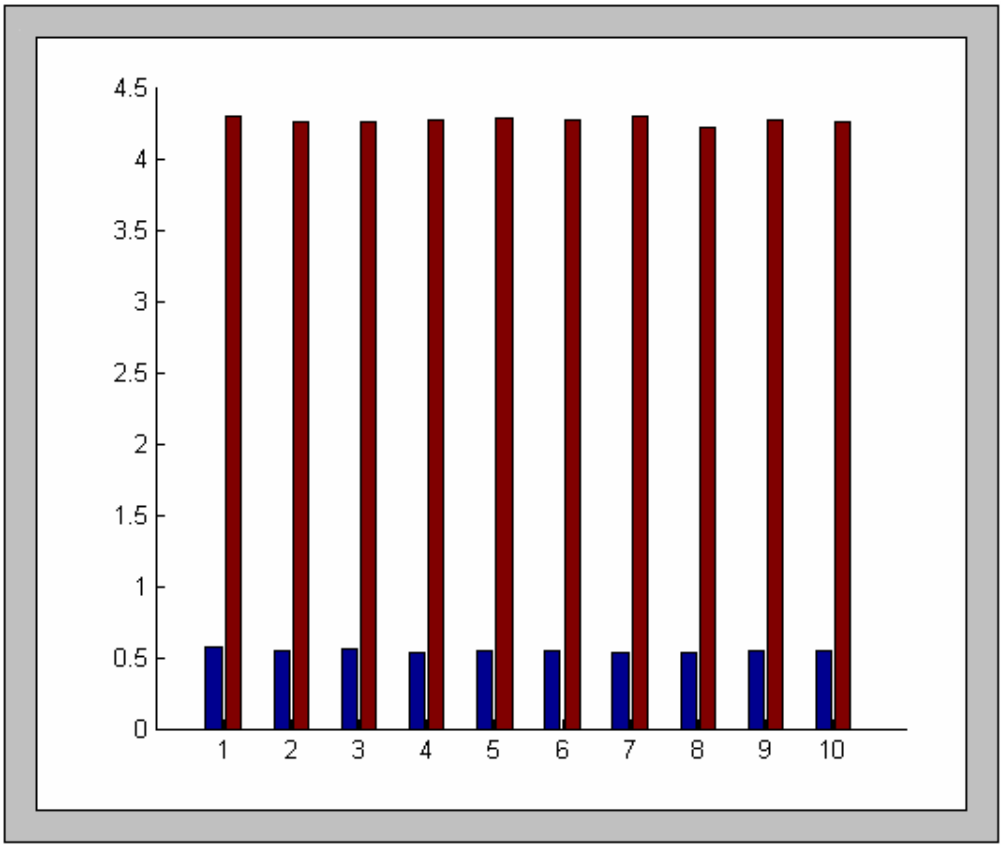
5.5. COMPARACIÓN GENERAL

Ya se determinó el área más conveniente para implantar la marca de agua y hacerla resistente a ciertos ataques, así como el porcentaje de inserción que permite cada técnica para incrustar marcas de agua robustas. Por otro lado, también se identificó qué tanto modifica la marca de agua robusta a la imagen original tanto para la TCD como para la TWD; comparando no solamente los histogramas, sino también el índice de correlación y el porcentaje de energía perdida.

Por último, se resumirán todas estas características de comparación entre ambas técnicas por medio de tres gráficas de barras correspondientes a las tablas 5.15 a la 5.17, donde en color azul se representa la TCD y en color rojo la TWD.

En la tabla 5.15 se compara la capacidad de incrustación de ambas técnicas. Los valores del eje horizontal corresponden a diez imágenes a las que se les incrustó la marca de agua, y el eje vertical incida el porcentaje de inserción que se logró en cada imagen de acuerdo al tamaño de la misma.

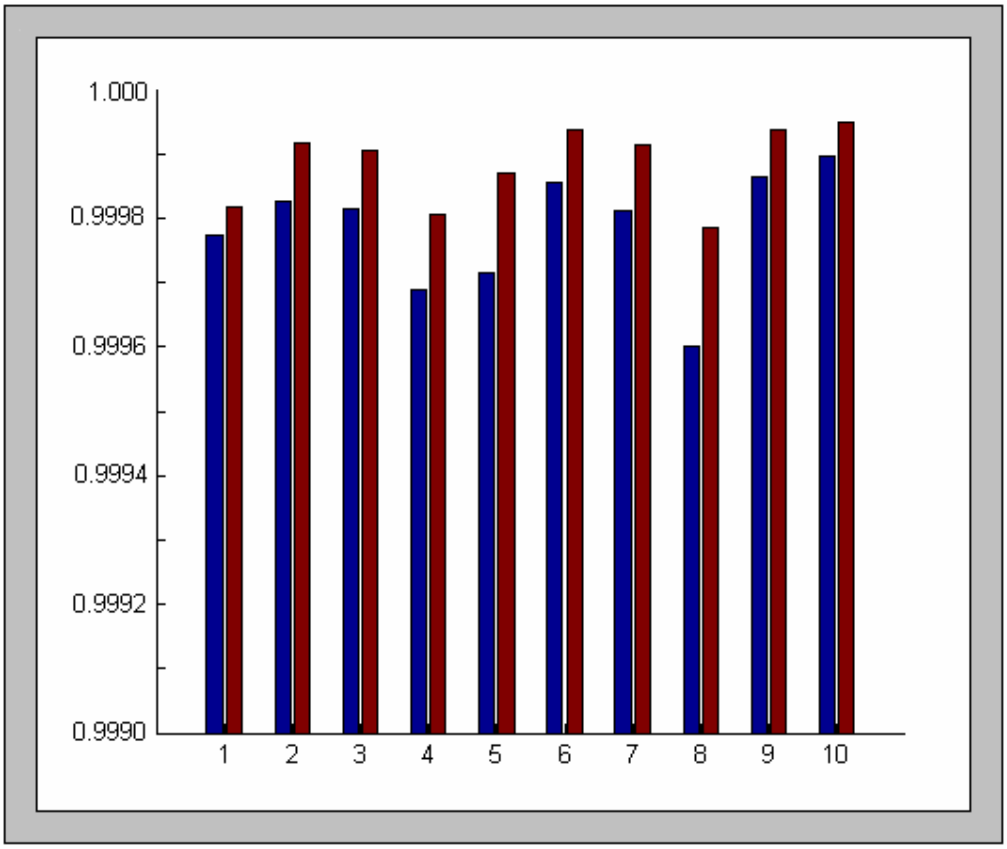
Tabla 5.15 Comparación de la TCD y la TWD en la capacidad de incrustación de marcas de agua robustas



Después de ver la tabla anterior queda muy claro el hecho de que la TWD para aplicaciones de marcas de agua robustas en imágenes es superior en cuanto a capacidad de inserción que la técnica existente de la TCD.

La siguiente tabla 5.16 es una gráfica de barras donde se van a comparar los mismos diez ejemplos de la tabla anterior pero ahora lo que se va a medir es el índice de correlación entre la imagen original y la misma después de la inserción de la marca de agua. En el eje vertical se encuentran los valores correspondientes al índice de correlación.

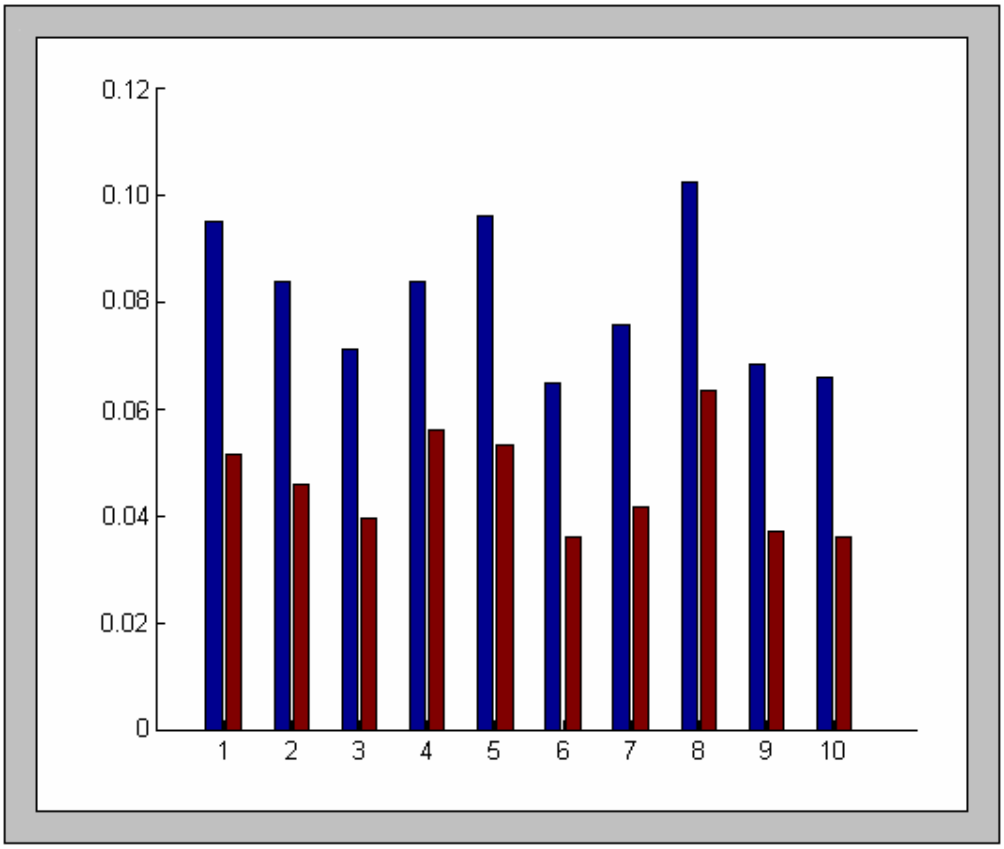
Tabla 5.16 Comparación de la TCD y la TWD en el índice de correlación entre la imagen y ésta después de la inserción de la marca de agua robusta



En la tabla 5.16 que mide el índice de correlación y que índica qué tanto ha cambiado la imagen con la marca de agua con respecto a la original, se muestra que en todos lo ejemplos siempre fue mejor la TWD, porque modifica más sutilmente a la imagen a diferencia de la TCD.

Por último, se va a comparar en la tabla 5.17 la energía que pierde la imagen original después de ser alterada con la incrustación de la marcas de agua. Los elementos a lo largo de eje horizontal siguen siendo las imágenes de los ejemplos anteriores y el eje vertical indica el porcentaje de energía perdida.

Tabla 5.17 Comparación de la TCD y la TWD en la pérdida de energía entre la imagen y ésta después de la inserción de la marca de agua robusta



Finalmente concluimos que la TWD no sólo es superior a la TCD en capacidad de inserción sino que también es la que menos altera a la imagen portadora, dato que se indica con el índice de correlación y con la energía perdida tal como lo muestra la tabla 5.17, donde en todos los ejemplos la técnica de la TWD fue la que tuvo menos pérdidas de energía.

CONCLUSIONES

El objetivo de este trabajo fue proponer una técnica de inserción de marcas de agua robustas en imágenes digitales de formato BMP, utilizando la Transformada Wavelet Discreta, y comparar con la técnica ya existente de la Transformada del Coseno Discreto. El propósito se cumplió y se muestra con los resultados de todo el capítulo V, mismos que permiten declarar lo siguiente:

Queda demostrada la legibilidad, seguridad y robustez de la técnica de la Transformada Wavelet Discreta para inserción de marcas de agua digitales.

- Es legible porque la información insertada en la imagen se puede recuperar después del proceso inverso.

- Es segura porque ante cualquier persona no autorizada no es evidente la existencia de la marca de agua ya que visiblemente es imposible notar su existencia.

- Y lo más importante es que las marcas de agua son robustas porque se demostró que son completamente resistentes a la compresión realizada por técnicas comerciales.

Igualmente las marcas de agua resisten en su totalidad un ataque de distorsión de brillo, ataques que alteran de forma uniforme a la imagen y este tipo de modificaciones nunca afectarán la información insertada. Tampoco el ruido multiplicativo con una varianza no mayor a 0.002 afectará en absoluto la información incrustada. Por otro lado, el ruido impulsivo -al igual que el ruido gaussiano- afectan la marca de agua, pero debemos recordar que para que un ataque sea efectivo, no debe alterar de forma visible la imagen, condición que no cumplen este par de ataques, ya que de forma visual se muestra claramente que la imagen fue alterada.

En todas las pruebas anteriores la TCD y la TWD mostraron resultados muy similares pero se debe resaltar el hecho de que siempre fue mejor el comportamiento de la TWD. Por ejemplo, al insertar la marca de agua, la TWD modifica menos a la imagen y conserva más energía. Asimismo, en todos las pruebas realizadas con los tres tipos de ruido, con esta técnica la marca de agua siempre tuvo mayor porcentaje de recuperación.

Finalmente, si se compara la capacidad de almacenamiento de información oculta, es aquí donde la TWD supera por mucho a la TCD. Tenemos una capacidad de inserción para marcas de agua robustas del 4.27% con respecto al tamaño de la imagen, contra un 0.54% correspondiente a la técnica de inserción de la TCD.

TRABAJO FUTURO

Las marcas de agua digitales tienen una amplia gama de aplicación, por lo que se comentaba al principio de este trabajo sobre las necesidades actuales de protección. Pero para una continuación más allegada lo ideal es seguir con la aplicación a imágenes y así aprovechar lo mejor posible la investigación actual.

Se proponen caminos distintos, pero todos interesantes y con una aplicación actual.

Primero es continuar investigando sobre posibles formas de alterar o erradicar marcas de agua en imágenes para crear un método más robusto de marcado, porque puede ser que en un tiempo muy corto ya existan nuevos ataques que ya fueron considerados en este trabajo, pero ya no se tendría que empezar de cero sino simplemente adaptar lo que ya se tiene a las nuevas necesidades de seguridad.

Otra propuesta es escalar a marcas de agua en video, lo cual no se desviaría mucho porque el video es sólo una composición de cierto número de imágenes; todos sabemos la problemática actual con la piratería, por lo que una aportación muy acertada sería lograr un marcado en video con el único propósito de no permitir de alguna manera reproducciones posteriores del mismo.

Una aplicación interesantes tanto para imágenes como video, sería lograr el marcado en tiempo real, es decir cámaras fotográficas o de video que al momento de tomar una foto o una toma de video inserten al instante la marca de agua, esto sería muy útil para no permitir que el material sea editado posteriormente, lo cual les sería muy útil a editores de periódicos, revistas y televisoras. Pero algo muy interesante en esta aplicación es que se necesitan dos marcas de agua, una robusta como la que hemos propuesto que contenga los datos del propietario y la otra que puede ir por ejemplo en las frecuencias altas, para que sea sensible a cualquier cambio por mínimo que sea. Entonces no sólo se asegura la propiedad sino también que sus mismos trabajadores no modifiquen “ligeramente” sus imágenes ya que se pueda mostrar que ha sido alterada por mínimo que sea el cambio.

Debe de haber muchas más necesidades de protección de las cuales no tengo conocimiento y otras más que con el tiempo irán surgiendo, y con seguridad puedo decir que esta investigación se debe considerar una buena base de partida.

ANEXOS

Se listan en orden cronológico las participaciones en congresos y artículos publicados que respaldan esta investigación. Y se adicionan en extenso los artículos.

- **"Comparación de las Técnicas de Transformada del Coseno Discreto y Wavelets para ocultar información en archivos BMP"**
  IEEE ROC&C, Acapulco, Noviembre 2003.

- "**Marcas de Agua robustas en imágenes digitales, aplicando la Transformada Wavelet**"
  8° Congreso Nacional de Ingeniería Electromecánica y de Sistemas, pp. 86-90, México D. F., Noviembre 2004.

- **"Transformada Wavelet para Marcas de Agua Digitales en Imágenes"**
  IEEE ROC&C, Acapulco, Noviembre 2004.

- **"Wavelets and Discrete Cosine Transform for Hidden Information into Images"**
  Sampling Theory in Signal and Image Processing (STSIP Journal), New York, 4, No.2, pp.141-150, May 2005.

- **"Wavelet Transform for Watermarks in Digital Images"**
  Proceeding of the Pakistan Academy of Sciences, 42, No.2, June 2005, in print.

Wavelets and Discrete Cosine Transform for hidden information into images

M. A. Acevedo
Sección de Estudios de Posgrado e Investigación, Escuela Superior de Ingeniería Mecánica y Eléctrica
Instituto Politécnico Nacional, Edif.. Z-4, 3er piso. Col Lindavista, 07738 México D.F.
e-mails: macevedo@ipn.mx

I. Orea-Flores
Sección de Estudios de Posgrado e Investigación, Escuela Superior de Ingeniería Mecánica y Eléctrica
Instituto Politécnico Nacional, Edif.. Z-4, 3er piso. Col Lindavista, 07738 México D.F.
e-mails: iorea@ipn.mx

J. López-Bonilla
Sección de Estudios de Posgrado e Investigación, Escuela Superior de Ingeniería Mecánica y Eléctrica
Instituto Politécnico Nacional, Edif.. Z-4, 3er piso. Col Lindavista, 07738 México D.F.
e-mails: jlopezb@ipn.mx

Abstract

In this work we perform some tests of steganography and watermarking on BMP format images. We use the Discrete Cosine Transform (DCT) and Wavelets in order to insert information on the high and medium frequencies. When steganography is used, we explain a method to introduce secret data in an image and we show the capacity of the image to accept this data. For the watermarking technique we indicate where the data should be placed in order to achieve a robust insertion of the data even on the presence of image compression. Finally, we make a comparison between these two techniques.

Key words and phrases : Discrete Cosine Transform, Wavelets, Watermarking, Steganography
2000 AMS Mathematics Subject Classification – 42C40, 65T60, 68P30

1 Introduction

Due to a high number of illegal copies of different types of media and espionage, it is of great importance to hide the information (steganography) or to autentificate it [1]. Since most of the communications channels are inherently insecure, we must find a way to interchange information in a secure manner even if using these channels. One alternative to achieving this goal is to transmit information that appears to be “normal” at a first glance while containing hidden information. We concentrate on BMP files for hiding information since it is an image format widely used [2].

In this work we present some results using the Discrete Cosine Transform (DCT) [3] and Wavelets for steganography and watermarking.

On the first part of this article we present a brief description of the DCT and Wavelets techniques in one and two dimensions (vectors and matrices respectively) used to insert information in the frequency domain. After this transformation, information is inserted in the middle and high frequency range of the BMP image.

The inverse procedure most be applied in order to recovery the original BMP file. We then obtain the correlation index of the original and modified image using these two techniques in order to have an insight on how much the resulting image has been modified. Finally, we make a comparison between the DCT and Wavelets to implement the steganography and watermarking on BMP files. Performance is measured through the correlation index as well as the information inserting capacity.

2 Discrete Cosine Transform

The DCT maps the values of the pixels of the image, one by one from the time domain to the frequency domain. Due to the arithmetic form of the DCT, it is reversible [2],[4]. Assuming a one-dimensional image consisting of a linear series of N pixels. Each pixel corresponds to a gray scale p(x) (0≤x<N) where p(x) is a function that varies in space. Then, this image can be represented by the sum of the components of this space f with a frequency ranging from 0 to N-1.

$$p(x) = \sqrt{\frac{2}{N}} \sum_{f=0}^{N-1} C(f) S(f) \cos\left[\frac{(2x+1)\pi f}{2N} \right] \tag{1}$$

$$= \frac{S(0)}{\sqrt{N}} + \sqrt{\frac{2}{N}} \sum_{f=1}^{N-1} S(f) \cos\left[\frac{(2x+1)\pi f}{2N} \right]$$

where

$$C(f) = \begin{cases} 1/\sqrt{2} & f = 0 \\ 1 & f > 0 \end{cases}$$

To calculate (1) we first need to find the coefficients S(f):

$$\{S(f), 0 \le f < N\}$$

The first term in (1) corresponds to the constant component or the zero frequency component. This can be calculated as the average value of p(x), given by:

$$S(0) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} p(x)$$

The general expression for S(f) is:

$$S(f) = \sqrt{\frac{2}{N}} C(f) \sum_{x=0}^{N-1} p(x) \cos\left[\frac{(2x+1)\pi f}{2N} \right] \tag{2}$$

Equation (2) is the one-dimensional DCT of p(x), and (1) is the inverse DCT of S(f) [2], [3], [4].

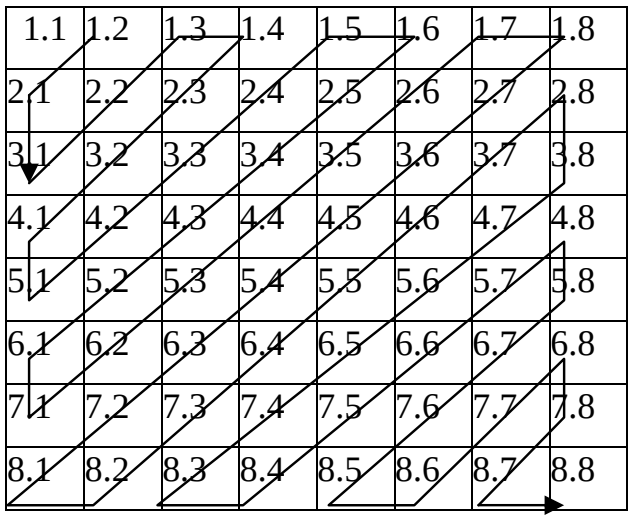


Fig. 1. Frequencies are placed in a diagonal form from the lowest value to the highest value

Frequency values are ordered diagonally as shown in fig 1. Hence, the lowest frequency is placed in position (1,1) while position (8,8) holds the highest frequency value.

3 Two Dimensional DCT

A *NxN* pixel matrix can be represented by the sum of *NxN* cosine functions in the form of:

$$p(x,y) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} C(u)C(v)S(u,v) \cos\left[\frac{(2x+1)\pi u}{2N}\right]\cos\left[\frac{(2y+1)\pi v}{2N}\right] \tag{3}$$

where:

$$S(0,0) = \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} p(x.y)$$

the general equation of *S(f)* is:

$$S(u,v) = \frac{2}{N} C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} p(x,y)\cos\left[\frac{(2x+1)\pi u}{2N}\right]\cos\left[\frac{(2y+1)\pi v}{2N}\right] \tag{4}$$

- Equation 4 is the two-dimensional DCT of *p(x,y).*

4 Steganography using the DCT

Modern steganography systems are very robust since they use some form of transformation from one domain to another.

Transformation methods from one domain to another hide the message in special areas of the image to be transmitted, making the system more robust to specialized attacks, like compression, allowing us to insert a watermark.

The process of insertion is carried out in the frequency domain, therefore we have to transform the image from the space domain to the frequency domain. However, we cannot transform the image in a RGB format directly, we most first convert it to the luminance and crominance equivalent using the next set of equations [1]:

$$Y = 0.99R + 0.587G + 0.114B$$

$$Cb = 0.5 + \frac{B - Y}{2}$$

$$Cr = 0.5 + \frac{R - Y}{1.6}$$

Once the image is in the YCbCr format we can transform it to the frequency domain.During the coding procedure, the image is divided in 8x8 blocks of pixels; exactly one bit of the hidden message is coded in each block. The process of insertion starts by selecting the block b_i in a pseudo-random manner. This block is used to code the *i-th* bit of the hidden message. We then transform the image to the frequency domain using the DCT, resulting the image blocks $B_i = D\{b_i\}$.

Then, we localize two coefficients in the block that will be used to insert the message. Each coefficient is denoted by two index (u_1, v_1) and (u_2, v_2). Both coefficients represent a component in the medium and high frequency range, this guarantees that the hidden information will be saved in a significant part of the image. This also assures that the insertion process will not degrade the image significantly since middle range frequency coefficients have very similar values. The coefficients used could be (4,1) and (3,2). Now, to insert a hidden message in the image we just have to compare the values of the coefficients in the high or middle frequency range.

One frequency block codes a “1” if $B_i(u_1, v_1) > B_i(u_2, v_2)$, otherwise, it codes a “0”. When compression is used, the coefficient values may be altered, therefore it is recommended that $|B_i(u_1, v_1) - B_i(u_2, v_2)| > x$ for every x bigger than zero, this could be achieved by adding a random number to both coefficients. The bigger value of x is chosen, the more robust the system is when compression is used, but the image could be more affected. We then perform the inverse DCT to have the image coefficients in the space domain [3]-[5].

5 Discrete Wavelet Transform (DWT)

Wavelet Haar transform breaks the discrete signal x=(x1,x2, … ,xN) in two sub-signals of half the length of the original. The first sub-signal a1=(a1,a2, ,aN/2) is called the average of signal x and is calculated as explained now: First value a1 is the average of the first couple of values of x: (x1+x2)/2, it is then multiplied by $\sqrt{2}$, thus a1=(x1+x2)/2½. Similarly, next value is calculated using the next couple of values of x as: a2=(x3+x4)/2½. All values of a1 are obtained in this

manner, by averaging pairs of values of x and then multiplying by $\sqrt{2}$. The general formula to obtain a1 is:

$$a_m = \frac{x_{2m-1} + x_{2m}}{\sqrt{2}} \tag{5}$$

For $m = 1,2,3,..., N/2$

The other sub-signal is called the difference of signal x, it is denoted by d1=(d1,d2, ,dN/2) and it is obtained as explained now: the first value of d1 corresponds to half the difference between the first couple of values of x: (x1-x2)/2 and it is then multiplied by $\sqrt{2}$ resulting d1=(x1-x2)/2½. The rest of the values of d1 are obtained in a similar way using:

$$d_m = \frac{x_{2m-1} - x_{2m}}{\sqrt{2}} \tag{6}$$

For $m = 1,2,3,..., N/2$

This procedure accommodates the low frequencies in a1 while the high frequencies are placed in d1.

The wavelet transform can be done in various levels, in this paper we only focus in the first level [3], [6], [7].

6 Discrete Wavelet Transform in Two Dimensions (TWD2)

A discrete image *x* is an M by N matrix of real numbers as shown in (7). The wavelet transformation in two dimensions is obtained in the same manner as it was done in the previous section for one dimension as explained in this part:

$$x = \begin{pmatrix} x_{1,M} & x_{2,M} & \cdots & x_{N,M} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,2} & x_{2,2} & \cdots & x_{N,2} \\ x_{1,1} & x_{2,1} & \cdots & x_{N,1} \end{pmatrix} \tag{7}$$

A. Apply the wavelet transform in each row of *x*, this generates a new matrix.

B. Apply the wavelet transform to the new matrix generated in the previous step but now to each column.

This will create four sub-images of *M/2* rows and *N/2* columns each:

$$f \rightarrow \begin{pmatrix} h^1 & | & d^1 \\ - & & - \\ a^1 & | & v^1 \end{pmatrix} \tag{8}$$

a^1 is calculated averaging over the rows and then averaging over the columns, the sub-image created is then a compression of the original with the low frequency components of the image.

h^1 is calculated as the average of the rows and the difference of the columns, this sub-image save the horizontal details of the image and contains the medium-low frequency components.

v^1 is similar to h^1 except that it holds the vertical details of the image and it contains the medium-high frequency components.

Finally, d^1 contains the diagonal details since it is obtained as the difference of both the rows and the columns and it contains the high frequency components [3], [6], [7].

7 Steganography using the Discrete Wavelet Transform

We now have the matrices a^1, h^1, v^1 and d^1; a^1 matrix is maintained without a change since medium frequencies components are contained in here while a hidden message can be embedded in the rest of the matrices. The insertion of the message is accomplished in this manner: we compare the first couple of values of each matrix, if the first value is higher than the second, we consider it to code a “1”, otherwise it is coded a “0”, we then compare the next pair of values and continue this procedure until the whole matrix is compared.

We have performed several tests using level 2, 3 and 4 Haar transform. The results form this tests lead us to conclude that it cannot be used for this application in case of compression. That is, high level Haar transform concentrates most of the energy of the image in low frequencies and we would like the energy to be distributed in middle-high frequencies since it is in this area where we insert the information, making the watermark robust to compression, therefore it is sufficient to use only level 1 Haar transform.

8 Implementation and Tests

Several tests were performed by inserting a hidden message in the luminance and crominance matrices. We have observed that this method is not robust against compression. Since most of the information is found in the luminance matrix, the crominance matrix is greatly affected by the compression procedure.

By introducing information in the luminance matrix only and in the medium-low frequencies we have observed that after compression we can recovery all the information by using the DCT method.

Under the same conditions we have applied the wavelet method introducing information in the medium-low frequencies only of sub-signal *h* of the luminance matrix. We have obtained satisfactory results since hidden information was successfully recovered after compression.

We compare the amount of information that can be introduced in an image by using the DCT and wavelet techniques. We have used an 192x296x3 pixels image equivalent to 166kbytes.

We discompose an image in its matrix components R, G and B for analyzed each plane of this. In fig 2, 3 and 4 we show the results of 5000 samples of each of the R, G and B matrices of the unaltered (original) image.

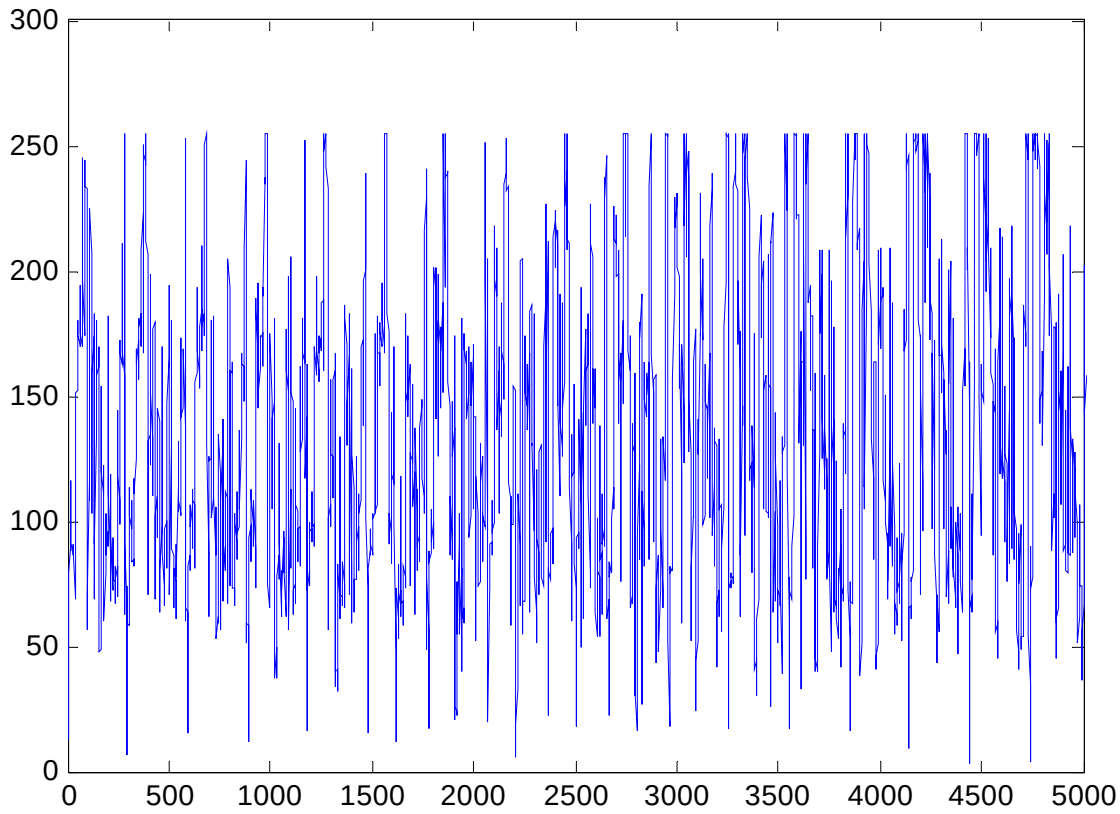


Fig. 2. 5000 samples of the R matrix of the original image.

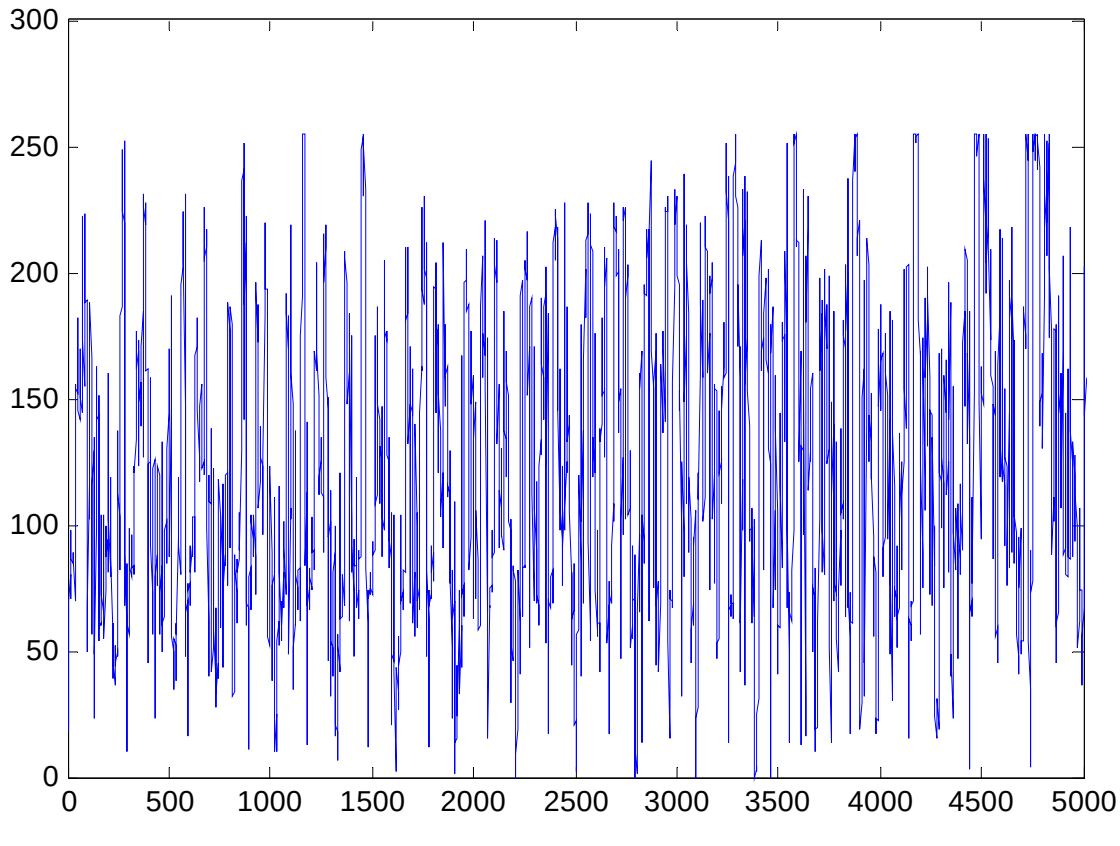


Fig. 3. 5000 samples of the G matrix of the original image.

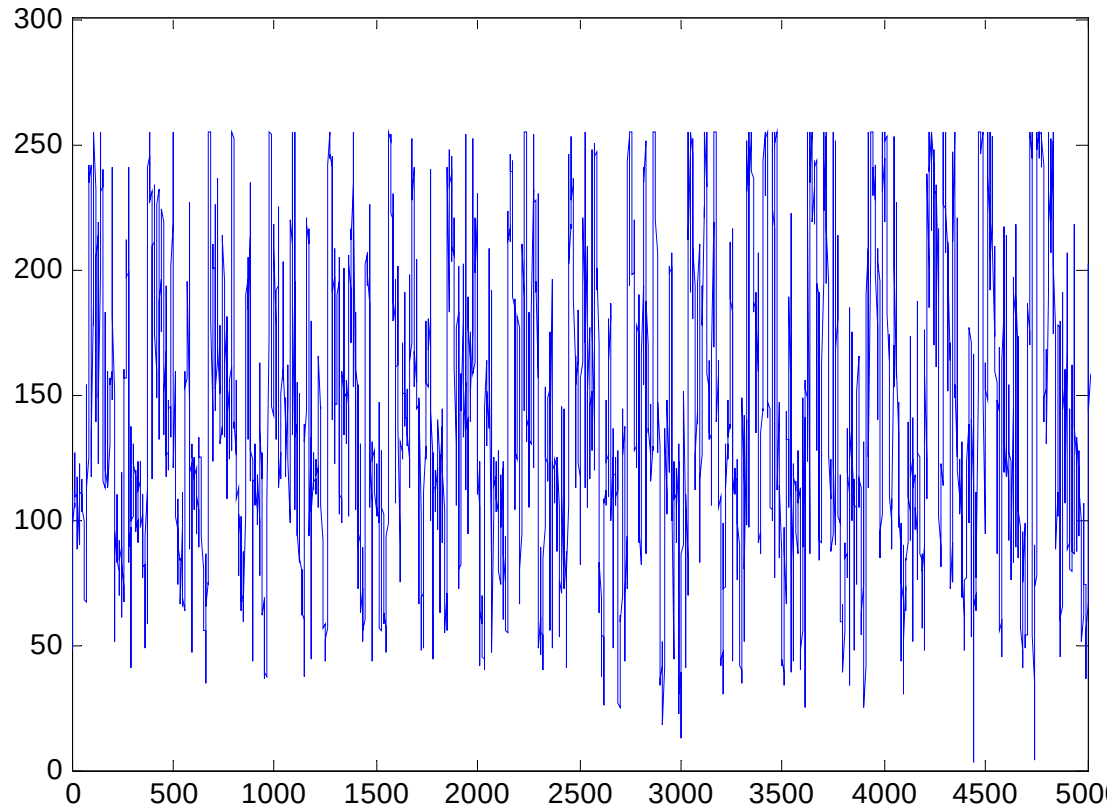


Fig. 4. 5000 samples of the B matrix of the original image.

By using the DCT for steganography we could insert up to 7992 bits in the image, while for watermarking we could introduce up to 888 bits of information. In figs 5, 6, and 7 we can observe the same samples as in the previous figures but modified with 7992 bits embedded using the DCT.

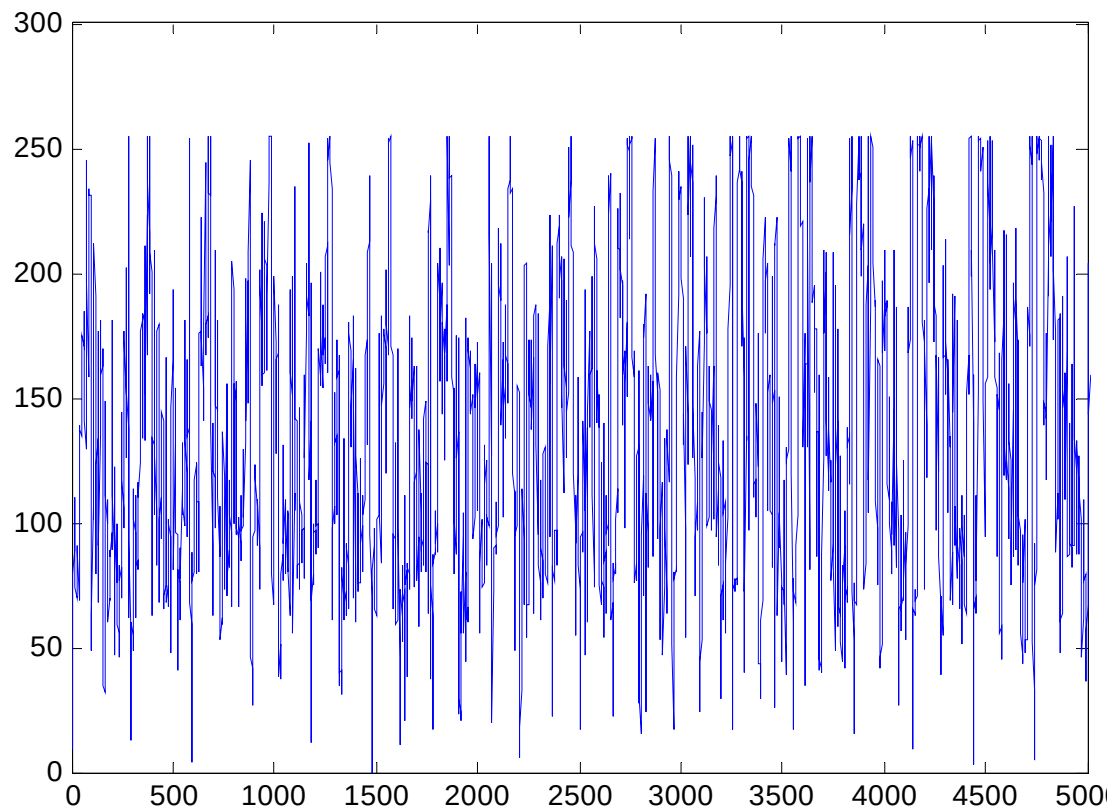


Fig. 5. 5000 samples of the R matrix modified with the DCT.

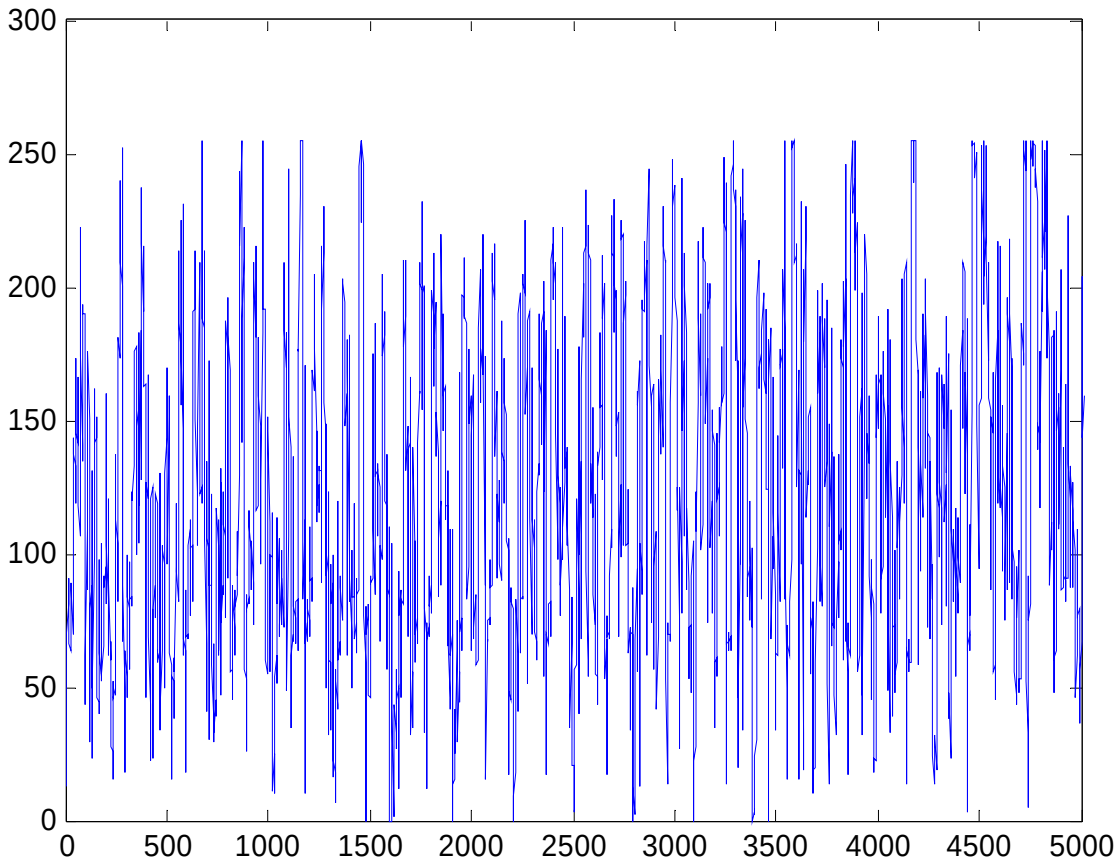


Fig. 6. 5000 samples of the G matrix modified with the DCT.

On the other hand, by using the wavelet transform for steganography it was possible to insert up to 85248 bits while for watermarking it was possible to insert up to 7104 bits. Figures 8, 9 and 10 show the graphics of the same samples selected in the original image with 85248 embedded bits using the wavelet.

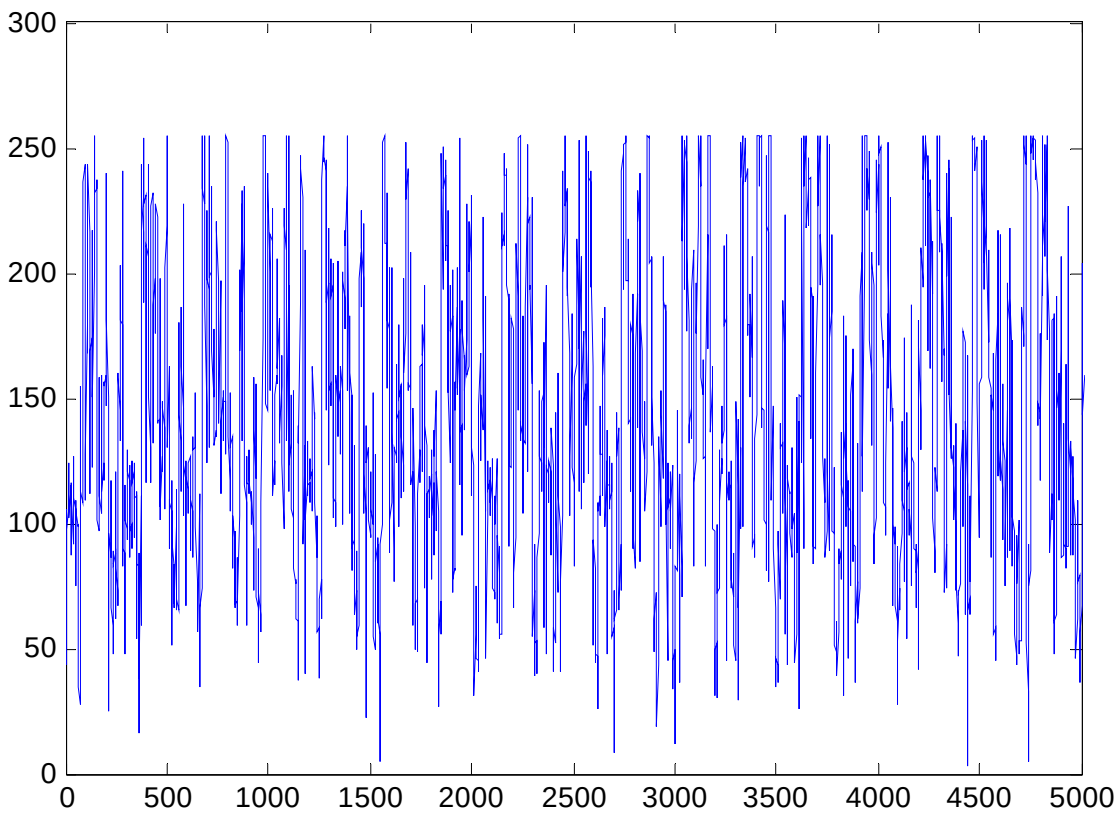


Fig. 7. 5000 samples of the B matrix modified with the DCT.

Finally, we obtained the correlation index between the original image and the modified image to observe how the energy is modified form the original image compared to the modified image with hidden information.

$$\rho_{xy}[l] = \frac{r_{xy}[l]}{\sqrt{r_{xx}[0]\ r_{yy}[0]}} \quad , \ l = 0, \pm 1, \pm 2 \ldots \tag{9}$$

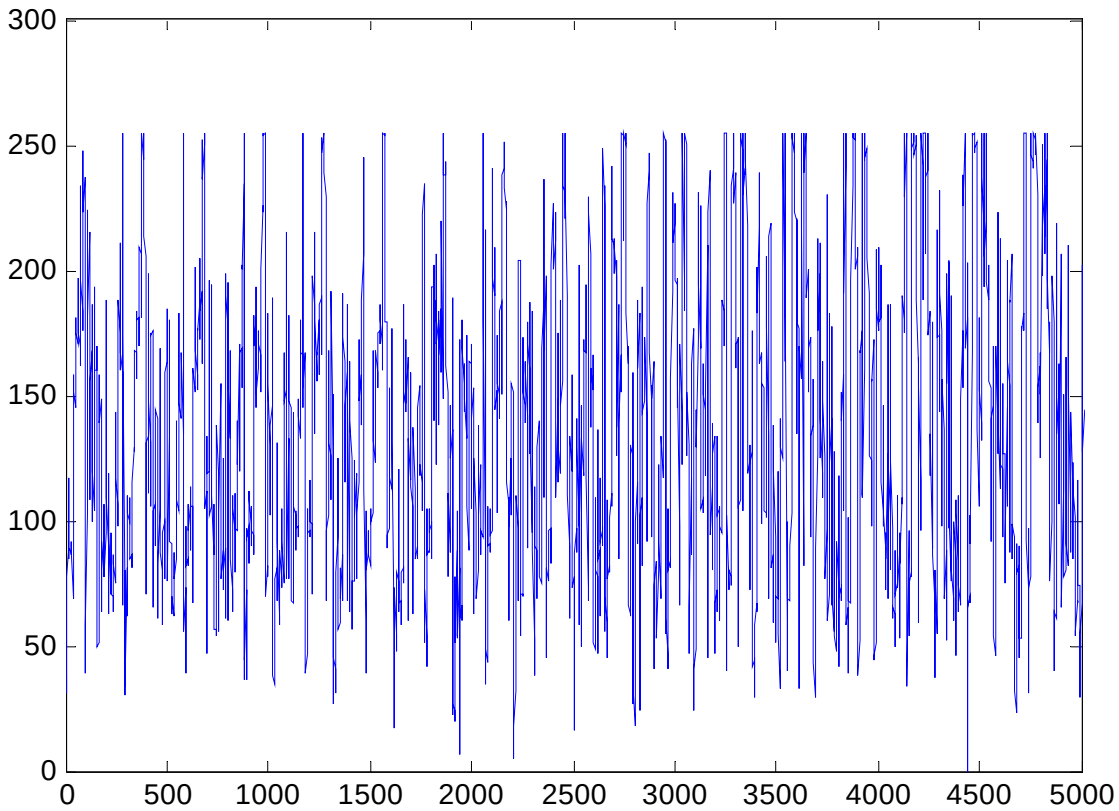


Fig. 8. 5000 samples of the R matrix modified with the wavelet transform.

Fig. 9 5000 samples of the G matrix modified with the wavelet transform.

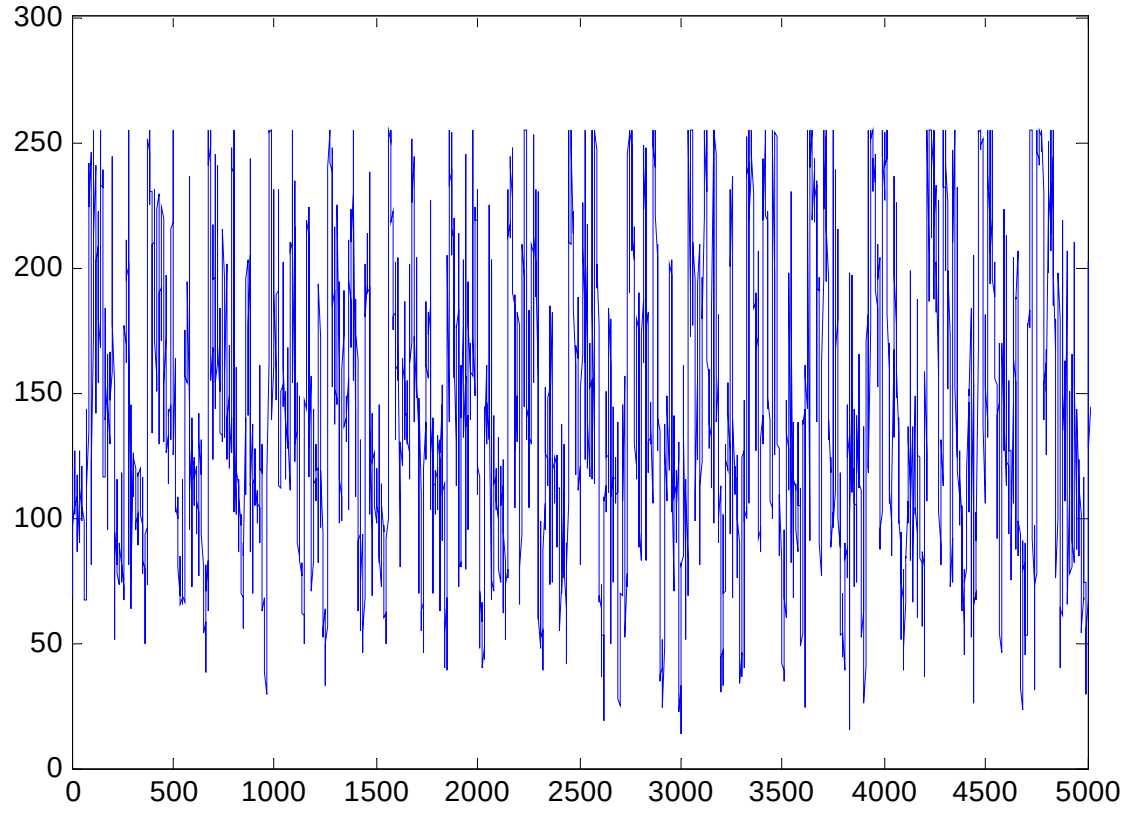


Fig. 10. 5000 samples of the B matrix modified with the wavelet transform.

Where:

$\rho_{xy}[l]$ correlation index
$r_{xy}[l]$ cross-correlation between the original image and the modified image
$r_{xx}[0]$ auto-correlation of the original image
$r_{yy}[0]$ auto-correlation of the modified image

We obtained some results of the correlation of matrices R, G and B of the original image and the modified image with 7992 embedded bits of information using the DCT.

For R:
r_{xx} = *1.3094e+009*
r_{yy} = *1.3087e+009*
r_{xy} = *1.3078 e+009*
ρ_{xy} = *0.9991*

For G:
r_{xx} = *524602704*
r_{yy} = *524111498*
r_{xy} = *523243479*
ρ_{xy} = *0.9979*

For B:
r_{xx} = *389251090*
r_{yy} = *389219220*
r_{xy} = *389205540*
ρ_{xy} = *0.9999*

Here we show the results of the correlation of the R, G and B matrices of the original image and the modified image with 85248 embedded bits of information using the wavelet transform.

For R:
r_{xx} = *1.3094e+009*
r_{yy} = *1.3078e+009*
r_{xy} = *1.3079 e+009*
ρ_{xy} = *0.9994*

For G:
r_{xx} = *524602704*
r_{yy} = *523707306*
r_{xy} = *523413901*
ρ_{xy} = *0.9986*

For B:
r_{xx} = *389251090*
r_{yy} = *389216544*
r_{xy} = *389196760*
ρ_{xy} = *0.9999*

Conclusions

By observing the results on the previous section for hiding information (steganography and watermarking) we can conclude that both techniques modify the original image file in a very small amount. We can also see that by inserting the information in specific areas with both techniques the embedded information can survive the process of compression.

Finally we compare the capacity to insert information and we can see that the wavelet technique is much better than the DCT technique.

After several tests with different images we obtained the next results: For the DCT we could hide approximately 0.54% of the information compared to the size of the original image file for watermarking. For steganography the percentage of information for hidden information is 4.82%.

For the Wavelet method, we could insert approximately 4.27% of information compared to the original size of the image file for watermarking. For steganography, the percentage is approximately 51.3% of embedded information.

Bibliography

[1] Cachin, C., “An Information –Theoretic Model for Steganography”, Second International Workshop on Information Hiding, vol. 1525 1998.
[2] Stefan Katzenbeisser, Fabien A. P.,Petitcolas, “Information Hiding, Principles of Steganography”, Artech House, 2000
[3] Rao, K. R., and P. Yip, Discrete Cosine Transform: Algorithms, Advantages, Applications, New York: Academic Press, 1990.
[4] D. Knuth, The Art of Computer Programming, Vol. 2, Seminumerical Algorithms, 2nd edition, Addison - Wesley, 1981.
[5] Bruce Schneirer, “Applied Cryptography”, John Wiley and sons, inc., 1994.
[6] James S. Walker, “A Primer on WAVELETS and their Scientific Applications”, Chapman & Hall/crc, 1999.
[7] Martin Vetterli, Jelena Kovacevic, “WAVELETS and subband coding” Prentice Hall, 1995.

Wavelet Transform for Watermarks in Digital Images

M. Acevedo-Mosqueda, J. López-Bonilla, I. Orea-Flores
Sección de Estudios de Posgrado e Investigación ESIME-IPN
UPALM Edificio Z-4 3er Piso, Col. Lindavista, México D.F. C.P. 07738
Email: iorea@ipn.mx, macevedo@ipn.mx, jlopezb@ipn.mx

***Abstract*- In this paper we study wavelet filters applied to watermarking in order to protect copyrights. Information is inserted in the transformed domain of the image. This transform is based on the analysis of the main components and wavelet transform. The watermarked image is reconstructed applying the inverse transform. We perform mathematical proofs over the image to demonstrate that the original image is slightly altered after the watermarking process. Finally, we simulate different attacks such as JPEG compression and adding noise to the watermarked image. We argue that this method is efficient based on robustness and security.**

***Key words* -- Wavelets, Watermarks, Copyrights**

I. INTRODUCTION

In these days, due to the increment of illegal copies and espionage in different communications media, digital watermarking is essential to protect copyrights in digital images [7]. This lead us to interchange information in a secure manner over insecure communication channels. Watermarking techniques slightly modify the original data, hence it is almost invisible [8].

In steganography, the main objective is to insert a message as a watermark inside a carrier image [1, 9]. Watermarking technique requires the following properties in order to use it: legibility, security, invisibility and robustness. Legibility refers to the ability to detect the embedded information whenever it is required to extract it, security consists in camouflage the watermark in such a way as to make it unnoticeable for the rest of the people; for purposes of invisibility it is very important to select the carrier images and finally, robustness refers to the ability for the watermark to resist a number of attacks [3, 4, 10]. These attacks include digital image processing operations such as compression, geometric distortion and different kinds of noise.

Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT) are the most popular domains for watermarks [11]. In general, the DWT produces images with more visible watermarks and with more storage capacity [12].

The first part of the paper focuses on the description of the DWT, the inverse DWT (which is used to reconstruct the image with an embedded watermark) and finally we explain the procedure to recover the embedded information. Then, we describe the different attacks that can alter the watermark, showing a table comparing the results from the tests by submitting the watermarked images to the different attacks.

II. WAVELET DISCRET TRANSFORM (DWT)

Signal x(n) is passed trough a bank of mirror filters in cuadrature [13]. Resulting signal of each filter is decimated by a factor of 2.

Signal resolution, which accounts for detailed amount of information inside the signal, is modified by the filters and is scaled by the decimation operation. Decimation of a signal corresponds to a reduction of the sampling frequency or to the discarding of some of the samples of the signal. This process of filtering and decimation is known as sub-band coding as shown in fig 1.

This procedure can be expressed as:

$$y_{high}[k] = \sum_{n} x[n] \cdot g[2k - n] \tag{1}$$

$$y_{low}[k] = \sum_{n} x[n] \cdot h[2k - n] \tag{2}$$

Where $y_{high}[k]$ and $y_{low}[k]$ are the output of the high pass filters and low pass filters respectively, after the decimation by 2.

This is the operation mode of the DWT, this procedure analyzes the signal in different frequency bands with different resolutions through decomposition of the different components of the signal from high energy to low energy. This decomposition of the signal in different frequency bands is accomplished through successive filtering of the signal in the time domain as show in fig 1. The original sequence x[n] is passed through a high pass filter g[n] and a low pass filter h[n].

Sub-band coding can be repeated to achieve more decomposition. Each level of filtering and decimation will result in half the number of samples (and hence, half the

number of time resolution.) Depending of the chosen wavelet, coefficients of g and h will change.

There are a number of different wavelets transforms, however we have only worked with the Haar wavelet transform, which after a number of tests was the more appropriate for this particular application, which indicates to apply the transform only at the first level. [2, 5, 6].

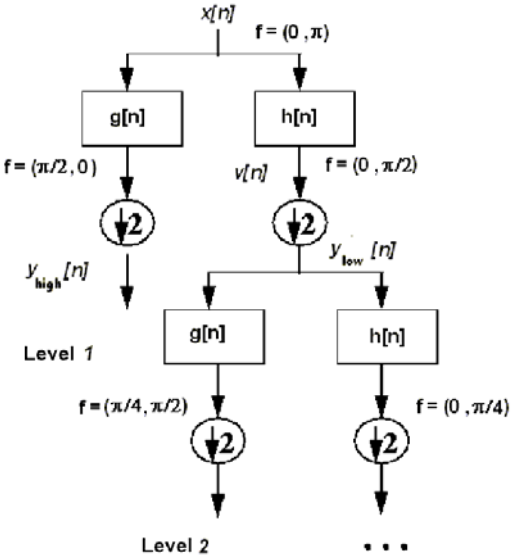


Fig. 1. Sub-band coding algorithm

DWT in two dimensions

A discrete image X is a matrix with M rows and N columns of real numbers, where M and N have to be even integers:

$$X = \begin{pmatrix} x_{1,M} & x_{2,M} & \cdots & x_{N,M} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,2} & x_{2,2} & \cdots & x_{N,2} \\ x_{1,1} & x_{2,1} & \cdots & x_{N,1} \end{pmatrix} \quad (3)$$

The wavelet transform in two dimensions is obtained with the same equations than for one dimension, performing the next steps:

A. Applying the wavelet transform to each row X, which will produce a new matrix.

B. Applying to this new matrix obtained in step A the wavelet transform again, but this time to each column.

This results in four sub-images of M/2 rows and N/2 columns:

$$f \rightarrow \begin{pmatrix} h^1 & | & d^1 \\ - & & - \\ a^1 & | & v^1 \end{pmatrix} \quad (4)$$

a^1 is calculated with the average of the rows followed by the average of the columns, resulting in this sub-image a compression of the original, it contains low frequency components.

h^1 is calculated with the average of the rows and the difference of the columns, here the horizontal details of the image are preserved and contains middle-low frequency components.

v^1 is similar to h, except that vertical and horizontal components are interchanged, this sub-image contains the vertical details, conserving components of middle-low frequency components.

Finally, d^1 contains the diagonal details and it is calculated as the difference of the columns and rows and contains the high frequency components. [2, 5, 6].

III. DWT APPLIED TO WATERMARKING

Once we have sub-matrices a^1, h^1 ,v^1 and d^1. Matrix a^1 is kept intact since it contains the low frequency components, if it is altered it could have a big impact in the image which is not recommendable. Matrices v^1 and d^1 are not used either to embed a watermark since they contain middle high and high frequencies respectively being the most vulnerable in case of an attack. This only leaves matrix h^1, which contains the middle low frequencies, this makes it the must robust part to attacks after low frequencies, but the difference is that changes in this matrix will not be perceptible.

The watermark is inserted following the next procedure: the first pairs of components of the matrix are compared, if the first is higher than the second one it is considered as a "1", otherwise it will be considered as "0", then the next pair of values are compared and the same insertion criteria is used until the whole matrix is compared. This is also the general procedure for a steganographic application.

For watermarking we have make several tests with different images, we have confirmed that by distributing the information among the luminance and crominance matrices it is not robust against compression. We have also proved

that the higher percentage of information is found in the luminance matrix, this means that the crominance matrices will be the more affected in case of compression.

By storing information only in the middle low frequencies of sub-matrix h1 of luminance we obtained satisfactory results.

IV. Attacks

There are various types of attacks to try to eliminate a watermark. It is important to notice that for an attack to be efficient it should eliminate the watermark without modifying visibly the image.

Types of attacks

A. Compression. When a commercial method of compression is applied to the image to eliminate the watermark, and then it is returned to the original format.

B. Geometric Distortion. Consists in summing to each pixel of image a small value to modify it completely without noticing visually.

C. Noise. There are different types of noise that can be summed to the image to alter it. Such as:

Multiplicative Noise: it uses the next equation $g = f + n * f$ to sum the noise to the image, where f is the image and n is a random variable uniformly distributed. The range in which n takes values depends on the variance. This noise softens the image in a uniform manner, hence for a small variance the effect on the image is also small.

Impulsive Noise: it adds random values to some of the pixels of the image, the amount of pixels that are affected is related to the variance. The elements altered by this noise are very noticeable in the image.

Gaussian Noise: it adds noise normally distributed (as shown in table 1). This noise is more aggressive than the rest since it distorts the whole image, making it very susceptible.

Type	PDF	Mean and Variance
Impulsive	$p_z(z) = \begin{cases} P_a & z = a \\ P_b & z = b \\ 0 & \text{otherwise} \end{cases}$ $b > a$	$m = aP_a + bP_b$ $\sigma^2 = (a-m)^2 P_a + (b-m)^2 P_b$
Gaussian	$p_z(z) = \frac{1}{\sqrt{2\pi}b} e^{-(z-a)^2/2b^2}$ $-\infty < z < \infty$	$m = a$ $\sigma^2 = b^2$

Table 1. Noise Models

V. Implementation and Tests

First we show, graphically and mathematically how the original image changes with respect to the image with the embedded watermark, then it can be seen how the image is affected with the watermark with each attack. Figures only show the test in one image due to the extension it occupies, but a table is annexed with the mathematical prove of five different images. All tests were done by introducing information at its maximum capacity [12].

Fig 2, 3 and 4 shows 3500 samples taken to each matrix R, G and B. The one in red corresponds to the original image and the one in blue show the image with the watermark.

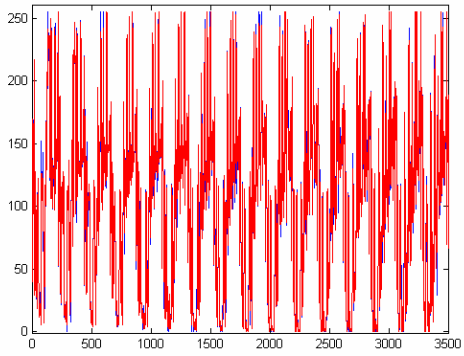


Fig. 2. Graphic of 3500 samples of matrix R, in red the original image and in blue the watermarked image.

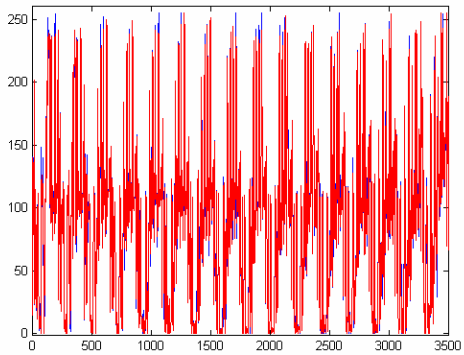


Fig. 3. Graphic of 3500 samples of matrix G, in red the original image and in blue the watermarked image.

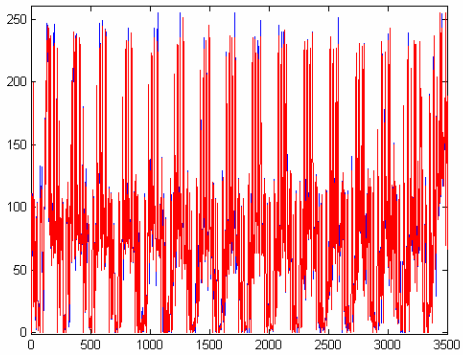


Fig. 4. Graphic of 3500 samples of matrix B, in red the original image and in blue the watermarked image.

In the three before figures we can see the changes suffered by the watermark in each plane, although when recovering the image, this changes are not noticeable.

Figs. 5, 6 and 7 show the same 3500 samples taken in each matrix R, G and B, but now in red we have the image with the watermark and in blue the same image with multiplicative noise with variance of 0.001.

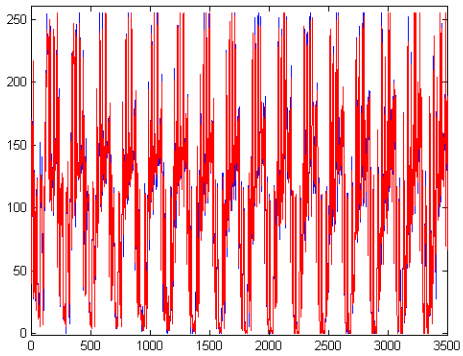


Fig. 5. Graphic of 3500 samples of matrix R, in red the watermarked image and in blue the watermaked image with multiplicative noise.

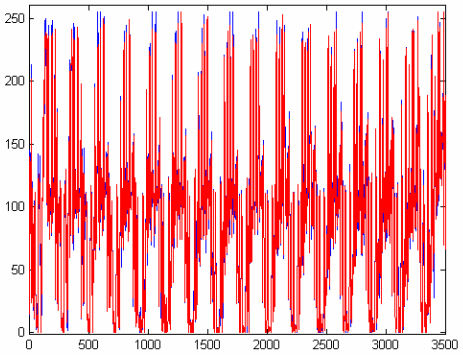


Fig. 6. Graphic of 3500 samples of matrix G, in red the watermarked image and in blue the watermaked image with multiplicative noise.

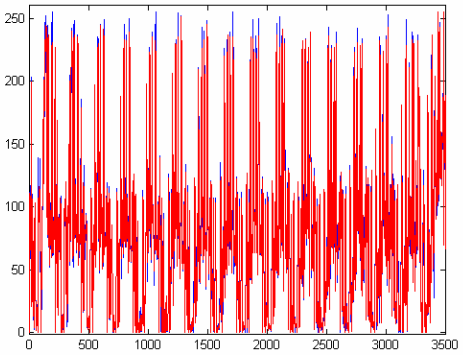


Fig. 7. Graphic of 3500 samples of matrix B, in red the watermarked image and in blue the watermaked image with multiplicative noise.

Multiplicative noise softens the image and with small variance, as the one used here of 0.001, the alteration is almost not perceptible, and the watermark resisted 100% in different images.

Figs. 8, 9 and 10 show the same samples selected in the previous graphs. In red we have the watermarked image and in blue the same image after adding the impulsive noise with variance of 0.001.

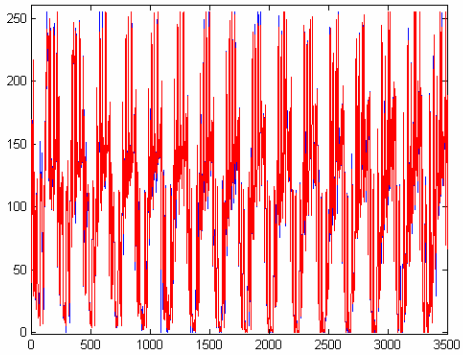


Fig. 8. Graphic of 3500 samples of matrix R, in red the watermarked image and in blue the watermaked image with impulsive noise.

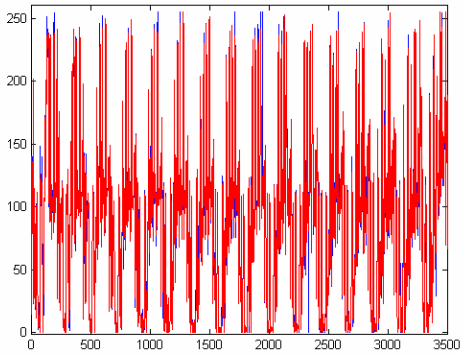


Fig. 9. Graphic of 3500 samples of matrix G, in red the watermarked image and in blue the watermaked image with impulsive noise.

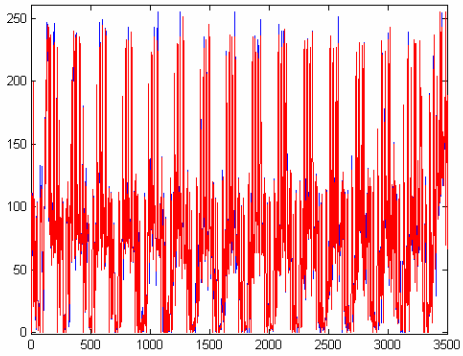


Fig. 10. Graphic of 3500 samples of matrix B, in red the watermarked image and in blue the watermaked image with impulsive noise.

Adding impulsive noise to the image, visually is very notorious, hence it is a very perceptible attack. After several tests with different images 12% of the embedded information was lost.

In Figs. 11, 12 and 13 we have the same samples taken in each matrix R, G and B, where the graph in red shows the watermarked image and in blue the same image with noise but now gaussian with variance of 0.001.

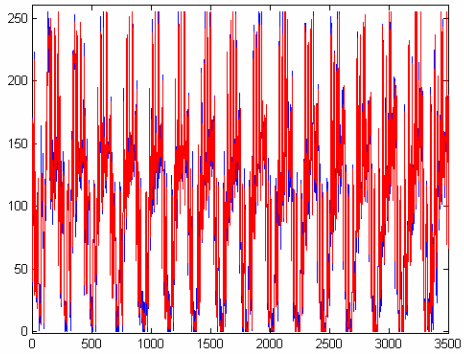


Fig. 11. Graphic of 3500 samples of matrix R, in red the watermarked image and in blue the watermaked image with gaussian noise.

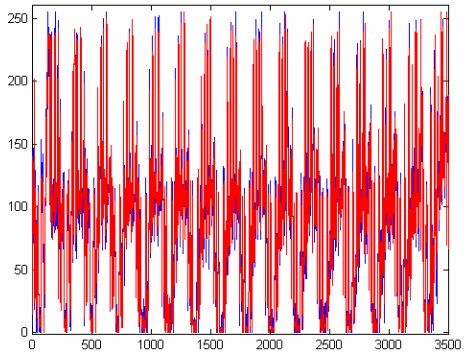


Fig. 12. Graphic of 3500 samples of matrix G, in red the watermarked image and in blue the watermaked image with gaussian noise.

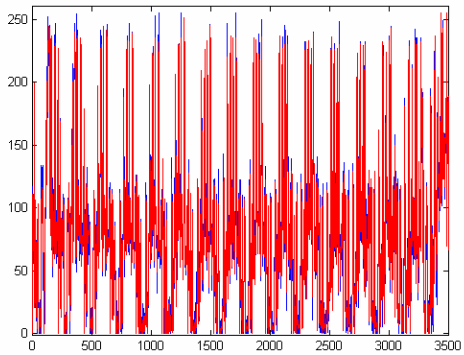


Fig. 13. Graphic of 3500 samples of matrix B, in red the watermarked image and in blue the watermaked image with gaussian noise.

As in the previous examples, the tests corresponds to a variance of 0.001, loosing an average of 16% of the watermark.

Gaussian noise and impulsive noise affects in different manner the image but they are much more notorious than multiplicative noise, which is reflected in these figures.

For the geometric distortion, we have done several tests using shifting in the range of 1 to 80. It is important to mention that using a shifting higher than 15 will produce a visible modification on the image. The purpose of using higher values of shifting in this work is to prove that watermark always resists the attack regardless of the value added since the inserted information is embedded comparing pairs of values, and the added value does not alter this relation. The histogram shown in Figure 14 shows the impact on an image caused by applying a shifting of 50.

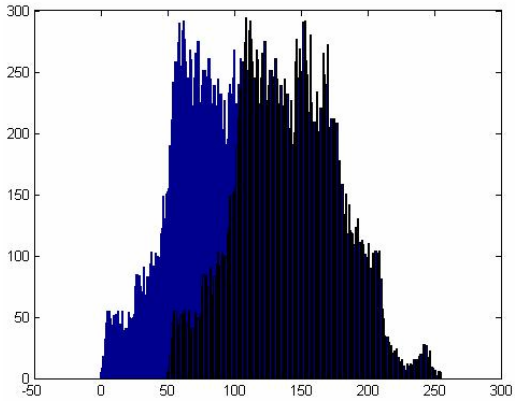


Fig. 14. In blue the Histogram of the watermarked image and in black the watermarked image with shifting of 50.

Compression was done with commercial software with formats BMP, JPEG and Zip. This software offer a compression rate in ranging from 50% to 70%. However, if the watermark is embedded in the zone that we propose in this paper, we achieved satisfactory results when the watermark was recovered.

The mathematical analysis was done with the correlation index, energy percentage recovered and PSNR (Peak Signal to Noise Ratio). Results are shown in tables 2, 3, 4, 5 and 6.

We calculated the correlation index between the original image and the modified image as follows:

$$\rho_{xy}[l] = \frac{r_{xy}[l]}{\sqrt{r_{xx}[0]\ r_{yy}[0]}} \qquad l = 0, \pm 1, \pm 2... \qquad (5)$$

Where:

$\rho_{xy}[l]$ Correlation index

$r_{xy}[l]$ Cross correlation between the original image and the modified image.

$r_{xx}[0]$ Autocorrelation of the original image.

$r_{yy}[0]$ Autocorrelation of the modified image.

And we calculated the PSNR as follows:

$$PSNR(dB) = 10\log_{10}\left(\frac{XY \max P_{x,y}^2}{\sum_{x,y}\left(P_{x,y} - \tilde{p}_{x,y}\right)^2}\right) \qquad (6)$$

Where:

X and Y Are the number of rows and columns, respectively.

$P_{x,y}$ Represents a pixel, whose coordinates are (x,y) in the original image.

$\tilde{P}_{x,y}$ Represents a pixel, whose coordinates are (x,y) in the watermarked image.

	Original Image	Multiplicative Noise	Impulsive Noise	Gaussian Noise	Compression Noise
Image 1 watermarked	0.9999802	0.9995113	0.9990186	0.9971078	0.9998389
Image 2 watermarked	0.9999452	0.9995288	0.9974101	0.9936245	0.9997492
Image 3 watermarked	0.9999680	0.9994625	0.9993945	0.9985986	0.9998637
Image 4 watermarked	0.9999527	0.9995152	0.9995084	0.9983921	0.9999640
Image 5 watermarked	0.9998189	0.9994995	0.9994154	0.9981030	0.9999698

Table 2. Matrix R correlation

	Original Image	Multiplicative Noise	Impulsive Noise	aussian Noise	Compression Noise
Image 1 watermarked	.9999890	.9995032	.9992693	.9975235	.9999630
Image 2 watermarked	.9999852	.9994990	.9967019	.9912684	.9998664
Image 3 watermarked	.9999759	.9995145	.9988478	.9967613	.9998922
Image 4 watermarked	.9999742	.9995039	.9995321	.9983535	.9999862
Image 5 watermarked	.9998982	.9994947	.9989822	.9968874	.9999764

Table 3. Matrix G correlation

	Original Image	Multiplicative Noise	Impulsive Noise	Gaussian Noise	Compression Noise
Image 1 watermarked	.9999960	.9994985	.9985537	.9956487	.9995689
Image 2 watermarked	.9999853	.9994938	.9936931	.9912684	.9990533
Image 3 watermarked	.9999510	.9996421	.9985542	.9956853	.9991845
Image 4 watermarked	.9999733	.9995036	.9993014	.9979530	.9992126
Image 5 watermarked	.9998845	.9994977	.9988778	.9960856	.9991357

Table 4. Matrix B correlation

	Original Image	Multiplicative Noise	Impulsive Noise	Gaussian Noise	Compression Noise
Image 1 watermarked	99.980944	100.05124	100.19359	100.54094	99.880423
Image 2 watermarked	99.950691	99.928101	100.73372	101.78531	99.751472
Image 3 watermarked	99.915630	100.02666	100.15554	100.46218	100.15554
Image 4 watermarked	99.969529	100.04989	100.07206	100.33814	99.936251
Image 5 watermarked	100.40056	100.08783	100.17762	100.56995	99.929731

Table 5. Energy percentage recovered of the watermarked image

	Image 1 watermarked	mage 2 watermarked	mage 3 watermarked	mage 4 watermarked	mage 5 watermarked
Original image	43.388288	43.241299	42.811934	43.201236	43.132489

Table 6. Metric distortion by PSNR (dB)

VI. Conclusions

The objective of this research is to demonstrate the legibility, security and robustness of this technique of embedding digital watermark, which in our opinion is accomplished for the following reasons. It is legible since the embedded information can be recovered using the inverse transform procedure. It is secure since for any non-authorized person it is not evident the existence of the watermark. And more importantly, it resists compression such as JPEG, geometric distortion and multiplicative noise, attacks that alter the image in a uniform manner and these types of attacks will not affect the embedded information, hence it will resist a watermark. On the other hand, impulsive noise and gaussian noise affect the watermark, but we should remember that if an attack is effective it should not alter visibly the image, and these two attacks clearly affect the image.

It should be noted that watermarked images have a high quality. This means that by embedding the watermark the image is not altered significantly. This can be seen in the first value of both the correlation and the energy tables and in table 6 of metric distortion.

Finally we would like to thank Professor Dr. Shihao Wang, Institute of Electronics, National Chiao Tung University, Taiwán, for all his observations and comments for the enrichment of this paper.

VII. References

1 Orea, I. 2002. Intercambio de información utilizando protocolos de canal subliminal. U.P.I.I.T.A-I.P.N, Mexico city

2 Katzenbeisser, S. and Petitcolas, F. 2002. Information Hiding. Principles of Steganography. Artech House, London

3 Knuth, D. 1981. The art of computer programming. Seminumerical algorithms. Vol 2. Addison Wesley, New York.

4 Schneirer, B. 1994. Applied cryptography. John Wiley and Sons, New York

5 Walter, J.S. 1999. A primer on wavelets and their scientific applications. Chapman & hall/CRC Press, London

6 Vetterli, M. and Kovacevic, J. 1995. Wavelets and sub-band coding. Prentice Hall, New Jersey

7 O´ Ruanaidh, J., Dowling, W. and Boland, F. 1996. Watermarking digital images for copyright protection. IEE Proc. Vision and Signal Processing 143: 250-256

8 Wang, S and Lin, Y. 2004. Wavelet tree quantization for copyright protection watermarking. IEEE Trans. Image Processing 13: 154-165

9 Artz, D. 2001. Digital steganography, hiding data within data, IEEE Internet Computing, 5: 75-80

10 Kaarna, A. and Toivanen, P. 2003. Digital watermarking of spectral images in PCA/Wavelet-transform domain. Proc. Intal. Geoscience and Remote Sensing Symposium (Toulouse, Frence) 6: 3564-3567

11 Loo, P. and Kingsbury, N. 2000. Digital Watermarking with complex wavelets. IEE Proc. Colloquium on Secure Images and Images Authentication, London

12 Acevedo, M and Orea, I. 2003. Comparación de las técnicas de transformada del coseno discreto y wavelets para ocultar información en archivos BMP. IEEE Conf. ROC&C, Acapulco city, Mexico

13 Mitra, S. 2003. Digital signal processing: a computer based approach. McGraw-Hill, New York, pp. 88-94