**UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO**

**FACULTAD DE INGENIERÍA**

# PROTECCIÓN DE DERECHOS DE AUTOR EN IMÁGENES DIGITALES DE COLOR USANDO MARCA DE AGUA HIBRIDA Y ROBUSTA

# T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACIÓN

PRESENTA
CARLOS ALDAIR ROMAN BALBUENA

DIRECTOR DE TESIS
DR. MANUEL CEDILLO HERNÁNDEZ

**MÉXICO, D.F.** **NOVIEMBRE 2015**

# Agradecimientos

A la Universidad Nacional Autónoma de México, por toda mi formación.

Un especial agradecimiento al Dr. Manuel Cedillo Hernández por haberme apoyado en la realización de este trabajo y haberme guiado de principio a fin en la elaboración del mismo.

A la Facultad de Ingeniería por todo lo que me ha bridado a lo largo de toda mi trayectoria académica.

Al programa de apoyo a proyectos de investigación e innovación tecnológica PAPIIT por el apoyo económico obtenido a través del proyecto con clave: IA105215 e intitulado: Diseño e implementación de algoritmos computacionales para el desarrollo de aplicaciones avanzadas relacionadas con el procesamiento de multimedia digital.

A mi madre y a mi padre por su constante ayuda, apoyo y consejos durante toda mi vida.

A mi hermano y hermana por su compañía y apoyo en el transcurso de toda mi vida.

Finalmente a todas mis amistades que me han acompañado a lo largo de estos años brindándome sus consejos, su apoyo y confianza.

# Resumen

En este trabajo se presenta un método de marcado de agua hibrido robusto e imperceptible con el fin de ser aplicado a imágenes digitales de color cuyo propósito es detectar copias ilegales, usando una autenticación de usuario. Con el objetivo de mejorar la robustez del método propuesto ante diversos ataques geométricos y de procesamiento de señal, se utilizan dos diferentes técnicas de marcado de agua para insertar un mismo patrón de marca de agua. Dicha marca de agua está compuesta por un patrón binario obtenido a partir de un hash criptográfico de los datos del usuario usando la función RIPEMD-160. La Transformada Discreta de Fourier (DFT) y un histograma bidimensional, ambos dentro del modelo de color YCbCr, son usados para añadir la misma secuencia de marca de agua. La calidad de la imagen marcada es medida usando las métricas de Relación Señal a Ruido Pico (PSNR) y el Índice de Similitud Estructural (SSIM). La diferencia de colores es medida usando la Diferencia de Color Normalizada (NCD). La Tasa de Bits Erróneos (BER) en conjunto con un umbral de decisión es utilizada en la etapa de detección para distinguir si una imagen está o no protegida. Se proponen mejoras para la determinación óptima de los parámetros críticos del algoritmo de marca de agua, tales como el factor de fuerza de inserción y la cantidad útil de la marca de agua (número de bits que la componen), así mismo también se evalúa el rendimiento del algoritmo de marcado en términos de robustez e imperceptibilidad con fines de proteger los derechos de autor en imágenes digitales de color. Los resultados experimentales muestran que el algoritmo propuesto es imperceptible y a su vez robusto ante distintos procesamientos de imagen digital de carácter intencional y no intencional, tales como distorsiones geométricas, compresión de datos, contaminación por ruido de canal y filtrado artístico.

# Abstract

In this paper presents a robust and imperceptible hybrid watermarking method in order to be applied to digital colored- images with the purpose of detecting illegal copies, using a customer robust authentication. In order to improve the robustness of the proposed method against several common signal processing and geometrical attacks, two different watermarking techniques are used to insert the same watermark pattern. The watermark is composed by a binary pattern obtained from a cryptographic hash of the customer data using the RIPEMD-160 function. Discrete Fourier Transform (DFT) and a bi-dimensional histogram, both into the YCbCr color model domain, are used to embed the same sequence watermark. The quality of the watermarked image is measured using the following well-known indices peak signal to noise ratio (PSNR) and structural similarity index (SSIM). The color difference is measured using the Normalized Color Difference (NCD). The Bit Error Rate (BER) in along with a decision threshold detection step to distinguish whether image or not is protected. Improvements for optimal determination of the critical parameters of the algorithm of watermark, such as the factor of insertion force and the useful amount of the watermark (number of bits that comprise it), are also proposed as assessment marking algorithm performance in terms of robustness and imperceptibility purposes of protecting copyright in digital color images. Experimental results show that the proposed algorithm is imperceptible and robust against several digital image processing intentional and unintentional, for instance geometric distortions, data compression, noise pollution and artistic channel filtering.

# Contenido

## Capítulo 1.

## Introducción



## Capítulo 2.

## Marco Teórico

## Capítulo 3.

## Algoritmo de marca de agua propuesto



## Capítulo 4.

## Resultados experimentales

## Capítulo 5

## Conclusiones generales y trabajo a futuro.

# Lista de Figuras y Tablas

## Capítulo 2.

## Marco Teórico



## Capítulo 3.

## Algoritmo de marca de agua propuesto

## Capítulo 4

## Resultados experimentales

# Capítulo 1
# Introducción

## 1.- Introducción General

En la actualidad la fácil manipulación de la información en formato digital ha provocado que resulte complicado conseguir una completa protección de los derechos de autor de los propietarios de dicha información, motivo por el cual, en las últimas dos décadas han surgido técnicas y propuestas de investigación, cuyo propósito es añadir información adicional a formatos digitales tales como imágenes, audio o video, con el propósito de proteger los derechos de autor y evitar que estos sean distribuidos ilegalmente.

Una técnica que en los últimos años ha tenido gran auge como propuesta de investigación es el marcado de agua digital, cuyo propósito es conseguir un nivel de seguridad tal que permita asegurar la protección de derechos de autor.

En el ámbito de las imágenes digitales, aunque en la actualidad existen distintos algoritmos de marca de agua propuestos en la literatura, que intentan proteger los derechos de autor de dichos materiales digitales, muchos de ellos se centran únicamente en obtener un alto grado de robustez ante diferentes procesamientos avanzados de señal, tales como la compresión de imágenes JPEG, la contaminación de imágenes por ruido Gaussiano e impulsivo, el filtrado, entre otros. Sin embargo, al solo considerar esta clase de procesamientos de señal, los algoritmos de marcado de agua digital pueden presentar una robustez débil al momento de recuperar o detectar la información insertada cuando la imagen ha sido procesada usando alguna distorsión geométrica, como por ejemplo el escalamiento, la rotación y la

traslación de píxeles, provocando que se elimine la sincronización con la cual la señal de marca de agua fue insertada originalmente.
Al perder la sincronización entre las etapas de inserción y detección, los algoritmos de marcado de agua digital pueden generar errores en el proceso de detección correspondiente.

Tomando en cuenta lo anterior, es importante que al momento del diseño de un algoritmo de marcado de agua se consideren tanto las distorsiones geométricas así como los procesamientos de señal avanzados y así poder cumplir con el objetivo principal que es la protección de derechos de autor.

Este trabajo está enfocado en el diseño de una solución en software que implemente un algoritmo de marcado de agua en imágenes digitales de color, que permita una alta imperceptibilidad y robustez para poder aportar una herramienta que salvaguarde los derechos de autor de los propietarios de imágenes digitales.

## 1.1 Objetivos

- Proponer y evaluar la implementación en una solución de software de un algoritmo de marcado de agua digital, con fines de protección de derechos de autor en imágenes digitales.
- Diseñar un prototipo de software bajo el paradigma de desarrollo orientado a objetos que permita integrar las etapas de generación, inserción y detección de una marca de agua digital para proteger los derechos de autor de imágenes digitales de color.
- Evaluar el rendimiento del algoritmo de marcado de agua digital en términos de robustez e imperceptibilidad.
- Proteger los derechos de autor de imágenes digitales de color ante distintos procesamientos de imagen digital de carácter intencional y no intencional.

## 1.2 Metodología

Se creará una base de datos utilizando el software MySQL Workbench ©, que posteriormente se conectara con la interfaz del prototipo de software.

Se desarrollará un módulo de administración usando el lenguaje de programación Java y el entorno de desarrollo integrado NetBeans ©, donde el propietario de la imagen digital podrá insertar, eliminar y buscar datos de clientes a los cuales se les ha permitido el uso de la imagen digital. Estos datos corresponden básicamente a: nombre del cliente, su RFC y datos de la institución de adscripción. Una vez que los datos han sido proporcionados, se hará uso de una función de resumen criptográfico del algoritmo "RIPEMD-160" implementada en Java, que almacenará el resultado en un campo adicional dentro de la base de datos.

Se desarrollará un módulo de inserción cuya interfaz gráfica de usuario (GUI) se implementará usando el lenguaje de programación Java en el entorno de desarrollo integrado NetBeans ©, y el algoritmo de marcado de agua será desarrollado en Matlab © para ser consumido a su vez por la GUI de Java. Este moduló marcará imágenes digitales utilizando la información del resumen criptográfico "RIPEMD-160" de la base de datos, que antes de ser insertada dentro de las imágenes será procesada mediante un algoritmo de generación de patrones de marca de agua programado en Matlab ©.

Se desarrollará un módulo de detección en el cual se extraerá la información de marca de agua que contenga una imagen digital protegida y se hará una búsqueda dentro de la base de datos con el propósito de detectar a que cliente fue asignada dicha copia digital.

## 1.3 Hipótesis

Fundamentados en los objetivos y en la metodología, se plantean las siguientes hipótesis cuya veracidad se pretende confirmar durante el desarrollo de este trabajo:

Una primera hipótesis consiste en suponer que la utilización de técnicas de marcas de agua aplicadas en imágenes digitales, las cuales se consideran inseparables del contenido del archivo y han sido propuestas en la literatura como una solución eficiente para la protección de los derechos de copia y propiedad de los archivos de datos multimedia, deberán permitir la identificación del cliente o consumidor autorizado de materiales digitales.

Una segunda hipótesis consiste en suponer que es posible aportar mejoras para la determinación óptima de los parámetros críticos del algoritmo de marca de agua, tales como el factor de fuerza de inserción y la cantidad útil de la marca de agua (número de bits que la componen), utilizando métodos analítico-experimentales para su diseño y desarrollo dentro del algoritmo de marca de agua.

## 1.4 Organización de tesis

En el capítulo 2 se abordará el marco teórico del trabajo propuesto. En el capítulo 3 se mencionará con detalle las 3 etapas del esquema de marcado de agua, las cuales refieren a la generación, inserción y detección de un patrón de marca de agua. En el capítulo 4 se mostrarán los resultados experimentales obtenidos y el trabajo finaliza con el capítulo 5, en donde se exponen las conclusiones y el trabajo futuro en la línea de investigación del marcado de agua para protección de derechos de autor y detección de copias ilegalmente distribuidas.

# Capítulo 2
# Marco Teórico

## Introducción

Actualmente el desarrollo de las tecnologías de la información y comunicación (TIC) permite de manera más sencilla realizar el intercambio de información digital sin tomar en cuenta si se infringen o no los derechos de autor y/o la propiedad intelectual de los autores de multimedia digital, lo que hace compleja la tarea de protección de dichos derechos.

Por esta razón, surge la necesidad de implementar herramientas tecnológicas que permitan proteger el derecho de autor ante usuarios o consumidores no autorizados con el objetivo de demostrar quién es el propietario legítimo del material digital.

Una de estas herramientas tecnológicas es la criptografía, la cual consiste en hacer ilegible la información durante una transmisión de datos desde el emisor hasta el receptor, para entonces finalmente permitir que los datos puedan ser descifrados por el destinatario al cual va dirigido, sin embargo, una vez descifrada la información, esta es totalmente legible y pierde toda protección.

Una técnica complementaria a la criptografía es la denominada marca de agua digital, la cual consiste en insertar información relacionada con el propietario del material digital (video, fotografía, audio, texto), esta puede ser o no perceptible a la vista u oído humanos según sea el caso.

Cuando un trabajo es protegido usando alguna técnica de marca de agua, este puede ser susceptible a distintos ataques intencionales o no intencionales provocando que dicha marca pueda ser o no eliminada.

Otra técnica de ocultamiento de datos en materiales digitales que frecuentemente es confundida y en ocasiones usada de manera incorrecta como sinónimo de la marca de agua digital es la denominada esteganografía, cuyo objetivo principal es ocultar la mayor cantidad de información en un material digital, contrario a la técnica de marca de agua, en la esteganografía lo importante es preservar el mensaje oculto y no necesariamente proteger los derechos de autor del material huésped.

En este capítulo se revisarán los elementos que conforman el marco teórico del presente trabajo, comenzando por la diferencia entre las técnicas criptográficas, de marca de agua digital y esteganografía. Posteriormente, se definirán conceptos propios de la técnica de marca de agua digital y finalmente se revisarán algunos elementos relacionados con las métricas para la evaluación de la robustez e imperceptibilidad del método propuesto.

## 2.1 Esteganografía

Como previamente se introdujo, dentro de la línea de investigación de ocultamiento de datos (*data hiding* en el término inglés), la esteganografía es confundida y en ocasiones usada de manera incorrecta como sinónimo de la marca de agua digital, sin embargo, su propósito principal es ocultar un mensaje con la mayor cantidad de información posible, dentro de algún material digital que sirva como huésped o vehículo, para entonces lograr pasar inadvertido dicho mensaje ante terceras partes, excepto para el destinatario. Al intentar proteger la información ocultando su existencia de la propia comunicación, nadie sabrá que se está mandando un mensaje oculto en el huésped, por lo tanto, este difícilmente podrá ser descubierto.

Una técnica utilizada comúnmente en la esteganografía es la denominada modificación del Bit Menos Significativo LSB (*Least Significant Bit* por sus siglas en inglés) usando imágenes digitales como huésped del mensaje oculto. Un ejemplo ilustrativo de esta técnica consiste en tener 2 imágenes donde una de ellas será la imagen huésped y la otra imagen será el mensaje a ocultar, por razones de carga útil, el mensaje a ocultar deberá ser de menor dimensión que la imagen huésped.

En términos generales, asumiendo que ambas imágenes (huésped y mensaje a ocultar) tienen una resolución de 8 bits por píxel en la escala de grises, tomando un píxel de la imagen "mensaje", este es descompuesto en sus 8 bits que lo componen, y cada bit será insertado reemplazando el bit menos significativo de un píxel de la imagen huésped, por lo tanto, por cada píxel del "mensaje" a ocultar serán necesarios 8 píxeles de la imagen huésped [1]. Finalmente, cuando se ha terminado el proceso de inserción, se genera un clon de la imagen huésped, que es denominado como imagen "Stego". Esto se ejemplifica en la Figura 2.1.

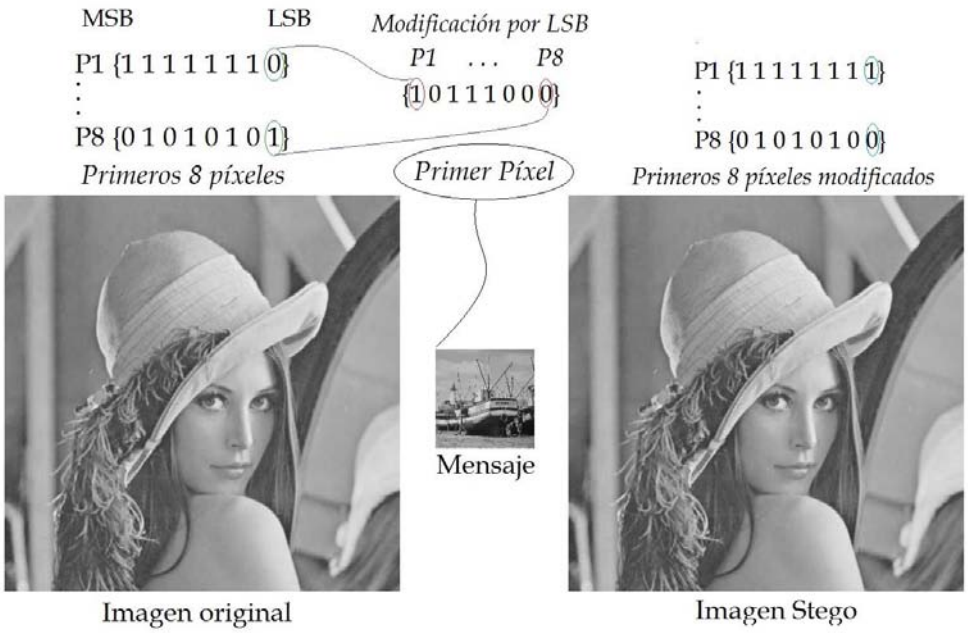



**Figura 2.1 Método de estenografía por modificación del bit menos significativo (LSB)**

## 2.2 Criptografía

La criptografía tiene como objetivo transformar la información para que no sea entendible a simple vista y proteger los datos contra cualquier modificación y comprobar la fuente de los mismos. El cifrado de datos es un proceso para transformar la información, también llamada texto plano, en un criptograma, el cual se caracteriza por ser ininteligible con la finalidad de transmitir un mensaje de forma segura a través de un canal donde la intercepción es posible. Para convertir el criptograma nuevamente en texto plano es necesario realizar el proceso inverso conocido como descifrado. Para realizar el cifrado y descifrado se requiere de una clave que debe ser conocida por el transmisor y el receptor del mensaje. Como se comentó anteriormente, una vez descifrada la información, esta es totalmente legible y pierde toda protección [2]. La Figura 2.2 muestra un esquema general de cifrado y descifrado de datos.

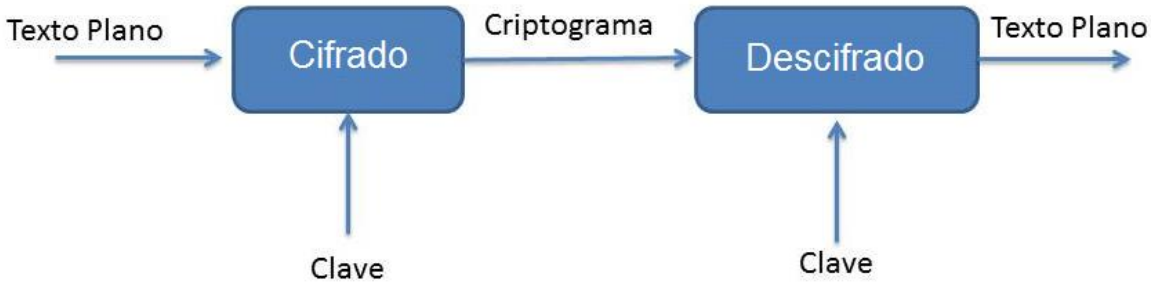
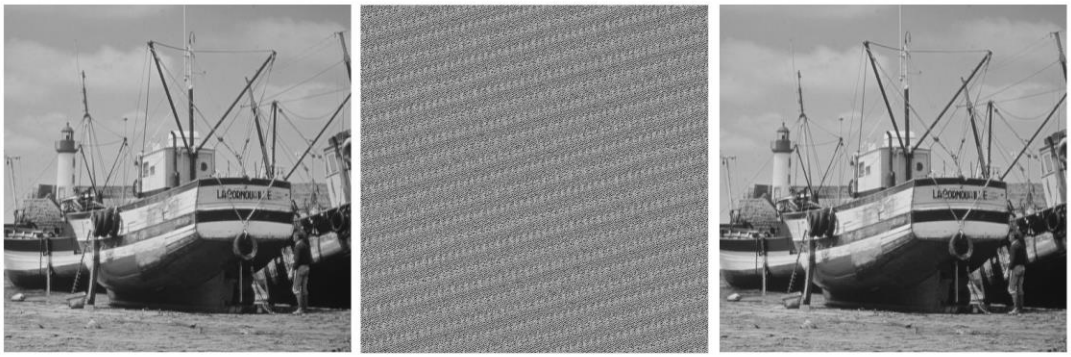



**Figura 2.2 Esquema general de cifrado y descifrado**

Un ejemplo de criptografía visual se puede observar en la Figura 2.3, la cual ilustra la técnica criptográfica basada en mezcla caótica.



(a) (b) (c)

**Figura 2.3 Método de cifrado de datos vía mezcla caótica. (a) Imagen original. (b) Datos cifrados vía algoritmo de mezcla caótica. (c) Imagen obtenida después de aplicar algoritmo de descifrado**

## 2.3 Historia y definición de marca de agua digital

La idea de comunicar secretamente información es tan vieja como la comunicación misma [3]. En la antigüedad se podían observar distintas técnicas del ocultamiento de información por ejemplo, Ovidio en su obra "El arte de amar" sugiere usar leche para escribir de forma invisible [3], otro ejemplo es el código Morse que nace con la idea de mandar mensajes secretos.

Con estos antecedentes surge la marca de agua digital, que es una técnica de ocultación de información usando una señal integrada en datos digitales que puede ser detectada y/o extraída mediante operaciones computacionales para afirmar la autenticidad de un objeto multimedia, el cual puede ser audio, imagen, texto o video.

El proceso de incrustación de una marca de agua digital consiste en la inserción de información en una señal portadora la cual puede tratarse de cualquier elemento digital.

El objetivo principal de insertar información en los contenidos multimedia es la protección de la propiedad intelectual y los derechos de autor. El material marcado puede ser publicado y/o difundido a través de una red de datos, comercializado en copias digitales y/o radio emitido; situaciones en las cuales el material puede sufrir alteraciones intencionales o no intencionales. En cualquier momento se puede realizar el proceso de detección y/o extracción de la marca de agua para demostrar, por ejemplo, la autoría o autenticidad del material. Por lo tanto, de manera general, el sistema de marcado de agua digital consta de una etapa de inserción y una etapa de detección de la marca de agua [2].

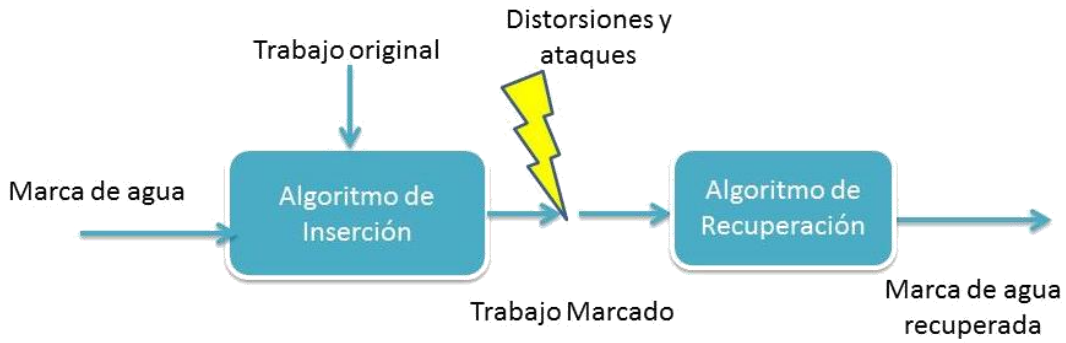



**Figura 2.4 Sistema general de marcado de agua digital**

El sistema de marcado de agua digital es similar a un sistema de comunicaciones donde se tiene un transmisor, un canal de comunicación y un receptor. En este modelo la inserción de la marca de agua en la señal portadora corresponde a la transmisión de la señal, las modificaciones realizadas por ataques y distorsiones al trabajo marcado corresponden a la transmisión a través del canal de comunicaciones y la recuperación de la información escondida es análoga a la recepción [2]. La forma general para insertar una marca de agua dentro de un material digital tiene la forma:

$$I' = I + (\alpha \cdot W) \qquad (2.1)$$

Donde $I$ denota el material original a proteger, $W$ es la marca de agua a incrustar, $\alpha$ es un factor de fuerza con el cual se insertará $W$ y finalmente el material protegido denotado como $I'$.

Al igual que un sistema de comunicaciones se pueden agregar procesos tales como la codificación fuente, codificación de canal, espectro disperso, detección y decodificación [2].

En al ámbito de imágenes digitales, a continuación se detallarán algunos aspectos que refieren con el diseño de un algoritmo de marca de agua digital.

## 2.4 Requerimientos

Los requerimientos básicos que un sistema de marca de agua digital debe contener son:

- **Robustez**.- Una marca de agua se considera robusta si puede resistir modificaciones producidas por los procesamientos intencionales y no intencionales a los cuales están expuestos los archivos multimedia.
- **Imperceptibilidad**.- Se dice que una marca de agua es imperceptible si la degradación causada por la inserción en los archivos multimedia es muy difícil de apreciar.
- **Carga útil**.- La carga útil de una imagen refiere a cuanta información puede contener la marca de agua sin que esta se note.
- **No ambigüedad**. Es la probabilidad que sea o no detectada una marca de agua en una imagen tomando en cuenta la probabilidad del falso negativo y del falso positivo de los cuales se hablara más adelante.

Los requerimientos anteriores deberán ser considerados en menor o mayor grado durante el diseño de un algoritmo de marcado de agua digital, dependiendo de la aplicación y el propósito del mismo.

## 2.5 Marca de agua robusta, frágil y semi-frágil

- **La marca de agua robusta** es aquella que está diseñada para poder sobrevivir a los distintos ataques intencionales o no intencionales, cuyo propósito sea o no eliminar la protección de la propiedad intelectual.
- **La marca de agua frágil** es aquella que está diseñada para la autenticación y verificación de la integridad de una imagen, sin embargo, es susceptible a cualquier ataque.
- **La marca de agua semi-frágil** es utilizada en aplicaciones de autenticación e integridad de datos, sin embargo, solo tolera distorsiones no intencionales como mejoras en la calidad o compresión de datos moderada.

## 2.6 Marca de agua visible e invisible

La marca de agua visible consiste en un patrón perceptible a la vista y se puede usar principalmente para:

- **Marca de agua visible**.- para una mayor protección de los derechos de autor. En tales situaciones, donde las imágenes son publicadas en internet con la intención de realizar una comercialización sin el pago de regalías al autor. El propietario aquí desea una marca de propiedad que es evidente visualmente y al mismo tiempo no impide que la imagen pueda ser usada para otros fines.

Un ejemplo de marcado de agua visible se ilustra en la Figura 2.5.

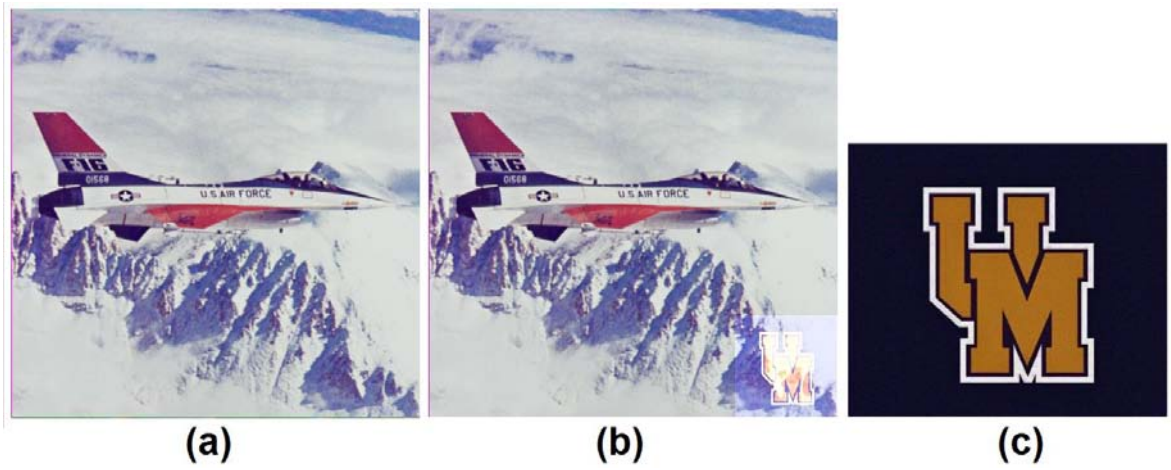



**Figura 2.5 (a) Imagen original, (b) Imagen con marca de agua visible, (c) Marca de agua original**

**La marca de agua invisible** consiste en aplicar las técnicas de marcado en el dominio espacial o bien en un dominio transformado, para realizar la inserción y así obtener una marca de agua imperceptible o invisible.

La marca de agua invisible se puede utilizar en los siguientes casos:

- **Marca de agua invisible**.- para detectar copias de imágenes ilegalmente distribuidas. En este escenario el vendedor o propietario de imágenes digitales está interesado en que las regalías por el uso de la imagen puedan ser pagados individualmente y evitar, por ejemplo, que un individuo pague una licencia de uso y una vez que la imagen se encuentra en su poder, este la ponga a disposición de terceras partes de forma gratuita, privando así al propietario de la imagen de los ingresos económicos por el uso de su imagen digital. En este escenario, las marcas de agua insertadas dentro de cada copia autorizada servirán para poner en evidencia al distribuidor de copias ilegales.

- Marca de agua invisible como prueba de propiedad intelectual. En este escenario, el propietario de las imágenes digitales sospecha que una de sus imágenes ha sido editada y/o publicada sin el pago de regalías. Aquí, la detección de la marca de agua en la imagen está destinada a servir como prueba ante un tribunal para poner en evidencia que la imagen publicada y/o editada es propiedad del dueño de la imagen digital.


**Figura 2.6 (a) Imagen original, (b) Imagen con marca de agua invisible, (c) Marca de agua que consiste en un patrón binario pseudo-aleatorio**

## 2.7 Tipos de detección

- **Detección ciega**.

  No se necesita la imagen original para detectar la marca de agua, esta última puede ser extraída o detectada usando únicamente la versión marcada empleando únicamente el algoritmo de detección/extracción correspondiente. El campo de aplicación para este tipo de algoritmos es más amplio, en particular aplicaciones de autenticación y protección de derechos de autor.

- **Detección no ciega**

  Necesita forzosamente la imagen original para recuperar o detectar la marca de agua insertada. Es muy eficaz para re-sincronizar las etapas de inserción-detección de marca de agua cuando el material protegido ha sido procesado por una distorsión geométrica, sin embargo, en muchos casos, el material digital original no se encuentra disponible, por lo que la aplicación de este tipo de algoritmos es muy limitado.

## 2.8 Dominios de inserción

- **Marca de agua en el dominio espacial**

  Se trata de una técnica que modifica directamente los pixeles que componen la imagen de acuerdo a la información que la marca de agua contiene. Usualmente sólo un subconjunto de la imagen es marcado en este dominio.

- **Marca de agua en el dominio transformado**

  La marca de agua se inserta en los coeficientes de la transformada de la señal o imagen portadora. Usualmente se elige la Transformada Discreta de Coseno (DCT), la Transformada Discreta de Wavelet (DWT), la transformada Contourlet o bien la Transformada Discreta de Fourier (DFT). Comúnmente el dominio transformado proporciona mayor robustez ante procesamientos avanzados de señal así como las distorsiones geométricas.

## 2.9 Aplicaciones de marca de agua digital

Algunas de las principales aplicaciones de marca de agua son:

- **Protección de derechos de autor**. Esta aplicación consiste en construir una marca de agua que contenga información que sea relevante y tenga relación directa con el autor o propietario de la imagen. De esta forma se puede evitar el uso no autorizado del material digital que se desea proteger. Para esta aplicación se requiere una alta robustez contra una gran cantidad de ataques intencionales y no intencionales. Además, es necesario que los esquemas de este tipo utilicen medidas de seguridad complementarias para evitar inserciones no autorizadas en imágenes protegidas [6].

- **Rastreo de copias**. Esta aplicación consiste en insertar una marca de agua diferente a copias de una misma imagen antes de realizar la distribución entre un pequeño grupo de personas. Si alguna de las personas que tienen una de las copias marcadas distribuye la imagen sin autorización, es posible rastrear al responsable detectando la marca de agua de alguna de las copias ilegales.

- **Protección de copias**. En escenarios donde se necesita garantía de seguridad para resguardar sistemas multimedia ante distribuciones no autorizadas. Para garantizar esta medida de seguridad es prudente utilizar marcas de agua dentro de los dispositivos electrónicos, sobre todo en sistemas cerrados o de propietarios. Al insertar esta marca dentro de los datos multimedia, se puede indicar a los reproductores el número de copias autorizadas de un determinado volumen. En estos tipos de esquemas se requiere una robustez contra ataques geométricos, cambio de formato, ruido, etc.

- **Autenticación de imágenes**. Esta aplicación tiene como objetivo el detectar la modificación o alteración en los datos y consiste principalmente en diseñar marcas de agua que se destruyan o modifiquen cuando las imágenes protegidas sufren cualquier tipo de distorsión. Los esquemas diseñados con este propósito son conocidos como esquemas de marca de agua frágil [6].

## 2.10 Tipos de ataques

Una imagen con marca de agua es probable que sea sometida a ciertas manipulaciones o ataques, algunos no intencionales tales como la compresión y la contaminación por ruido durante la trasmisión a través de un canal de comunicaciones, e intencionales tales como las distorsiones geométricas, el filtrado etc. A continuación se muestran los tipos de distorsiones más comunes que puede sufrir una imagen.

- Compresión con pérdida: Muchos esquemas de compresión como JPEG en imagen y MPEG en video, potencialmente pueden degradar su calidad a través de la pérdida irrecuperable de datos.
- Distorsiones geométricas tales como la traslación de píxeles, recorte de imagen, rotación, escalamiento, transformaciones del tipo *affine*, proyectivas, entre otros.
- Operaciones de procesamiento avanzado de señal, incluyen lo siguiente.
  - Conversión Digital / Analógico
  - La conversión Analógico / Digital
  - Cuantización
  - Filtrado lineal tales como paso alta, paso baja, paso banda
  - Filtrado no lineal, como el filtrado de mediana
  - Reducción de color
  - Aumento de contraste
  - Disminución de brillo
  - Corrección gamma
  - Ecualización de histograma
  - Especificación de histograma, entre otros
- Software especializado para evaluar robustez, tales como:
  - Stirmark Benchmark
  - Unzign

En la Figura 2.7 se muestra un concentrado de distorsiones intencionales y no intencionales.

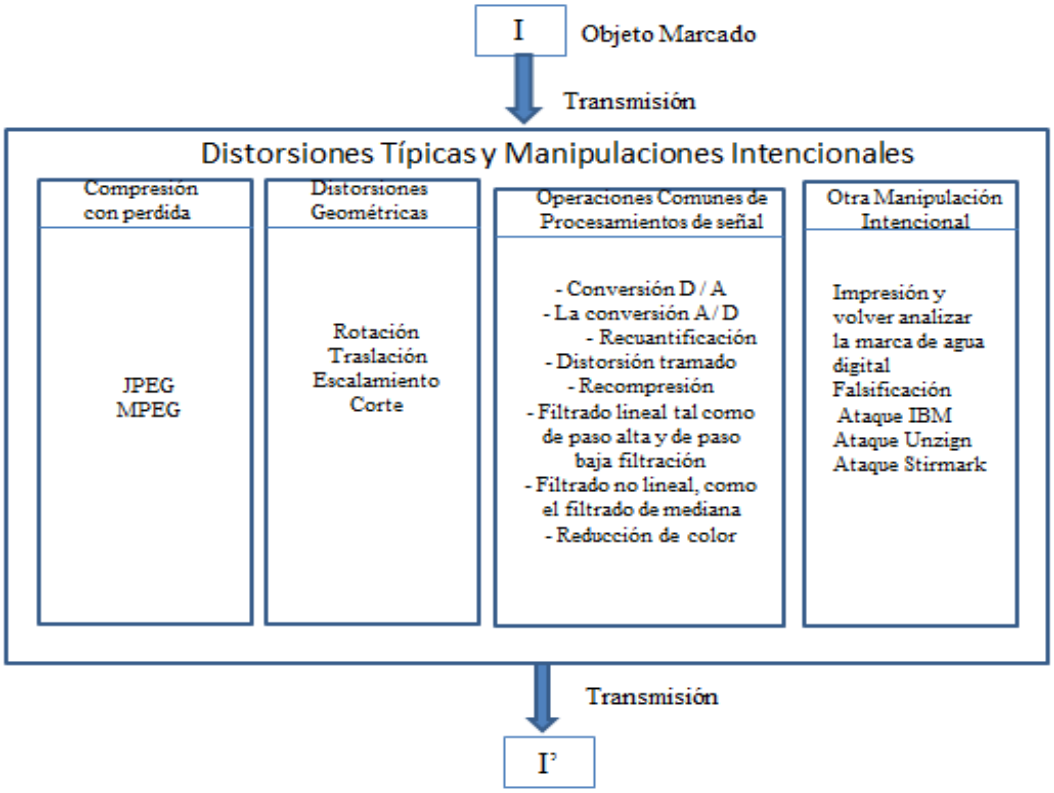



**Fig. 2.7 Ataques en marcas de agua digitales**

## 2.10.1 Distorsiones geométricas

Las distorsiones geométricas tales como la traslación, rotación, escalamiento y recorte son las transformaciones lineales que se ocupan más comúnmente para manipulación de imágenes digitales [6]. Se tiene una imagen cualquiera $f(x,y)$ , donde $x$ e $y$ se encuentran en los intervalos $0<x<N_C$ y $0<y<N_R$ , donde $N_C$ y $N_R$ representan el total de columnas y renglones respectivamente.

Estas distorsiones geométricas están dadas por las siguientes ecuaciones [6]:

$$f_{traslación}(x,y)=f\,(x+x_{0,}\,y+y_0) \tag{2.2}$$

donde $x_0$ , $y_0$ son parámetros de traslación.

$$f_{rotación}(x,y)=f\,(x\cos\theta - ysen\theta, xsen\theta + y\cos\theta) \tag{2.3}$$

donde $\theta$ denota ángulo de rotación

$$f_{escalamiento}(x,y)=\,f\,(sx+sy) \tag{2.4}$$

Donde *s* es un factor de escalamiento.

A estas ecuaciones y a sus posibles composiciones, se les conoce como transformaciones *affines* y se caracterizan por conservar el paralelismo así como el centro de masa de las imágenes. En la Figura 2.8 se ilustran las distorsiones geométricas de traslación, rotación y escalamiento.

## 2.10.2 Procesamientos avanzados de señal

Algunos procesamientos avanzados de señal consisten en:

- **Compresión con pérdida**: Se trata de un procedimiento de codificación de fuente que tiene como principal objetivo representar cierta cantidad de información de una imagen utilizando una menor cantidad de la misma, siendo entonces imposible una reconstrucción exacta de los datos originales.
- **Contraste**: Este proceso consiste en el aumento de luminosidad entre las zonas más obscuras o más claras de una imagen digital.
- **Brillo:** Este proceso consiste en el aumento o disminución entre la zonas más obscuras o claras de la imagen digital pero reduciendo el detalle y el contraste.


**Fig. 2.8 (a) Imagen Original. (b) Imagen trasladada 150 píxeles en cada eje. (c) Imagen rotada 45°. (d) Imagen escala con un factor *s*=0.5**

- **Ruido Gaussiano:** Este proceso consiste en insertar un tipo de ruido que puede ser tratable tanto en el dominio espacial así como en el dominio frecuencial. El nivel de contaminación por este tipo de ruido depende directamente del valor de la varianza.

- **Filtro de Mediana:** Este proceso consiste en reemplazar el valor central de un conjunto de valores existentes en una vecindad para cada pixel de la imagen [7].

- **Filtro Gaussiano:** Este proceso consiste principalmente en remover el ruido de una imagen digital mediante una máscara que considera una distribución de tipo Gaussiana [8], ocasionando que la imagen se emborrone y tenga perdida en sus detalles.
- **Ecualización y especificación del histograma:** Generalmente son procesamientos utilizados para mejorar la calidad de las imágenes [9]. La Figura 2.9 ilustra algunos procesamientos avanzados de señal.

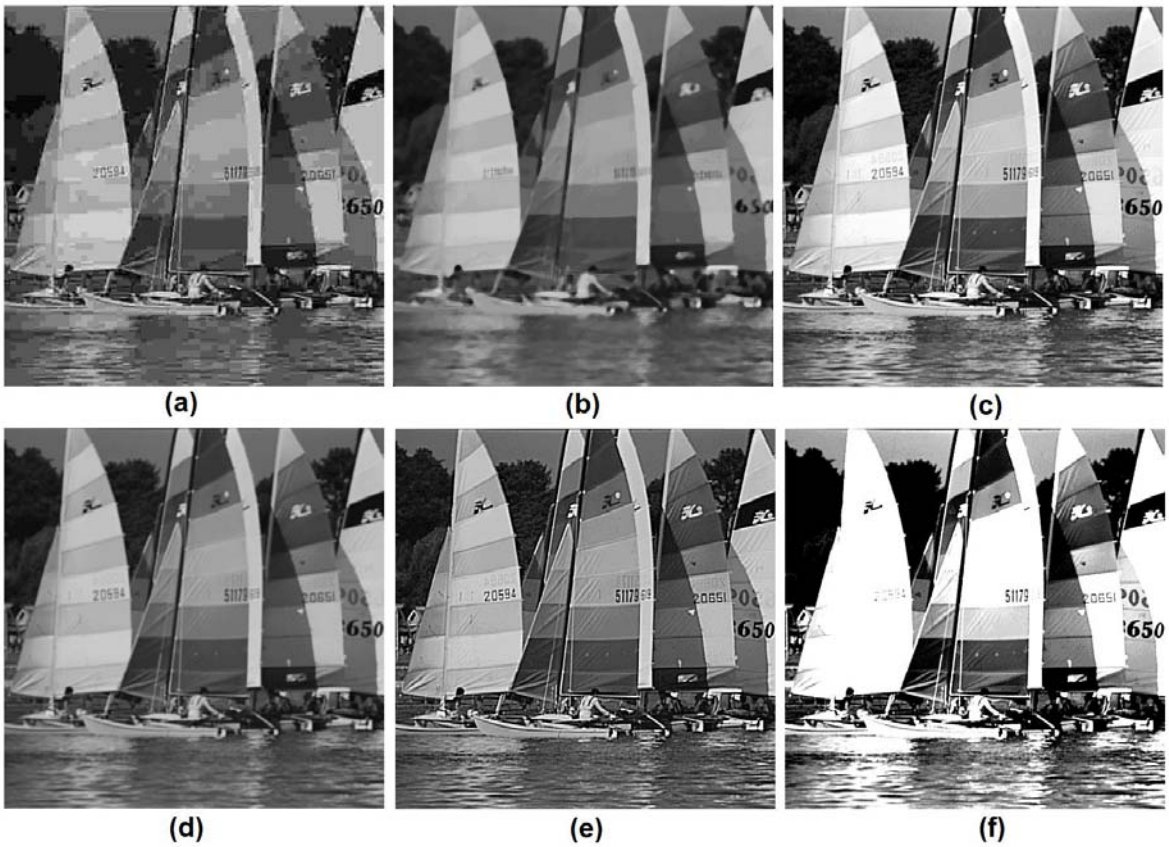



**Fig. 2.9 (a) Compresión JPEG con factor de calidad 5. (b) Filtrado mediano con ventana 7x7. (c) Ecualización de histograma con 64 niveles de cuantización. (d) Filtrado Gaussiano con ventana 7x7. (e) Sharpening y (f) Aumento de contraste**

## 2.11 Evaluación de imperceptibilidad

Para evaluar apropiadamente los métodos de marcado de agua se sugiere que todos se sometan a una evaluación que considere ciertas condiciones equiparables. A continuación se mencionan un par de métricas utilizadas comúnmente para medir el nivel de distorsión provocado en la imagen cuando la marca ha sido insertada dentro de esta.

### 2.11.1 Relación señal a ruido pico (PSNR)

En relación a la imperceptibilidad es práctica común hacer uso de una métrica conocida como Relación Señal a Ruido Pico (*Peak Signal to Noise Ratio* PSNR, por sus siglas en inglés) que mide en decibelios la cantidad de distorsión que sufre una señal al agregarle ruido. En los esquemas de marcado de agua digital, la señal de marca de agua es considerada como ruido que provoca una distorsión en la imagen original. Para definir esta medida en imágenes de color RGB se toma en cuenta la media aritmética del error cuadrático medio (*Mean Square Error* MSE) de las tres componentes [3]. La PSNR para una imagen de color se define como:

$$PSNR(dB) = 10\log_{10}\left(\frac{Valor\ Máximo\ de\ Píxel^{2}}{\left(MSE_{Y} + MSE_{Cb} + MSE_{Cr}\right)/3}\right) \tag{2.5}$$

### 2.11.2 Índice de similitud estructural (SSIM)

El SSIM es una métrica para medir la similitud entre dos imágenes donde se considera la degradación de la imagen como un cambio percibido en los pixeles más significativos visualmente. Un valor de 1 indica que la imagen original y la de referencia son la misma, valores alejados de la unidad y cercanos a 0 indican que ambas imágenes tiene diferencias considerables a simple vista. Está definido por 2.6:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^{\ 2} + \mu_y^{\ 2} + C_1)(\sigma_x^{\ 2} + \sigma_y^{\ 2} + C_2)} \tag{2.6}$$

## 2.11.3 Diferencia de color normalizada (NCD)

La Diferencia de Color Normalizada NCD (por sus siglas en inglés *Normalized Color Difference*) [10], [11], es una medida basada en el espacio de color CIELAB representada por un único número y se utiliza para medir el cambio de color entre dos imágenes, está dada por (2.7):

$$NCD = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left(\sqrt{\left(\left(\Delta L(i,j)^2\right)+\left(\Delta a(i,j)^2\right)+\left(\Delta b(i,j)^2\right)\right)}\right)}{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left(\sqrt{\left(\left(L(i,j)^2\right)+\left(a(i,j)^2\right)+\left(b(i,j)^2\right)\right)}\right)}, \tag{2.7}$$

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

## 2.12 Evaluación de robustez

Para evaluar apropiadamente los sistemas de marcas de agua se sugiere que todos los esquemas de marcas de agua se evalúen bajo condiciones equiparables. Para realizar la evaluación de la robustez de una marca de agua se usan distintas métricas tales como coeficiente de correlación normalizada (NCC), correlación cruzada (CC), tasa de bits erróneos (BER), entre otros.

## 2.12.1 Tasa de bits erróneos (BER)

La tasa de bits erróneos (BER) es una métrica la cual indica el porcentaje de bits que fueron recuperados en el receptor erróneamente con respecto al total de bits enviados durante una transmisión de datos. Un valor igual a 0 indica que todos los bits fueron

recuperados correctamente, por otra parte, un valor de 1 indica que todos los bits fueron recuperados de forma errónea. La BER está dada por (2.8):

$$BER = \frac{Bits\ Erroneos}{Número\ Total\ de\ Bits} \tag{2.8}$$

Un ejemplo acerca de la aplicación de esta métrica se ilustra en la figura 2.10.

$$Secuencia\ Transmitida: \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1$$
$$Secuencia\ en\ el\ receptor: 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1$$
$$BER = 2/8 = 0.25 = 25\%\ de\ bits\ recibidos\ con\ error$$

**Fig. 2.10 Ejemplo de tasa de bits erróneos**

## 2.12.2 Probabilidad de falso positivo y falso negativo

En el ámbito del marcado de agua digital, la probabilidad de falso positivo se refiere a la probabilidad de no detectar una marca de agua en una imagen digital cuando en realidad la imagen está protegida y contiene la marca de agua.

Por su parte, la probabilidad de falso negativo se refiere a la probabilidad de considerar una imagen como autentica o que contiene una marca de agua digital, cuando en realidad está no está protegida y no contiene marca de agua alguna.

En el capítulo 3 se mostrará con mayor detalle la estimación de estas probabilidades.

# Capítulo 3
# Algoritmo de marca de agua propuesto

## Introducción

Durante los últimos años, las tecnologías de imagen digital, vídeo y audio, han sido ampliamente utilizadas dentro de la infraestructura de tecnologías de la información y comunicación, permitiendo que los datos multimedia puedan ser copiados y distribuidos fácilmente sin ningún tipo de control. Este hecho sugiere la necesidad de desarrollar métodos informáticos eficientes para resolver problemas relacionados con los derechos de autor del titular de los datos multimedia. La marca de agua digital se considera como una solución adecuada para la autenticación y la protección de los derechos de autor de datos digitales [12].

Con el fin de detectar el origen de copias ilegales, el propietario de la imagen digital puede utilizar la técnica de marca de agua digital como herramienta tecnológica complementaria durante un proceso legal. En este contexto, el propietario puede integrar diferentes marcas de agua relacionadas con la identidad del usuario en cada una de las copias de imágenes digitales que se suministran a los distintos consumidores, permitiendo que el esquema de marcado de agua pueda identificar que clientes han infringido su contrato de licencia, al proporcionar copias ilegitimas a terceras partes.

En la Figura 3.1 se muestra un diagrama general del método de marca de agua propuesto, el cual involucra diferentes etapas como lo son la generación, inserción y detección de la marca de agua digital. Los detalles de cada uno de los elementos que componen el diagrama serán explicados con detalle a lo largo de este capítulo.

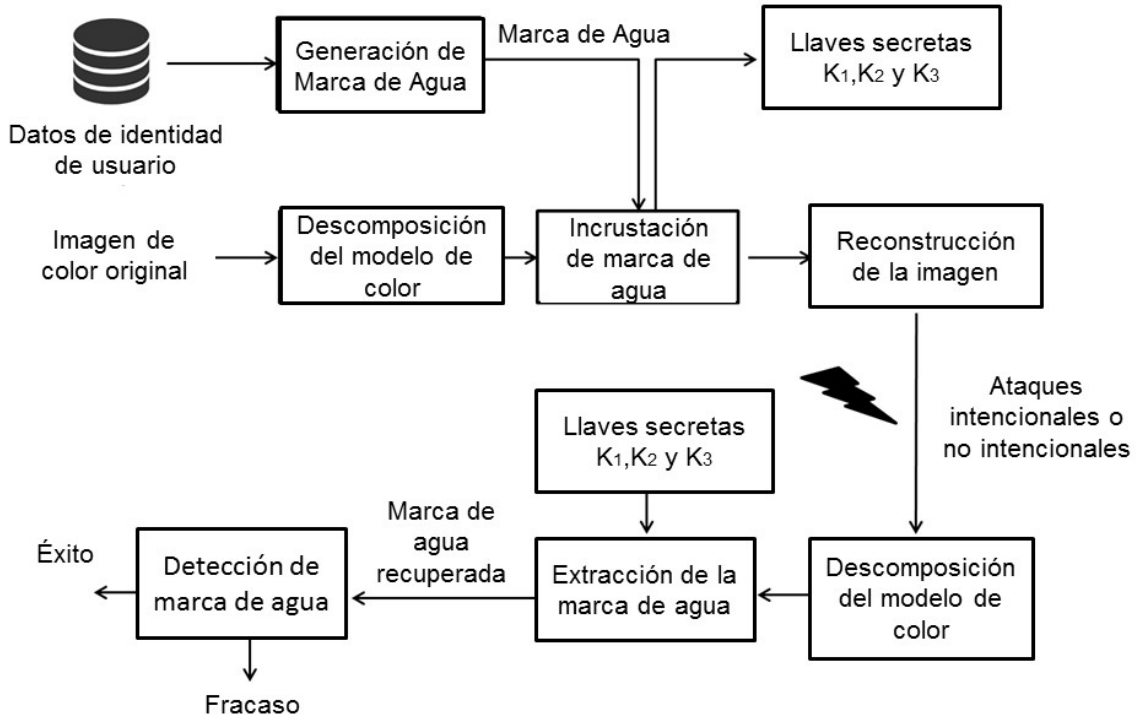



**Figura 3.1.** Diagrama general del método propuesto de marcado de agua

## 3.1 Algoritmo de resúmenes criptográficos RIPEMD-160

Uno de los elementos del método de marca de agua que incorpora mayor seguridad es el uso del algoritmo de resúmenes criptográficos denominado RIPEMD-160.

Las funciones hash son funciones que mapean cadenas de bits de un tamaño arbitrario a cadenas de tamaño fijo. Una función hash de un solo sentido debe satisfacer las siguientes propiedades:

**Resistencia pre-imagen**: es computacionalmente inviable encontrar alguna entrada en la cual los hashes pre-especifiquen cualquier salida.

**Segunda resistencia pre-imagen**: no es computacionalmente viable encontrar alguna segunda entrada la cual tenga la misma salida como alguna entrada especificada.

Para una función hash unidireccional ideal, con un resultado de *m*-bit, la búsqueda de una pre-imagen o una segunda pre-imagen requiere aproximadamente $2^m$ operaciones. Una función hash resistente a colisiones es una función hash unidireccional que satisface una condición adicional:

**Resistencia a colisiones**: refiere a que debe ser computacionalmente inviable encontrar una colisión, es decir, dos distintas entradas que produzcan el mismo resumen criptográfico.

Para una función hash ideal con un resultado de *m*-bit resistente a colisiones, la vía más rápida para encontrar una colisión es haciendo uso de ataques tipo *square root* o de tipo *birthday*, las cuales necesitan aproximadamente $2^{m/2}$ operaciones [19].

Los primeros algoritmos de funciones hash estaban basados en cifrado de bloque (tales como el DES)[20][21][22]. Aunque en principio se tenía bastante confianza en la seguridad de estos algoritmos, su rendimiento no era del todo bueno, ya que eran típicamente de 2 a 4 veces más lentos que el correspondiente cifrado por bloques. Las funciones hash basadas en aritmética modular son también bastante lentos, y existen serias dudas en su seguridad.

Las funciones hash más populares, las cuales son actualmente usadas en una gran variedad de aplicaciones, corresponden a las de diseño personalizado de la familia MD4. MD4 fue

propuesto en 1990 por R. Rivest [23,24]; el cual es un algoritmo bastante rápido y trabaja con procesadores de 32-bit. Sin embargo, debido a una vulnerabilidad inesperada identificada en [23], R. Rivest diseño en el año de 1991 una versión más robusta de MD4, llamada MD5 [24]. MD5 es probablemente la función hash de mayor uso a pesar de que se menciona en [13] que la función de compresión de MD5 no es resistente a colisiones: la colisión encontrada cambia las variables de concatenación en vez del bloque de mensaje. Esto no representa una amenaza para aplicaciones estándar de MD5, pero implica una violación a uno de los principios de diseño. El consorcio RIPE tuvo como objetivo principal crear un portafolio de primitivas de integridad [26]. Basados en la evaluación independiente de MD4 y MD5 [17][18], el consorcio propuso una versión mejorada de MD4, a la cual llamaron RIPEMD.

RIPEMD es usado en aplicaciones bancarias y fue, junto con SHA-1, considerado en el año de 1996 como candidato para ser estandarizado en la norma ISO/IEC JTC1/SC27. Sin embargo, por aspectos de mejoras en seguridad, para entonces considerar el esquema dentro de la estandarización, los autores de RIPEMD diseñaron una versión mejorada denominada RIPEMD-160 la cual desde 1996 se esperaba que fuera segura por 10 años o más. Hasta la fecha no se ha reportado alguna colisión detectada para RIPEMD-160.

En términos generales, el tamaño en bits del resumen criptográfico y la variable de concatenación para RIPEMD-160 fue incrementado a 160 bits, es decir, 5 palabras de 32 bits, el número de rondas fue incrementado de tres a cinco y algunos aspectos en términos de funciones Booleanas y el orden de las palabras de mensaje fueron implementados en dicho algoritmo. Un ejemplo de salida del algoritmo RIPEMD-160 se muestra en la Figura 3.2.

RIPEMD-160:

```
""
9c1185a5c5e9fc54612808977ee8f548b2258d31
"a"
0bdc9d2d256b3ee9daae347be6f4dc835a467ffe
"abc"
8eb208f7e05d987a9b044a8e98c6b087f15a0bfc
"message digest"
5d0689ef49d2fae572b881b123a85ffa21595f36
"abcdefghijklmnopqrstuvwxyz"
f71c27109c692c1b56bbdceb5b9d2865b3708dbc
"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"
12a053384a9c0c88e405a06c27dcf49ada62eb2b
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"
b0e20b6e3116640286ed3a87a5713079b21f5189
8 times "1234567890"
9b752e45573d4b39f4dbd3323cab82bf63326bfb
1 million times "a"
52783243c1697bdbe16d37f97f68f08325dc1528
```

**Figura 3.2.** Valores de prueba y los correspondientes resúmenes criptográficos usando RIPEMD-160

## 3.2 Generación de marca de agua

A continuación se describe paso a paso el proceso de generación de marca de agua:

1. El primer paso consiste en registrar dentro de una base de datos el nombre del cliente o consumidor, su Registro Federal de Contribuyentes (RFC) y su afiliación o institución de adscripción. Posteriormente, dada la información anterior aplicar el algoritmo de resumen criptográfico RIPEMD-160 a dichos datos. El resumen es almacenado dentro de un campo en la base de datos y para este proceso es denotado como *MD*.

2. La representación original de *MD* se encuentra en código hexadecimal. Dicha representación es convertida del sistema base 16 a base 2.
3. Posteriormente, una vez obtenida la representación binaria de MD, este es dividido en dos bloques de 80 bits cada uno y se aplica una operación XOR entre ambos bloques de la siguiente forma:

$$Wm = bck_k \oplus bck_l \tag{3.1}$$

donde $m$ y $k$ = 1. . . 80 y $l$ = 81. . . 160, *bck* denota el $k$-ésimo y el $l$-ésimo bit de cada bloque respectivamente, y $W$ corresponde al resultado de la operación XOR.

4. Por su cálculo los 80 bits resultantes son directamente dependientes de los datos de identidad del cliente. Con el fin de preservar el compromiso entre los requerimientos de carga útil-robustez-imperceptibilidad, la carga útil $L$ del patrón de marca de agua unidimensional $W$ es ajustado de $L$=80 a $L$=64 bits. Este ajuste en la carga útil no afecta el rendimiento del algoritmo de marcado de agua [3].

## 3.3 Inserción de marca de agua

En este trabajo de tesis se presenta un método de marcado de agua híbrido, robusto e imperceptible aplicado a imágenes digitales de color con el objetivo de detectar copias ilegales, mediante la autenticación del cliente o usuario a quien se le proporciona una copia de la imagen original. La adopción de una estrategia de marcado híbrido, robusto e imperceptible obedece al propósito de mejorar principalmente la robustez frente a una gran variedad de distorsiones intencionales o no intencionales, considerando gran parte de los diferentes tipos de procesamiento avanzado de señal y distorsiones geométricas comunes en el ámbito de procesamiento de imágenes digitales. En este contexto, el propietario de la imagen original puede integrar diferentes marcas de agua relacionadas con la identidad del

cliente dentro de cada una de las copias digitales de las imágenes que se suministran a los diferentes usuarios.

El proceso de inserción de marca de agua dentro de la imagen se realizó mediante dos métodos, uno en el dominio espacial y otro en el dominio de la frecuencia. Lo anterior, por un lado, para incrementar la robustez ante los ataques geométricos mediante la inserción en un histograma bidimensional que contiene información del dominio espacial, por otra parte, para hacer frente a los ataques de procesamiento avanzado de señal tales como la compresión JPEG, el filtrado, ecualización de histograma, etc., así como ante algunos ataques geométricos de tipo RST, se hace uso de la inserción en el dominio de la frecuencia. En la literatura, diversos aportes están relacionados con marcado de agua resistente a distorsión geométrica. En principio, podemos encontrar algoritmos basados en dominios invariantes tales como Fourier–Mellin [31,32], dominio log polar [33], dominio de la transformada Radon [34], momentos geométricos [35,36] y momentos de Zernike [37], los cuales han sido usados para insertar marcas de agua y mantener al mismo tiempo la sincronización del método ante distorsión geométrica. Estos métodos han demostrado robustez ante distorsiones de tipo escalamiento y rotación, debido a que utilizan un dominio con características invariantes a distorsiones geométricas, sin embargo, típicamente suelen ser altamente vulnerables ante ataques de tipo recorte y otras transformaciones aún más agresivas como lo son las de tipo *affine* y proyectivas. Por otro lado, muchos de los algoritmos antes mencionados han sido diseñados para implementarse en imágenes de escala de grises y su aplicación en imagen de color puede ser inadecuada si se toma en cuenta que originalmente fueron diseñados para trabajar con un solo canal de color individual [38].

En este sentido, diversos métodos de marcado de agua para imágenes de color han sido propuestos en la literatura, algunos de ellos basados en el dominio de la frecuencia [40–42] y modificación de histograma [43–49]. De este modo, debido a que el histograma de una imagen es considerado en la literatura como un dominio invariante geométricamente, un camino para insertar un patrón de marca de agua dentro de una imagen de color es haciendo

uso de su histograma de color. Si la marca de agua puede ser insertada en este dominio, entonces está podrá sobrevivir a muchas distorsiones geométricas.

Los autores del trabajo publicado en [43] hacen uso de una especificación exacta de histograma para insertar la marca de agua dentro de imágenes de color. Por su parte, en [44], el método de especificación de histograma propuesto previamente por Coltuc y Bolon en [43] es extendido a histogramas con información cromática y la secuencia de marca de agua se inserta dentro del plano cromático de una imagen de color. Los autores del trabajo en [45] proponen un método que inserta una marca de agua dentro de un histograma de color usando la métrica restringida *Earth Mover Distance* (EMD) para optimizar la modificación de la imagen, de acuerdo a un histograma dado. En [46], los autores segmentan y modifican un espacio característico tridimensional compuesto por un histograma en 3D, con el objetivo de insertar el patrón de marca de agua. En [47], los autores proponen un algoritmo de marcado de agua basado en agrupación de histograma, donde se introducen canales tolerantes a fallos para reducir y eliminar la perturbación causada por los ataques geométricos. En [48], se propone un esquema de marca de agua reversible, el cual está basado en modificación de histogramas 1D.

Casi todos los trabajos previos mencionados con anterioridad muestran una gran robustez ante ataques geométricos, sin embargo, la mayoría no provee suficiente robustez ante procesamientos avanzados de señal tales como el filtrado, contaminación por ruido y compresión de imagen así como distorsiones combinadas que involucran algún ataque geométrico así como algún procesamiento avanzado de señal. Para incrementar la robustez sin afectar el requerimiento de imperceptibilidad, una línea de investigación promisoria consiste en el desarrollo de algoritmos de marcado de agua híbridos, los cuales combinan la información espacial y de color de una imagen digital [38].

En este sentido, los autores del trabajo en [49] proponen un método de marca de agua híbrido con propósitos de autenticación. Debido a la diferente naturaleza que origina los

procesamientos de señal avanzados y los ataques geométricos, dos diferentes marcas de agua son insertadas dentro de ese algoritmo. La primera es insertada dentro del dominio de la transformada discreta de coseno (DCT) combinado con una función caótica.

La segunda marca de agua es insertada en una modificación de un histograma en 1D de la imagen. Este método de marca de agua híbrido combina la robustez que tiene el dominio DCT-caótico ante filtrado, ruido y compresión, con la robustez del dominio del histograma 1D ante distorsiones geométricas. El método muestra la robustez de la marca de agua ante distorsión geométrica, procesamiento avanzado de señal y filtrado artístico aplicado con el software comercial Photoshop®. Sin embargo, muestra vulnerabilidad ante ataques de tipo recorte de imagen, y ataques combinados que involucran esta distorsión geométrica. En las siguientes secciones se hará una descripción detallada del algoritmo propuesto en esta tesis.

## 3.3.1 Inserción de marca de agua en el dominio transformado

### 3.3.1.1 Transformada Discreta de Fourier (DFT) bidimensional

La transformada discreta de Fourier de una función bidimensional *f(x, y)* de tamaño *M*x*N* está dada por (3.2):

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) e^{-j2\pi(ux/M+vy/N)} \qquad (3.2)$$

Para $x$=0, 1,2,…, $M$-1, $y$=0, 1,2…,$N$-1

De manera similar, dada *F (u, v)*, obtenemos *f(x, y)* vía la transformada discreta de Fourier inversa dada por (3.3):

$$f(x,y)=\frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}F(u,v)e^{j2\pi(ux/M+vy/N)} \tag{3.3}$$

Para $u$=0,1,2,…, $M$-1, $v$=0,1,2…, $N$-1. Las ecuaciones (3.2) y (3.3) comprenden el par de transformadas discretas de Fourier bi-dimensionales (DFT) [1].

Las variables $u$, $v$ son las variables de la transformada o de frecuencia, mientras que $x$, $y$ son las variables espaciales o coordenadas de los píxeles de la imagen.

### 3.3.1.2 Propiedad de traslación de la DFT bidimensional

Se tiene que $M(u,v)=|F(u,v)|$ es la magnitud de la DFT y $P(u,v)$ es la fase. La traslación en el dominio espacial está dada por (3.4):

$$f(x-x_0,y-y_0)\Leftrightarrow F(u,v)e^{-j2\pi(\frac{ux_0}{M}+\frac{vy_0}{N})} \tag{3.4}$$

Entonces, la traslación en el dominio espacial no afecta la magnitud de la transformada discreta de Fourier, dado que:

$$|DFT[f(x-x_0,y-y_0)]|\Leftrightarrow M(u,v) \tag{3.5}$$

La propiedad de traslación se ilustra en la Figura 3.3.

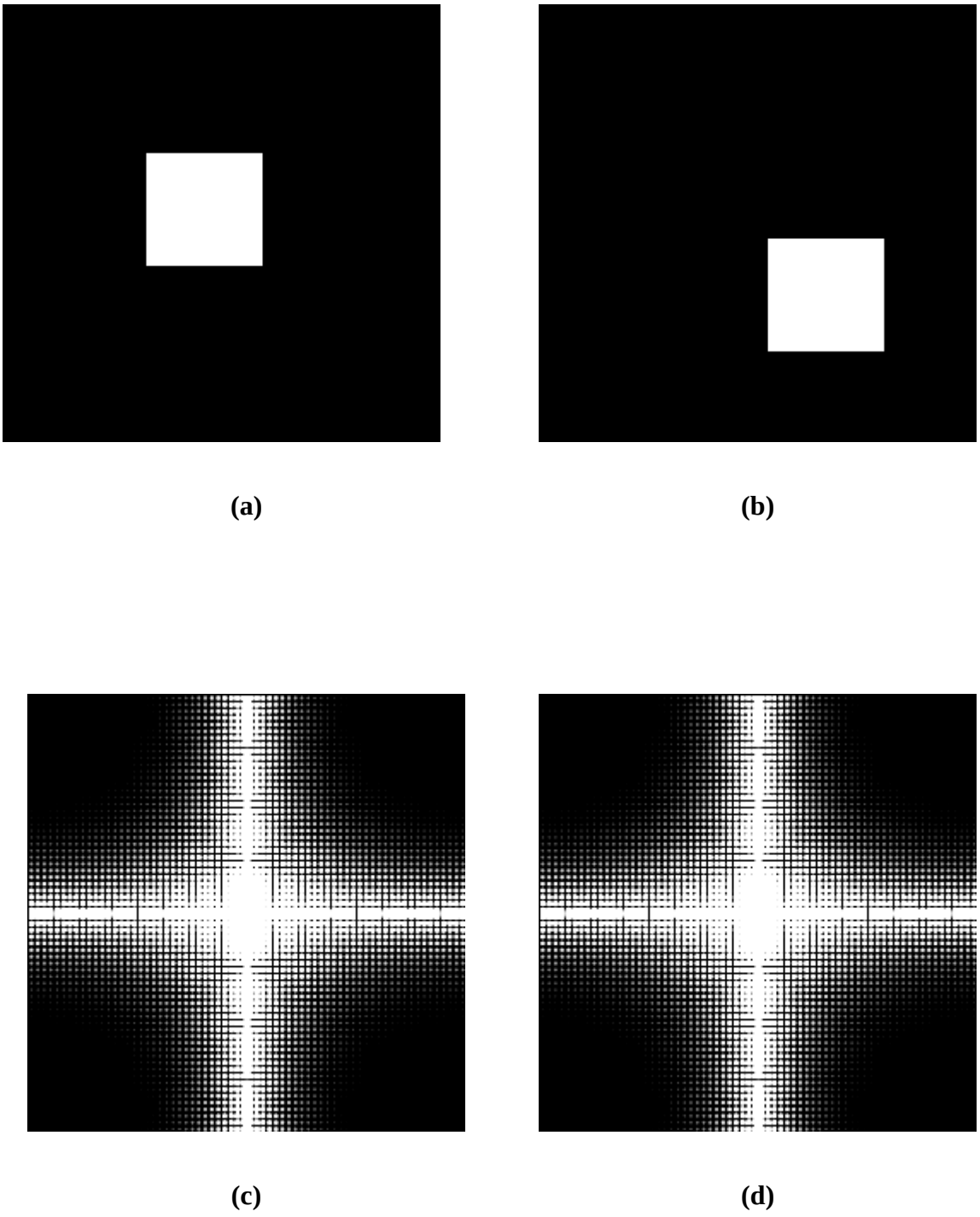



**Figura 3.3.** (a) Imagen original. (b) Imagen trasladada en los ejes $x$=$y$=50. (c) Magnitud de Fourier obtenida de (a). (d) Magnitud de Fourier obtenida de (b)

### 3.3.1.3 Propiedad de rotación de la DFT bidimensional

Está propiedad refiere a que si una imagen es rotada con un ángulo $\theta$, los coeficientes de la transformada bidimensional DFT 2D se rotan con el mismo ángulo $\theta$, como se muestra en (3.6):

$$DFT[f(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)] = F(u\cos\theta - v\sin\theta, u\sin\theta + v\cos\theta) \quad (3.6)$$

La propiedad de rotación se ilustra en la Figura 3.4.

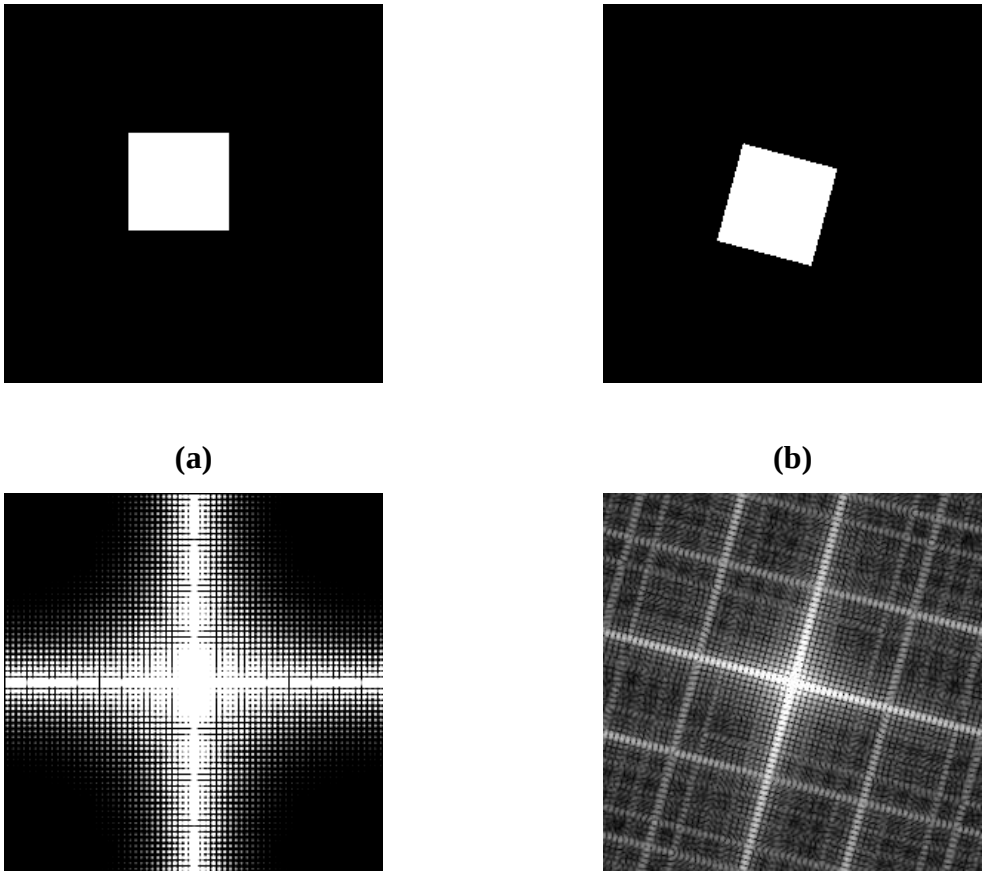



**Figura 3.4.** (a) Imagen original. (b) Imagen rotada 75°. (c) Magnitud de Fourier obtenida de (a). (d) Magnitud de Fourier obtenida de (b)

### 3.3.1.4 Propiedad de escalamiento de la DFT bidimensional

La propiedad de escalamiento de la DFT bidimensional indica que un escalamiento en el dominio espacial, produce un escalamiento inverso en el dominio de la frecuencia. Lo anterior está dado por (3.7):

$$DFT[f(sx,sy)] = \frac{1}{s}F(\frac{u}{s},\frac{v}{s}) \tag{3.7}$$

La ilustración de esta propiedad se muestra en la Figura 3.5 para un escalamiento menor a 1 y en la Figura 3.6 para un escalamiento mayor a 1.

### 3.3.1.5 Inserción en la DFT bidimensional

La magnitud $M(u,v)$ de la DFT bidimensional posee tres propiedades geométricas las cuales son la rotación, el escalamiento y la traslación (*RST* por sus siglas en inglés). Sin embargo, utilizar únicamente esta transformación como dominio de inserción, no brindaría al método de marcado de agua robustez ante otras transformaciones geométricas como lo son las denominadas *affines* y proyectivas. Esta es la razón por la cual el diseño del método es denominado de tipo *híbrido*, porque considera como dominio complementario el histograma bidimensional de la imagen digital. Por otra parte, hacer uso de la DFT dota al método de robustez además de los ataques de tipo *RST*, ante una gran variedad de procesamientos de señal avanzado, como lo es la compresión con pérdida JPEG, el filtrado de imagen, la contaminación por ruido Gaussiano e impulsivo del tipo sal-pimienta, entre otros. Para llevar a cabo el método de inserción de marca de agua en el dominio de la frecuencia se siguieron los siguientes pasos:

1.- Dada la imagen original *I(x, y)*, está es convertida de su representación en el modelo de color RGB al espacio de color YCbCr. Posteriormente, se aíslan las tres componentes respectivamente.

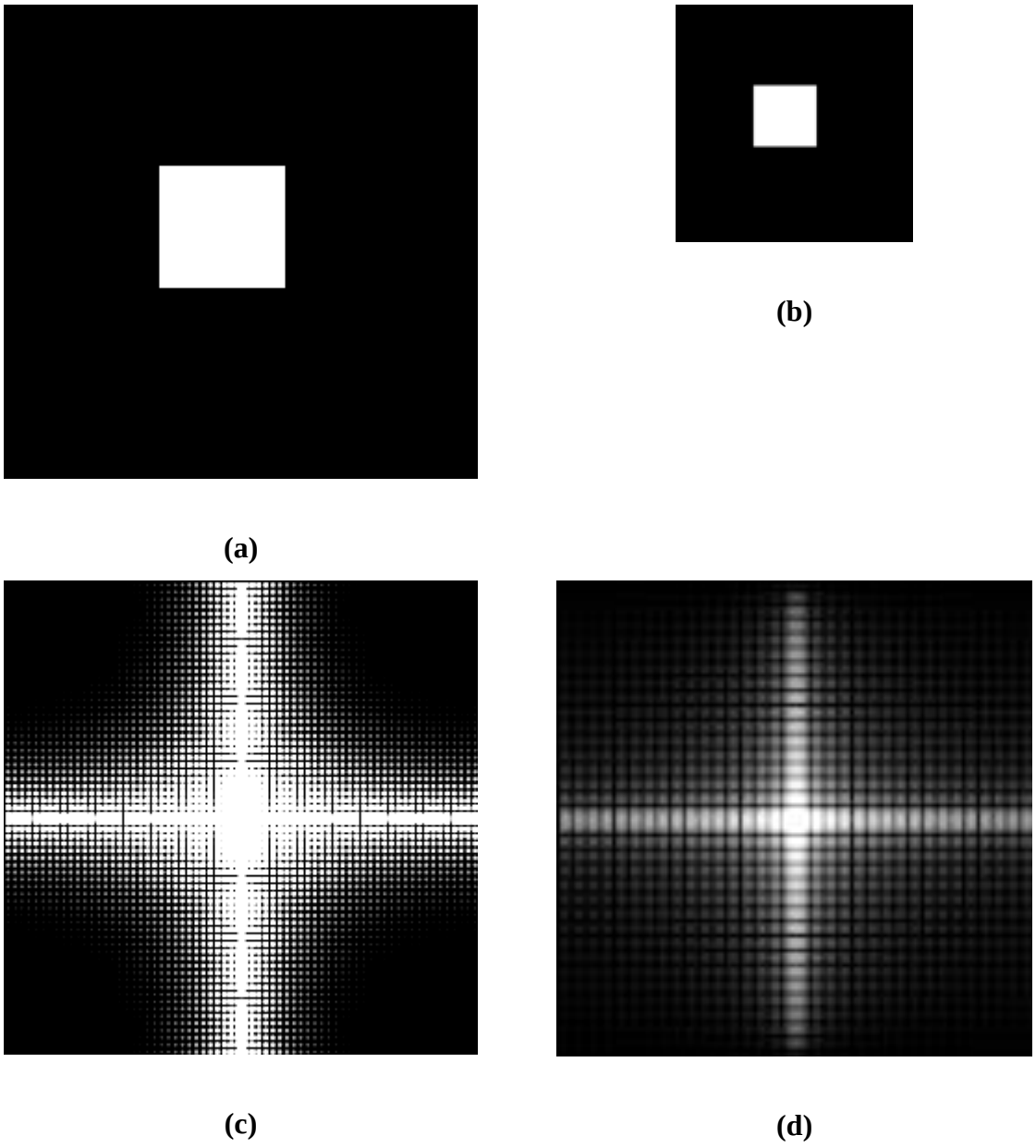



**Figura 3.5.** (a) Imagen original. (b) Imagen re-escalada con un factor de escala de 0.5. (c) Magnitud de Fourier obtenida de (a). (d) Magnitud de Fourier obtenida de (b)

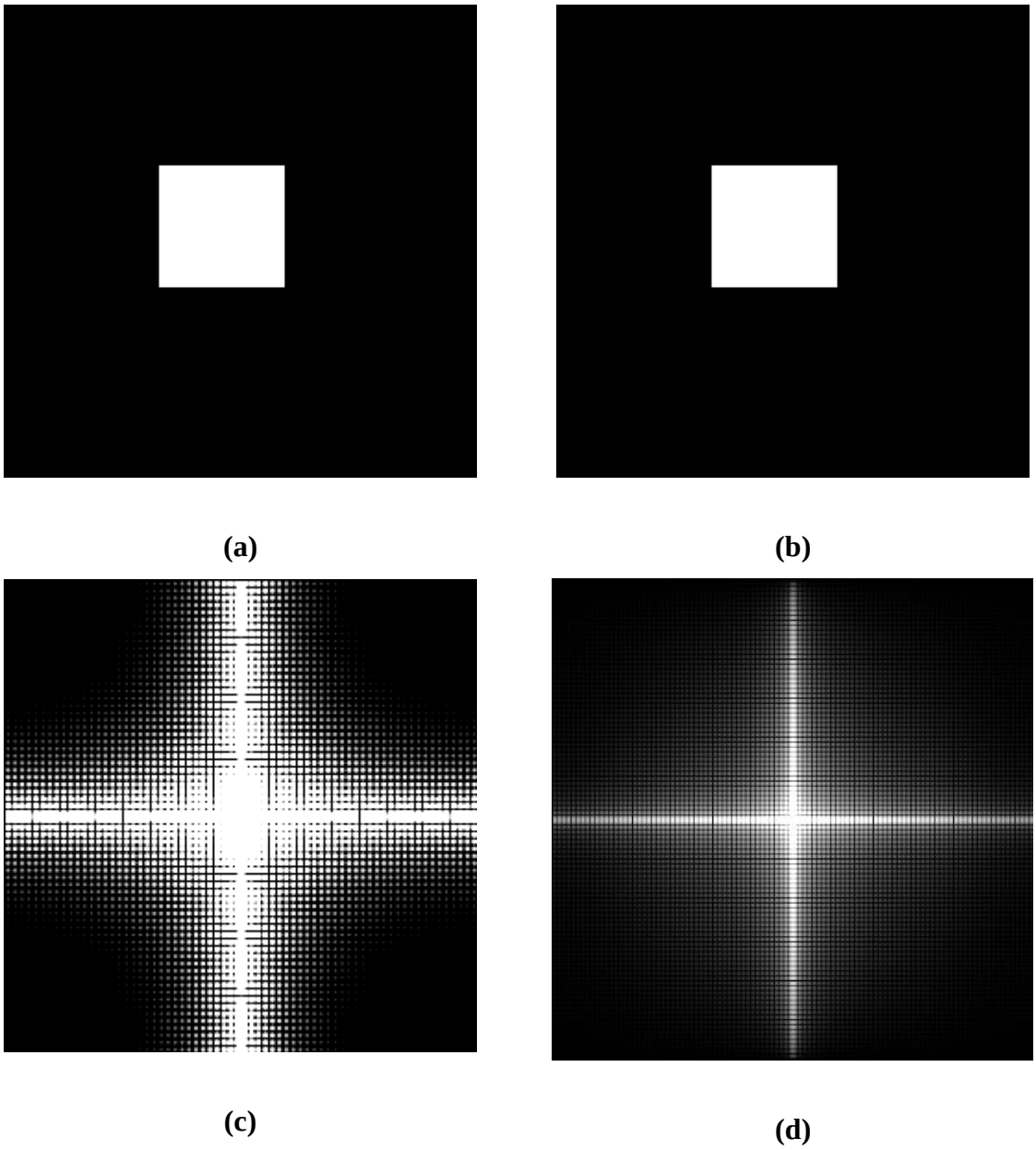



**Figura 3.6.** (a) Imagen original. (b) Imagen re-escalada con un factor de escala de 1.5. (c) Magnitud de Fourier obtenida de (a). (d) Magnitud de Fourier obtenida de (b)

La razón por la cual se adoptó el modelo de color YCbCr para insertar la marca de agua es: si se hace uso de un modelo de color correlacionado como lo es el RGB, la modificación de una componente independientemente de las otras quizás no sea la mejor elección, esto porque los colores percibidos dentro de una imagen digital son dependientes de las tres componentes juntas en RGB. En cambio, el modelo YCbCr permite obtener componentes no correlacionadas y tiene la ventaja de poder separar la información de luminancia de la información de crominancia [38].

2.- Ajustar las dimensiones de la componente de luminancia $Y$ a un tamaño de $N_1xN_2$. Estas dimensiones se almacenaran y se consideraran como una clave secreta $K_1$ en la etapa de detección. La componente escalada se denota como $Y_r\ (x,y)$.

3.- Aplicar la DFT bidimensional $F(u,v)$ a la componente $Y_r(x,y)$ y obtener las componentes de magnitud $M(u,v)=|F(u,v)|$ y fase $P(u\ v)$.

4.- Una vez obtenida la magnitud $M(u,v)$ y esta ha sido previamente centrada mediante (3.8):

$$f(x,y)(-1)^{x+y} \tag{3.8}$$

Basados en la distribución de la energía dentro de $M(u,v)$, seleccionar un par de radios $r_1$, $r_2$ alrededor del término de frecuencia cero en $M(u,v)$ y calcular su respectiva región anular $A=\pi\ (r_2^2-r_1^2)$ la cual debe cubrir la banda de frecuencias medias.

Con el fin de preservar la robustez con respecto a la compresión con pérdida JPEG y al mismo tiempo mantener una alta imperceptibilidad [37], [39], el objetivo entonces será encontrar el par correcto de radios $r_1$, $r_2$. Estos valores serán proporcionados como clave secreta $K_2$ en la etapa de detección.

5.- De acuerdo a la propiedad de simetría de la DFT, se consideran los cuadrantes 1 y 2 de la parte media alta de $M(u,v)$ y calcular la diferencia de magnitud entre los coeficientes de cada uno de los cuadrantes, como se muestra en (3.9):

$$d = M_i(u_j, v_j) - M_i(-u_j.v_j) \quad , \quad (3.9)$$

dentro del área anular $A$, donde $i=1,\ldots, L$ denota un índice que apunta a cada bit de marca de aguas $W_i$, y $j$ denota las coordenadas dentro de $M(u,v)$.

6.- Considerando un factor de fuerza de inserción de marca de agua denotado como $\alpha$, modificar los coeficientes de frecuencia media $M'(u,v)$ como se muestra en las Figuras 3.7 y 3.8. La Figura 3.7 muestra el pseudocódigo correspondiente a las reglas de inserción de marcado de agua, cuando el $i$-ésimo bit de marca de agua $W_i=0$ y $W_i=1$ respectivamente.

$$\begin{aligned}
&SI \quad (W_i = 0)\ \&\ (d \geq -\alpha)\ ENTONCES \\
&\quad M_i^{'}(u_j, v_j) = M_i(u_j, v_j) - (\alpha + d) \\
&\quad M_i^{'}(-u_j, v_j) = M_i(-u_j, v_j) + (\alpha + d) \\
&FIN\ SI
\end{aligned}$$

$$\begin{aligned}
&SI \quad (W_i = 1)\ \&\ (d \leq \alpha)\ ENTONCES \\
&\quad M_i^{'}(u_j, v_j) = M_i(u_j, v_j) + (\alpha - d) \\
&\quad M_i^{'}(-u_j, v_j) = M_i(-u_j, v_j) - (\alpha - d) \\
&FIN\ SI
\end{aligned}$$

**Figura 3.7.** Pseudo-código de las reglas de inserción en el dominio de la frecuencia.

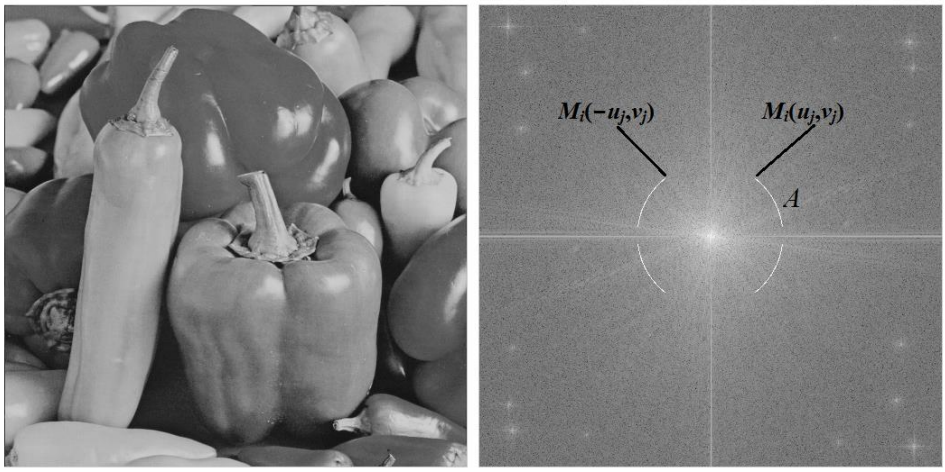



**Figura 3.8.** Ilustración de la modificación en el dominio de la frecuencia. a) componente de luminancia *Y* de la imagen de color original. b) Magnitud de la DFT con marca de agua, obtenida de la imagen a). Para fines ilustrativos se utiliza un valor muy grande del factor de fuerza de inserción de marca de agua $\alpha$.

7.- Para producir valores reales una vez que la magnitud de la DFT ha sido modificada conforme a las reglas de marcado del paso 6, los coeficientes de frecuencia media de la parte media baja de los cuadrantes 3 y 4 debe ser modificada de forma simétrica. La componente marcada $Y_W(x,y)$ se obtiene aplicando la transformada inversa de Fourier IDFT definida previamente en (3.3), usando la magnitud marcada $M'(u,v)$ en conjunto con su preservada y no alterada información de fase $P(u,v)$. Finalmente, la componente marcada $Y_W(x,y)$ es res-escalada a las dimensiones de la imagen de color original. Los resultados en términos de robustez e imperceptibilidad se mostrarán en el capítulo 4.

## 3.3.2 Inserción de marca de agua en el dominio espacial

### 3.3.2.1 Histograma bidimensional

En gráficos de computadora y fotografía digital, un histograma de color es una representación de la distribución de colores en una imagen, derivado de contar el número de píxeles de cada color. Estas representaciones pueden ser presentadas en forma unidimensional (1D), bidimensional (2D) y tridimensional (3D) [6]. En la Figura 3.9 se muestra un ejemplo de histogramas unidimensionales obtenidos de las componentes del modelo de color RGB de una imagen de color.

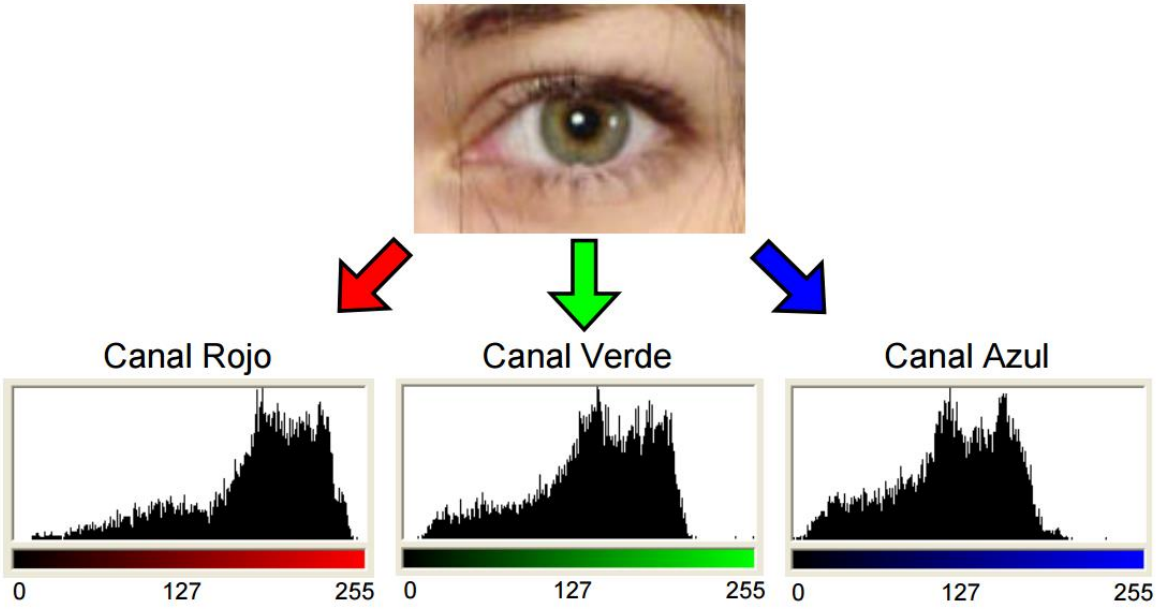



**Figura 3.9.** Ejemplo de histogramas 1D de cada componente de color RGB de una imagen.

Por su parte, un histograma bidimensional es una matriz donde la dimensión de cada uno de los ejes (x, y) es determinada por el rango de colores de cada componente a utilizar.

En particular, el histograma 2D es utilizado para representar la probabilidad de la coocurrencia, es decir, aparición simultánea de dos valores de niveles de gris cuando sus pixeles correspondientes se encuentran separados a una distancia específica. Este se puede definir como una matriz $H_{2D}$ que contiene información del nivel de gris de cada píxel y del nivel de gris promedio de la vecindad de un píxel dentro de la escala utilizada, esto es:

$$H_{2D}(i,j) \leftarrow \text{Número de píxeles que cumplen } Cb(m_1,m_2)=j \ \& \ Cr(n_1,n_2)=i \quad , \tag{3.10}$$

*donde:*

$n_1, m_1 = 1 \ldots N$

$n_2, m_2 = 1 \ldots M$

$NxM$ = Rango de color de la componente $0 \leq i, j \leq L-1, L=2^8$ .

En un histograma 2D los valores promedios locales representan la información espacial, sin tener una representación del punto preciso de la información que refleja cada píxel que compone la imagen, aunque permite tener una idea de la distribución espacial de los pixeles asociados a ciertas regiones en la imagen [6].

En la Figura 3.10 se muestra un conjunto de 5 imágenes de color y su correspondiente histograma 2D. Para generar los histogramas 2D se hace uso del modelo de color YCbCr, tomando en cuenta las componentes de crominancia de diferencia azul y roja denotadas como $C_b$, $C_r$ respectivamente en cada una de las imágenes.

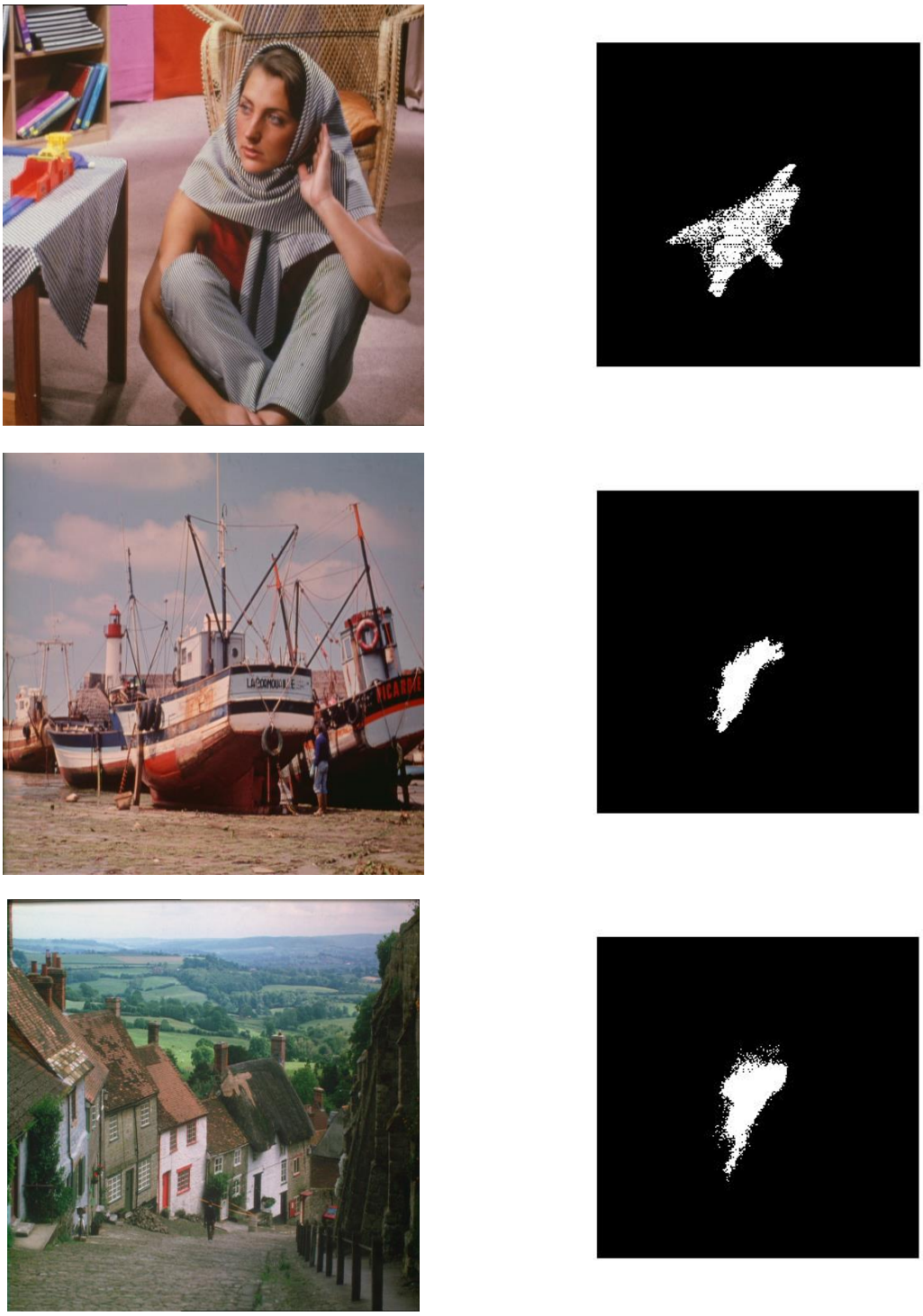


**Figura 3.10.** Conjunto de imágenes de color y su correspondiente histograma en 2D.

### 3.3.2.2 Inserción en el histograma bidimensional Cb-Cr

Para realizar la inserción en el histograma bidimensional Cb-Cr se realiza lo siguiente:

1.- Utilizando las componentes de crominancia, *Cb, Cr*, obtener el respectivo histograma bidimensional de color denotado como *H*.
2.- Ajustar la forma de la secuencia original *1D* de la marca de agua *W*, en una forma bidimensional denotada como $W_{rs}$ de tamaño $L = Q_1 \times Q_2$ (donde $Q_1$ y $Q_2$ son números enteros).
3.-Segmentar el histograma *H* en bloques de tamaño $L = Q_1 \times Q_2$ y seleccionar un bloque $B_H$ adecuado para insertar la secuencia de marca de agua. La característica principal para elegir un bloque $B_H$ es que casi todos los valores de los píxeles en $B_H$ deben ser distintos de cero. Debido a que puede haber muchos bloques que satisfacen esta condición; de entre ellos, se selecciona un bloque aleatoriamente, por lo que el número de bloque se proporcionará como clave secreta $K_3$ en la etapa de detección. El valor de píxel de $B_H(s,t)$ es modificado de acuerdo al bit de marca de agua $W_{rs}(s,t)$, como se muestra en la Figura 3.11.

$$SI \quad W_{rs}(s,t) = 0 \; ENTONCES$$
$$B_H(s,t) = 0$$
$$FIN \; SI$$

$$SI \quad W_{rs}(s,t) = 1 \; ENTONCES$$
$$B_H(s,t) \neq 0$$
$$FIN \; SI$$

**Figura 3.11**. Pseudo-código de reglas de inserción en histograma bidimensional *H*.

Donde $s = 1,..., Q_1$, $t = 1,..., Q_2$. Varias situaciones pueden surgir: Si $W_{rs}(s,t) = 0$ y $B_H(s,t) = 0$, así como si $W_{rs}(s,t) = 1$ y $B_H(s,t) \neq 0$, entonces no es necesario modificar $B_H(s,t)$. Sin embargo, en otros casos, $B_H(s\ t)$ debe ser modificado. En el caso del primer pseudo-código de la Figura 3.11, $B_H(s,t)$ debe ser forzado a tener un valor cero, distribuyendo su valor uniformemente como sea posible entre sus cuatro vecinos. En el caso del segundo pseudocodigo de la Figura 3.11, $B_H(s,t)$ debe ser obligado a ser diferente de cero, lo cual puede lograrse substrayendo un valor de pixel de algún vecino lejano y asignárselo a $B_H(s,t)$. Así, este método de inserción usando un histograma bidimensional como dominio de inserción, asegura la satisfacción del requerimiento de imperceptibilidad, debido a que los valores modificados son asignados a los píxeles vecinos, entonces el cambio en los colores de la imagen es muy ligero, manteniendo siempre inalterado el número total de píxeles respecto a los originales.

4.- Una vez que el histograma $H$ ha sido modificado, todos los valores de los píxeles se restauran y se obtienen las componentes de crominancia marcadas $Cb_w$ y $Cr_w$.

5.- Finalmente, la imagen de marca de agua $I_w$ es reconstruida usando $Y_W$ obtenida en la sección 3.3.1.5 en conjunción con las componentes marcadas $Cb_w$, $Cr_w$, restaurando así las componentes marcadas a su representación en el modelo de color RGB.

Los resultados en términos de robustez e imperceptibilidad se mostrarán en el capítulo 4.

## 3.4 Detección de marca de agua

Una vez que la imagen original ha sido marcada, es necesario desarrollar un algoritmo que permita detectar la presencia o ausencia de la marca de agua dentro de la misma, proceso que se explica a continuación.

1.- Convertir la imagen de color marcada $I_w$ del modelo de color RGB a su representación en el modelo de color YCbCr y obtener las componentes marcadas $Y_w$, $Cb_w$ and $Cr_w$.

2.- Para extraer los bits de marca de agua de la componente marcada $Y_w$, se hace uso de las llaves secretas $K_1$ y $K_2$, y se replican los pasos 2 al 5 del proceso de inserción en el dominio de la frecuencia descrito en la sección 3.3.1.5 de este capítulo. Entonces se genera un patrón de marca de agua extraída denotado como $W_1$, usando la función *sign* como sigue: si *sign* ($d_i$) es positivo '+' o cero '0' entonces $w'_i$=1, en otro caso $w'_i$=0, donde $i$ = 1, . . ., $L$.

3.- Para extraer los bits de marca de agua de las componentes marcadas $Cb_w$ y $Cr_w$, se calcula el histograma 2D marcado $H_w$ y este se segmenta en bloques de tamaño $L=Q_1 \times Q_2$. Usando la llave secreta $K_3$ se obtiene el bloque marcado $B_H$. Entonces a partir de la información del bloque $B_H$, el patrón de marca de agua extraído $W_2$ es generado de acuerdo a las siguientes condiciones: si $B_H(s,t)>0$ entonces $W_2(s,t)=1$, en otro caso $W_2(s,t)=0$, donde $s$=1, …, $Q_1$, $t$=1,…, $Q_2$. Finalmente, se re-ajusta el patrón $W_2$ a una forma en 1D.

4.- Usando todos los resúmenes criptográficos almacenados dentro de la base de datos de clientes, generar los respectivos patrones de marca de agua W usando el proceso de generación de marca de agua descrito en la sección 3.2 de este capítulo y obtener la tasa de bits erróneos (BER) entre cada patrón W y W1. Un valor umbra TBER debe ser definido para determinar si la marca de agua W está presente o no dentro de la imagen. En este sentido, considerando una distribución binomial con probabilidad de éxito igual a 0.5, la probabilidad de falsa alarma Pfa para L bits de marca de agua insertados está dada por (3.11), y otro valor umbral Tfa debe ser controlado para hacer que la Pfa sea más pequeña que un valor predeterminado [50].

$$P_{fa} = \sum_{r=T_{fa}}^{L} (0.5)^L \cdot \left( \frac{L!}{r!(L-r)!} \right) \tag{3.11}$$

Donde $L$ es el total de bits de la marca de agua, cuyo valor es empíricamente establecido como $L$=64. Empíricamente se establece que la probabilidad de falsa alarma debe ser menor que $P_{fa}$=3.86x10$^{-5}$ para considerar confiable la detección, cuando $T_{fa}$=48, para entonces determinar un adecuado valor umbral $T_{BER}$=(1- $T_{fa}$/$L$=1-(48/64)) = 0.25.

Por lo anterior, si la tasa de bits erróneos BER entre $W$ y $W_1$ es mayor que 25% (mayor que 16 bits erróneos), la detección de la marca de agua se considera fallida y entonces, el proceso de detección determina la BER entre $W$ y $W_2$, en caso contrario, la marca de agua se considera detectada satisfactoriamente y el proceso de detección termina. La misma condición se aplica para la BER entre $W$ and $W_2$; si está es mayor que 25%, el proceso de detección se considera fallido y termina la detección, en otro caso, la marca de agua es detectada con éxito y el proceso de detección termina.

5.- Finalmente, se recuperan de la base de datos la información de identidad del consumidor usando el índice en el cual el proceso de detección fue satisfactorio y se lleva a cabo la correcta autenticación del usuario de la imagen marcada.

Los resultados en términos de robustez e imperceptibilidad se mostrarán en el capítulo 4.

# Capítulo 4
# Resultados experimentales

## Introducción

Basados en los objetivos y la metodología mencionados en el Capítulo 1 de este trabajo de tesis, en este capítulo se mostrarán los resultados experimentales obtenidos en las etapas de generación, inserción y detección de marca de agua respectivamente. En principio se mostrarán los elementos que componen el prototipo de software, correspondientes a cada una de las etapas del esquema de marcado de agua. Posteriormente, se mostrarán los resultados experimentales obtenidos en términos de robustez e imperceptibilidad de la marca de agua.

## 4.1 Modulo de administración de clientes

Se creó una base de datos utilizando el manejador de bases de datos MySQL Workbench ©, la cual fue conectada con la interfaz del prototipo de software. La base de datos experimental consiste básicamente en una tabla que contiene los siguientes campos: identificador del cliente, nombre del cliente, RFC, datos de la institución de adscripción y el resumen criptográfico de los datos anteriores. En la Figura 4.1 se muestra el *script* utilizado para la construcción de la base de datos.

```
-- MySQL dump 10.13  Distrib 5.6.23, for Win64 (x86_64)
--
-- Host: localhost    Database: test
-- ------------------------------------------------------
-- Server version     5.6.24-log

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS,
FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `user`
--

DROP TABLE IF EXISTS `user`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `user` (
`iduser` int(11) NOT NULL AUTO_INCREMENT,
`nombre` varchar(45) NOT NULL,
`institucion` varchar(45) NOT NULL,
`rfc` varchar(19) NOT NULL,
`mdigest` varchar(45) NOT NULL,
PRIMARY KEY (`iduser`),
UNIQUE KEY `iduser_UNIQUE` (`iduser`)
) ENGINE=InnoDB AUTO_INCREMENT=3 DEFAULT CHARSET=utf8;
/*!40101 SET character_set_client = @saved_cs_client */;

--
```

**Figura 4.1.** *Script* de generación de base de datos del esquema propuesto.

Una vez generada la base de datos, se procedió con la construcción de la interfaz gráfica de usuario (GUI) correspondiente al módulo de administración de clientes usando el lenguaje de programación Java y el entorno de desarrollo integrado NetBeans ©, donde el propietario de la imagen digital podrá insertar, eliminar y buscar datos de clientes a los cuales se les ha permitido el uso de la imagen digital. La interfaz gráfica se muestra en la Figura 4.2.

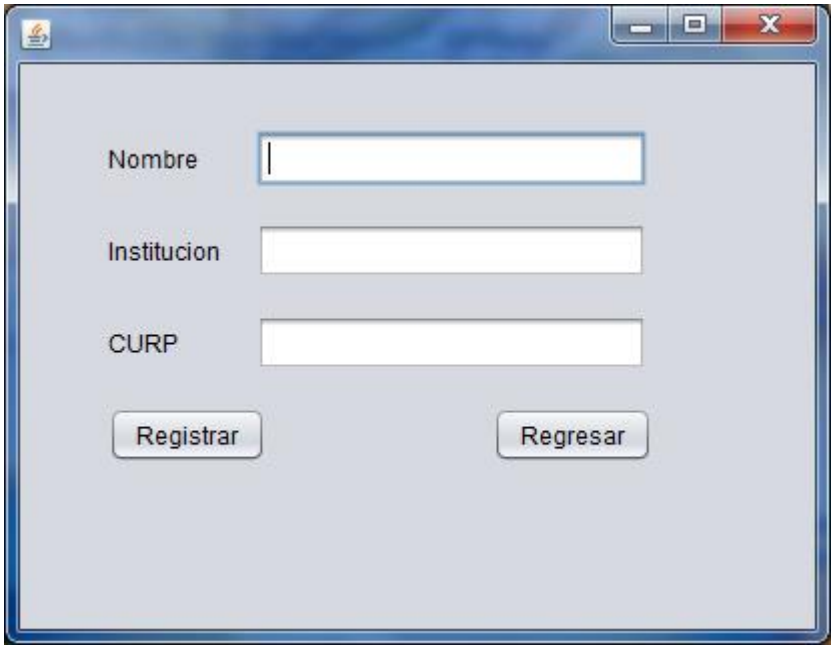



**Figura 4.2.** Interfaz gráfica de usuario del módulo de administración de clientes

## 4.2 Módulo de inserción de marca de agua

Una vez que los datos correspondientes al nombre, RFC e institución han sido proporcionados, se hará uso de una función de resumen criptográfico del algoritmo "RIPEMD-160" implementada en Java, que almacenará el *message digest* en un campo adicional dentro de la base de datos llamado *mdigest*, como se mostró previamente en la Figura 4.1. El archivo JAR del algoritmo "RIPEMD-160", así como la licencia de uso se encuentran disponibles en: Copyright (c) 2000-2005 The Legion Of The Bouncy Castle (http://www.bouncycastle.org), bajo la licencia GNU, como se muestra en la Figura 4.3.

```
The software in this package is distributed under the GNU General Public
 License (with "Library Exception" described below).

 A copy of GNU General Public License (GPL) is included in this
distribution,
in the file COPYING.  If you do not have the source code, it is available
at:

    http://www.gnu.org/software/classpathx/crypto

 In addition, the files distributed under GPL include the following special
 exception:

    As a special exception, if you link this library with other files to
    produce an executable, this library does not by itself cause the
```

```
resulting executable to be covered by the GNU General Public License.

This exception does not however invalidate any other reasons why the
executable file might be covered by the GNU General Public License.

As such, this software can be used to run Free as well as proprietary
applications and applets: static linking is permitted, so this can even be
used in embedded configurations.
```

**Figura 4.3.** Licencia de uso del algoritmo RIPEMD-160 implementado en Java.

Las librerías que se incluyen dentro del desarrollo del aplicativo en Java, para poder trabajar con el algoritmo RIPEMD-160, se muestran en la Figura 4.4.

```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */
package ripemd160;
import java.io.*;
import org.bouncycastle.crypto.digests.RIPEMD160Digest;
import org.bouncycastle.util.encoders.Hex;
import java.sql.*;
```

**Figura 4.4.** Librerías del algoritmo RIPEMD-160 implementado en Java.

La inserción de la marca de agua se lleva a cabo mediante una llamada desde una GUI Java a un archivo ejecutable creado previamente en Matlab ©, como se muestra en la Figura 4.5.

```
String command = "insercion.exe " + path + " " + alfa + " " + hash + "";
Process p = Runtime.getRuntime().exec(command);
```

**Figura 4.5.** Proceso de inserción de marca de agua desde Java.

El crear el ejecutable usando Matlab © y posteriormente hacer el llamado desde Java, obedece a un tema específico de distribución de la aplicación. Lo único que se necesitaría para poder ejecutar el archivo *.exe, sería instalar el componente MATLAB © Component Runtime (MCR) en el equipo de cómputo correspondiente, los términos de uso y las diferentes versiones se encuentran disponibles en: http://www.mathworks.com/products/compiler/mcr/ .La interfaz gráfica de usuario del módulo de inserción se muestra en la Figura 4.6.

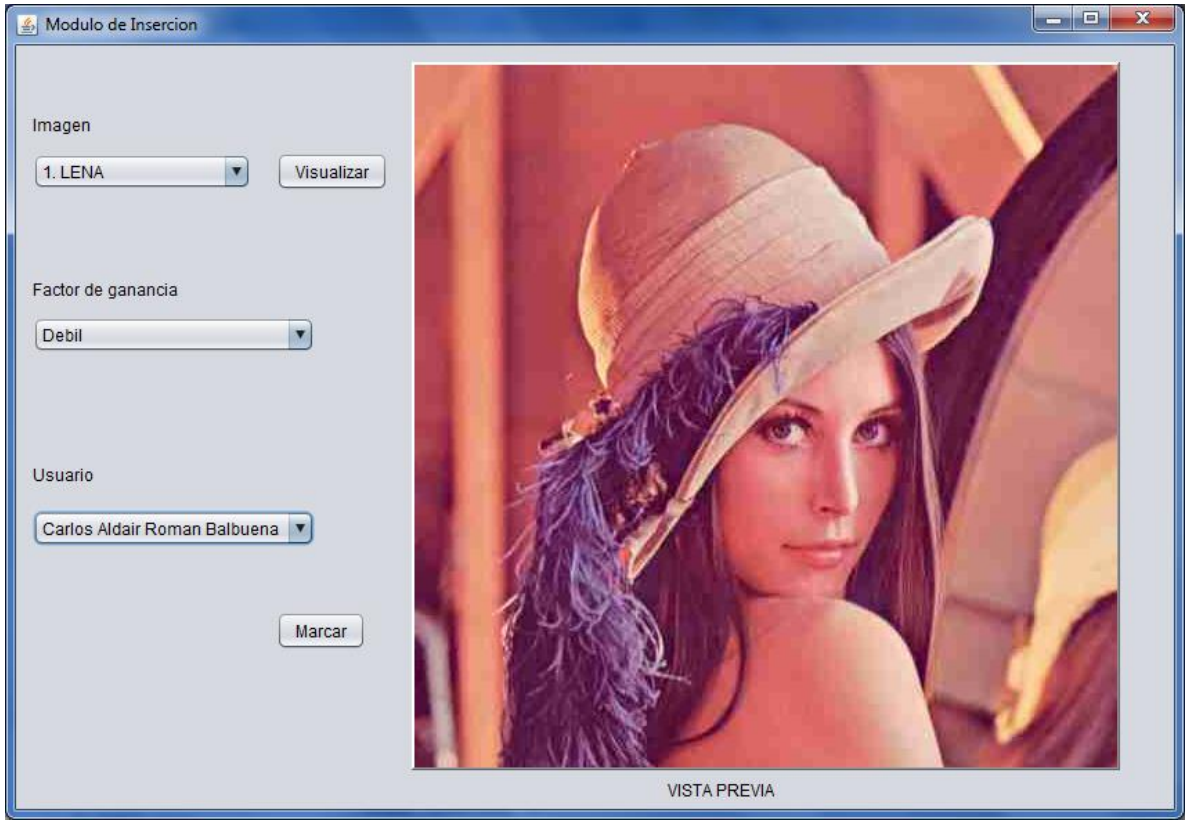



**Figura 4.6.** Interfaz gráfica de usuario del módulo de inserción de marca de agua

## 4.3 Modulo de detección de marca de agua

En el módulo de detección se extraerá la información de marca de agua que contenga una imagen digital protegida y se hará una búsqueda dentro de la base de datos con el propósito de detectar a que cliente fue asignada dicha copia digital. Para realizar la búsqueda de una manera más dinámica, se implementó un proceso por lotes que invoca al archivo ejecutable correspondiente al proceso de detección, pasándole como parámetros únicamente la ruta de la imagen marcada y los datos de la conexión a la base de datos, es decir, el usuario, la instancia de BD y el password, como se muestra en la Figura 4.7.

```
echo.
::Llamada al proceso de detección
deteccion.exe "%var%" %instancia% %usuario% %password%
```

**Figura 4.7.** Llamada al archivo ejecutable correspondiente al proceso de detección mediante un proceso por lotes

El archivo ejecutable, así como el código asociado a la conexión con la BD y el algoritmo de detección fueron generado e implementados usando el entorno de desarrollo integrado Matlab ©, respectivamente.

## 4.4 Imperceptibilidad y robustez de marca de agua

En este apartado se muestran los resultados experimentales obtenidos en términos de la robustez así como la imperceptibilidad de la marca de agua.

### 4.4.1 Parámetros de configuración

Los resultados experimentales del algoritmo de marca de agua propuesto en este trabajo de tesis fueron llevados a cabo desde un punto de vista de atención a los requerimientos de imperceptibilidad y robustez. Se hizo uso de 1000 imágenes de prueba con diferente contenido y dimensiones de 1024x768, 800x600 y 512x512 píxeles, todas con una resolución de 24 bits/píxel. Los experimentos fueron llevados a cabo en una computadora personal bajo el sistema operativo Microsoft Windows 7©, con un procesador Intel Core i7© a 2.4Ghz y 8 GB en memoria RAM. Los algoritmos de inserción y detección fueron implementados en Matlab© 8.1 y la interfaz gráfica de usuario en Java usando el IDE NetBeans©. La base de datos fue implementada usando MySQL© 5.6.25. Como patrón de marca de agua $W$, se hizo uso de una secuencia binaria en 1D de longitud $L$=64 bits [3]. La llave secreta $K_1$ se estableció como $K_1$={$N_1$=$N_2$=500}. La llave secreta $K_2$ se compone de un par de radios utilizados en el proceso de inserción en el dominio de la frecuencia, donde los valores finales fueron establecidos como $K_2$={$r_1$=81,$r_2$=82}[3]. El factor de fuerza de inserción de marca de agua utilizado en el proceso de inserción en el dominio de la frecuencia es $\alpha$ = 15000. Los valores enteros $Q_1$ y $Q_2$ utilizados en el proceso de inserción

en el histograma bidimensional a los cuales se les asignó un valor de $Q_1=Q_2=8$ cuando $L=64$. Finalmente la calidad de la imagen marcada es medida usando los índices PSNR y SSIM. La diferencia de color entre la imagen original y marcada fue medida usando la métrica de diferencia de color normalizada NCD.

### 4.4.2 Imperceptibilidad de marca de agua

Como se muestra en las Figuras 4.8 y 4.9, un valor grande correspondiente al factor de fuerza de inserción de la marca de agua $\alpha$ puede incrementar la robustez de la marca de agua ante distorsiones geométricas y procesamientos de señal avanzados, sin embargo la imperceptibilidad de la marca puede verse afectada. Para preservar el compromiso (*trade-off* en inglés) entre los requerimientos de robustez e imperceptibilidad, basados en los experimentos, se consideró establecer un factor de fuerza de inserción $\alpha=15000$ como un valor que satisface los requerimientos del algoritmo. En la Figura 4.10 se muestran la NCD de 5 imágenes de prueba originales con respecto a sus versiones marcadas considerando un valor de $L=64$, $\alpha=15000$, $K_1=\{N_1=N_2=500\}$, $K_2=\{r_1=81,r_2=82\}$ y $Q_1=Q_2=8$. A partir de la Figura 4.10, se puede observar que el esquema de marcado de agua propuesto proporciona una excelente fidelidad en la imagen marcada, debido a que la diferencia de colores entre las imágenes original y marcada es insignificante, ya que los valores están muy cercanos a 0.

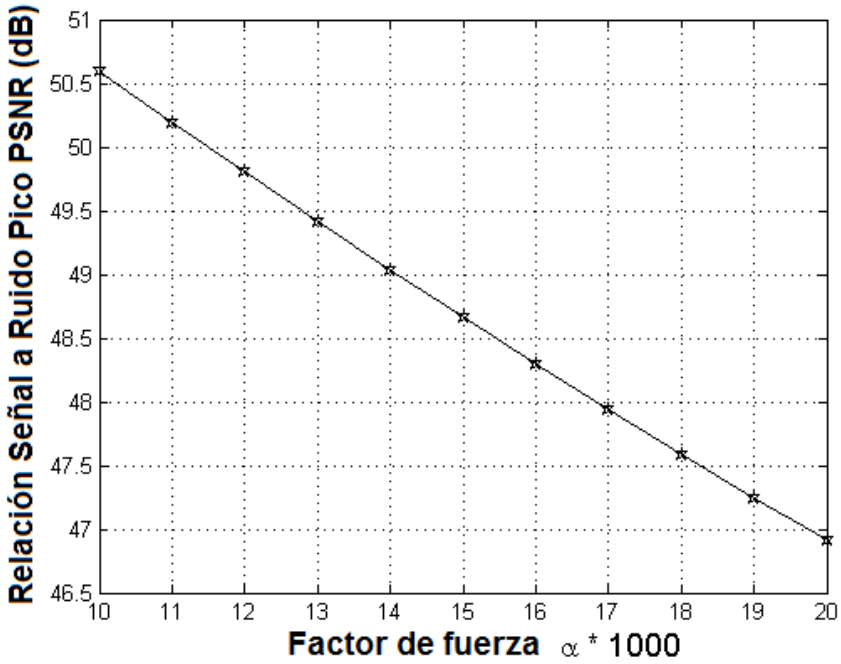



**Figura 4.8.** Valor de PSNR (dB) promedio obtenido con un factor de fuerza de inserción $\alpha$ variable.

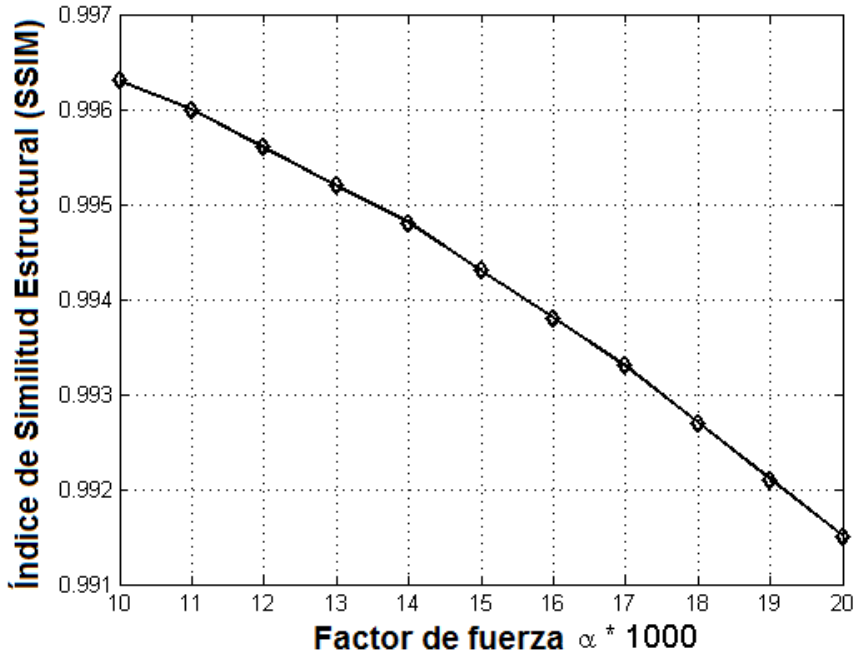



**Figura 4.9.** Valor de SSIM promedio obtenido con un factor de fuerza de inserción $\alpha$ variable.

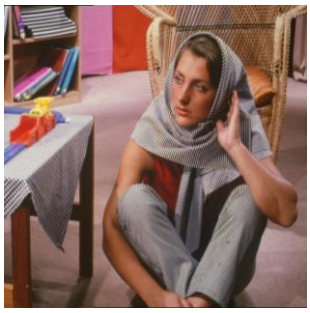
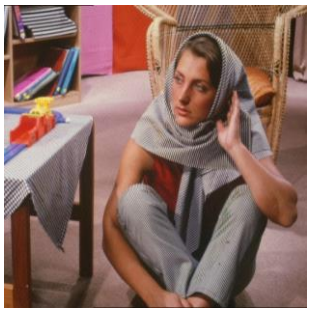
| *Imagen original* | *Imagen marcada* | *NCD* |
|---|---|---|
|  |  | 0.0066 |
|  |  | 0.0129 |
|  |  | 0.0105 |
|  |  | 0.0049 |
|  |  | 0.0074 |

**Figura 4.10.** NCD de imágenes originales respecto a su versión

### 4.4.3 Robustez de marca de agua

Para evaluar la robustez del esquema de cara de agua propuesto, las diferentes distorsiones aplicadas a las imágenes protegidas se clasifican en geométricas, procesamiento avanzado de señal, distorsiones combinadas y filtrado artístico, como se muestra en la Tabla 1.

| **Distorsiones** | |
|---|---|
| Geométricas | (a) Rotación de 105°<br>(b) Rotación de 35° con auto-recorte y re-escalamiento<br>(c) Traslación $x$=70,$y$=90<br>(d) Recorte centrado 30%<br>(e) Escalamiento con factor $fs$=0.5<br>(f) Escalamiento con factor $fs$=2<br>(g) Flipping<br>(h) Transformación affine<br>(i) Recorte del 75%<br>(j) Deformación en planos paralelos<br>(k) Relación de aspecto<br>(l) Transformación proyectiva. |
| Procesamiento avanzado de señal | (m) Compresión JPEG con factor de compresión 70<br>(n) Compresión JPEG con factor de compresión 50<br>(o) Compresión JPEG con factor de compresión 20<br>(p) Ajuste de brillo<br>(q) Contraste mejorado<br>(r) Ruido Gausiano con $\mu$=0 y $\sigma^2$ =0.004<br>(s) Ruido impulsivo con densidad 0.02<br>(t) Filtrado de mediana con ventana 3x3<br>(u) Sharpening<br>(v) Filtro Gausiano 3x3. |
| Combinadas | Compuestas por:<br>Compresión JPEG con factor de compresión 70 + distorsión geométrica a partir del inciso (a) hasta el (f) asi como procesamiento avanzado de señal desde el inciso (p) hasta el (v). |
| Filtrado artístico | (1) Brillo en la lente, (2) Efecto celofan, (3) Efecto pelicula, (4) Foto antigua, (5) Vidrio, (6) Gravado, (7) Impresión periodico, (8) Jitter, (9) Marco tipo viñeta, (10) Emborronado por movimiento, (11) Textura, (12) Azulejos |

**Tabla 4.1.** Conjunto de distorsiones consideradas dentro de los resultados experimentales

Empíricamente, como se estableció en el capítulo 3 de esta tesis, la probabilidad de falsa alarma debe ser menor que $P_{fa}$=3.86x10$^{-5}$ para considerar confiable la detección, cuando $T_{fa}$=48, para entonces determinar un adecuado valor umbral $T_{BER}$=(1- $T_{fa}/L$=1-(48/64)) = 0.25. Valores de BER mayores a 0.25 son considerados como una detección fallida.

En las Figuras 4.11, 4.13 y 4.14 se muestran las respuestas del detector de marca de agua ante las distorsiones geométricas, procesamientos avanzados de señal y distorsiones combinadas respectivamente. Para ser más precisos y concentrar los resultados en una sola gráfica, los valores que se muestran en las Figura 4.11, 4.13 y 4.14 son el promedio obtenido de todas las imágenes, en términos de la tasa de bits erróneos BER. Los resultados en cada gráfica son mostrados en las formas HT y DFT, donde HT denota la salida del detector correspondiente al histograma bidimensional y la forma DFT corresponde a la salida del detector usando la inserción en el dominio de la frecuencia.

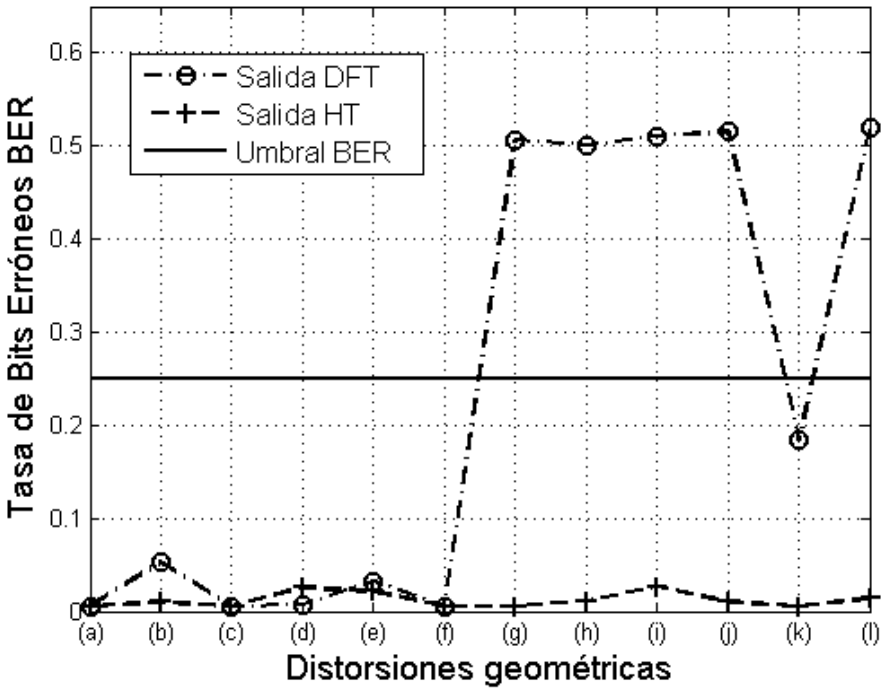



**Figura 4.11.** BER obtenido después de aplicar cada una de las distorsiones geométricas de la Tabla 4.1.

A partir de la Figura 4.11 se puede observar que la salida del detector correspondiente a HT tiene un mejor rendimiento ante las distorsiones geométricas con respecto a la salida DFT, esto se debe a que mientras el dominio DFT presenta robustez ante los ataques de rotación, escalamiento, traslación (RST), así como ante el recorte de imagen, la inserción dentro del

histograma bidimensional permite extender la robustez del método ante otro tipo de distorsiones que son más agresivas con la imagen, como lo es el caso de la transformación de tipo affine y proyectiva, como se muestra en la Figura 4.12.

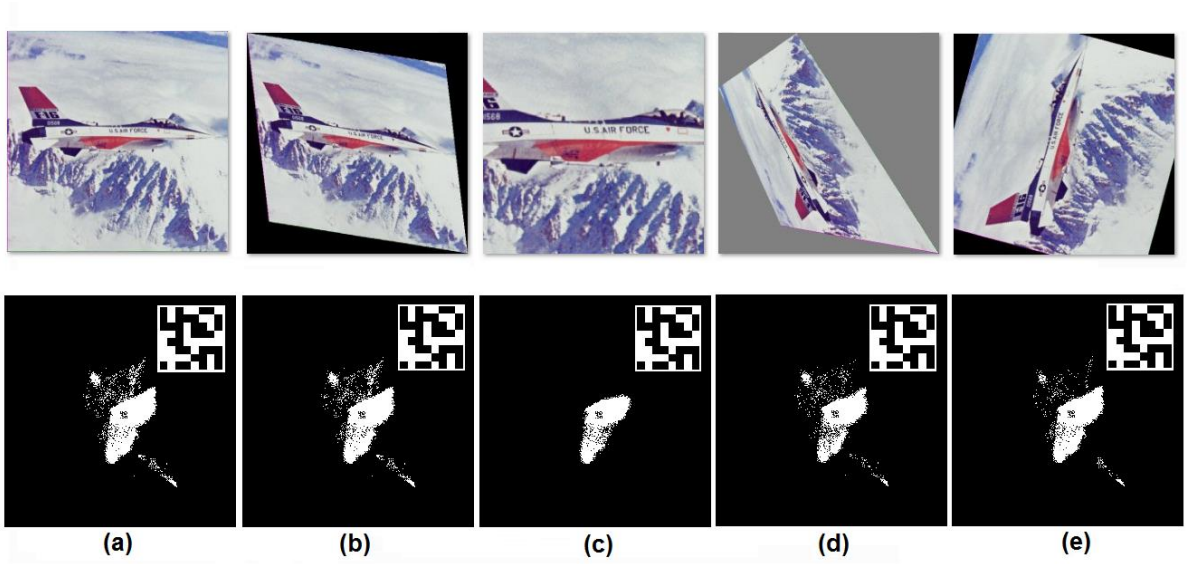



**Figura 4.12.** Imagen marcada antes y después de ataques geométricos agresivos, junto con su histograma 2D Cb-Cr recuperado y un acercamiento a la región recuperada usando la llave secreta $K_3$, que muestra la marca de agua recuperada. (a) Sin distorsión. (b) Transformación affine. (c) Recorte con re-escalamiento. (d) Transformación proyectiva y (e) Rotación con auto-recorte y re-escalamiento.

Sin embargo, como se muestra en las Figuras 4.13 y 4.14, la salida del detector DFT obtiene un mejor rendimiento ante los procesamientos avanzados de señal incluyendo compresión con perdida JPEG, mejoramiento de imagen, contaminación por ruido, filtrado y ataques combinados, con respecto a la salida del detector HT. Por lo tanto, conforme a los resultados obtenidos, se puede afirmar que el diseño de marcado de agua híbrido permite hacer frente a una mayor cantidad de distorsiones geométricas, de procesamiento avanzado de señal y combinación de ambos tipos.

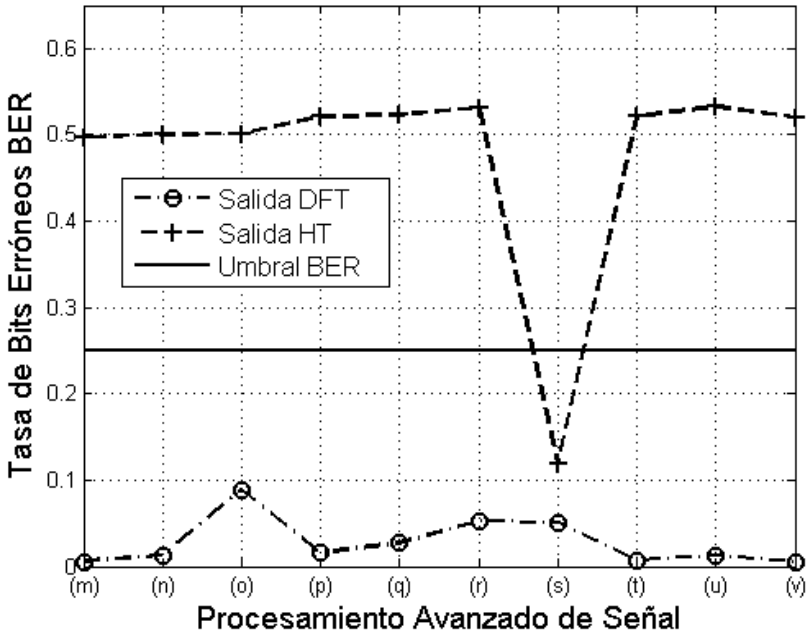



**Figura 4.13.** BER obtenido después de aplicar cada uno de los procesamientos avanzados de señal de la Tabla 4.1.

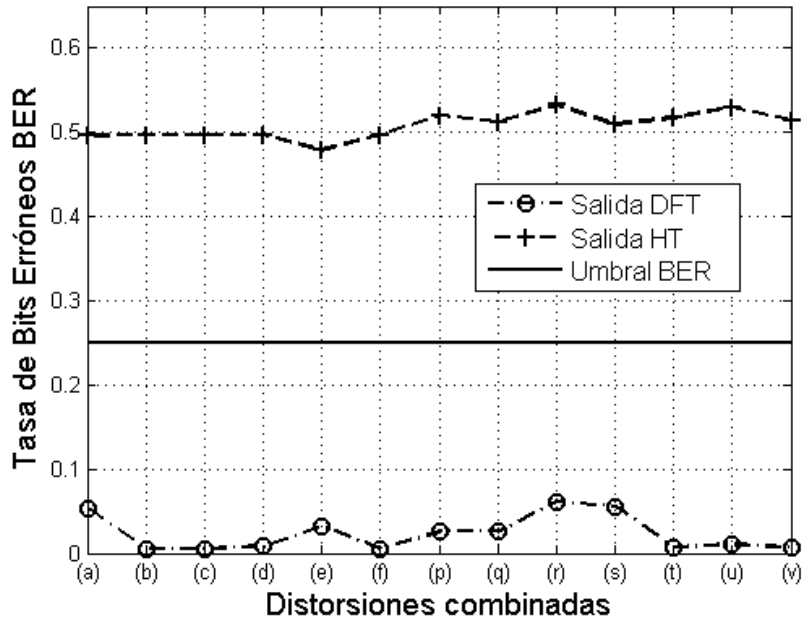
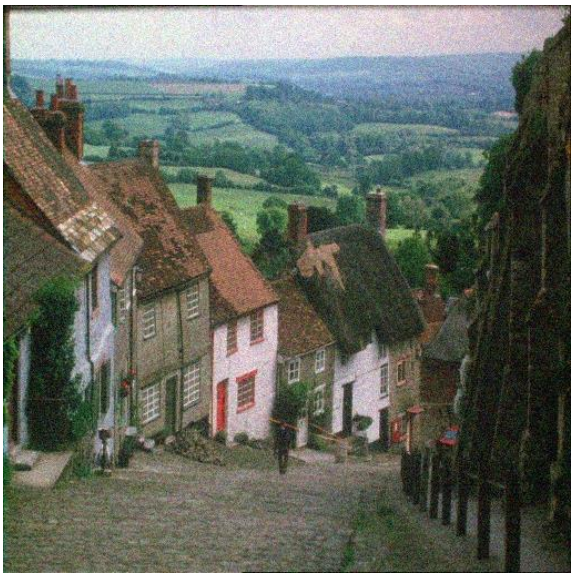



**Figura 4.14.** BER obtenido después de aplicar cada una de las distorsiones combinadas de la Tabla 4.1.

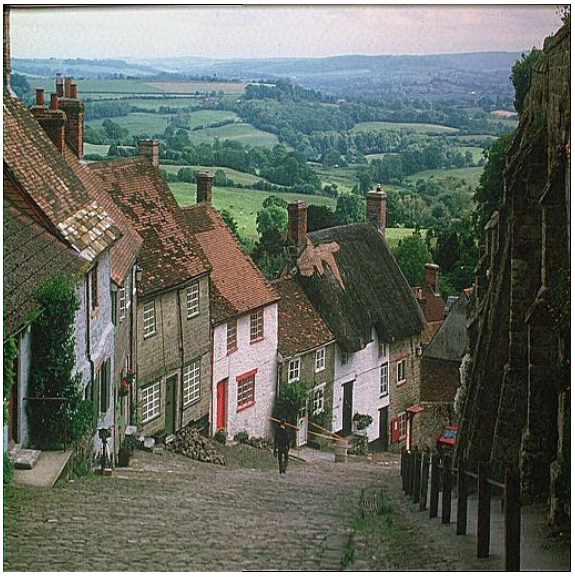
La Figura 4.15 muestra algunos ataques agresivos de tipo procesamiento avanzado de señal.

(a)



(b)

(c)



(d)

**Figura 4.15.** Distorsiones agresivas de tipo procesamiento de señal avanzado. (a) Compresión JPEG con factor de calidad 20. (b) Contaminación por ruido Gausiano. (c) Aumento de brillo y (d) Sharpening.

Para mostrar la robustez ante el filtrado de tipo artístico, se aplicaron diferentes filtros a la imagen de Lena usando el editor de imágenes Photoshop ©, los cuales se mencionan en la Tabla 4.1 y se muestran en la Figura 4.16.

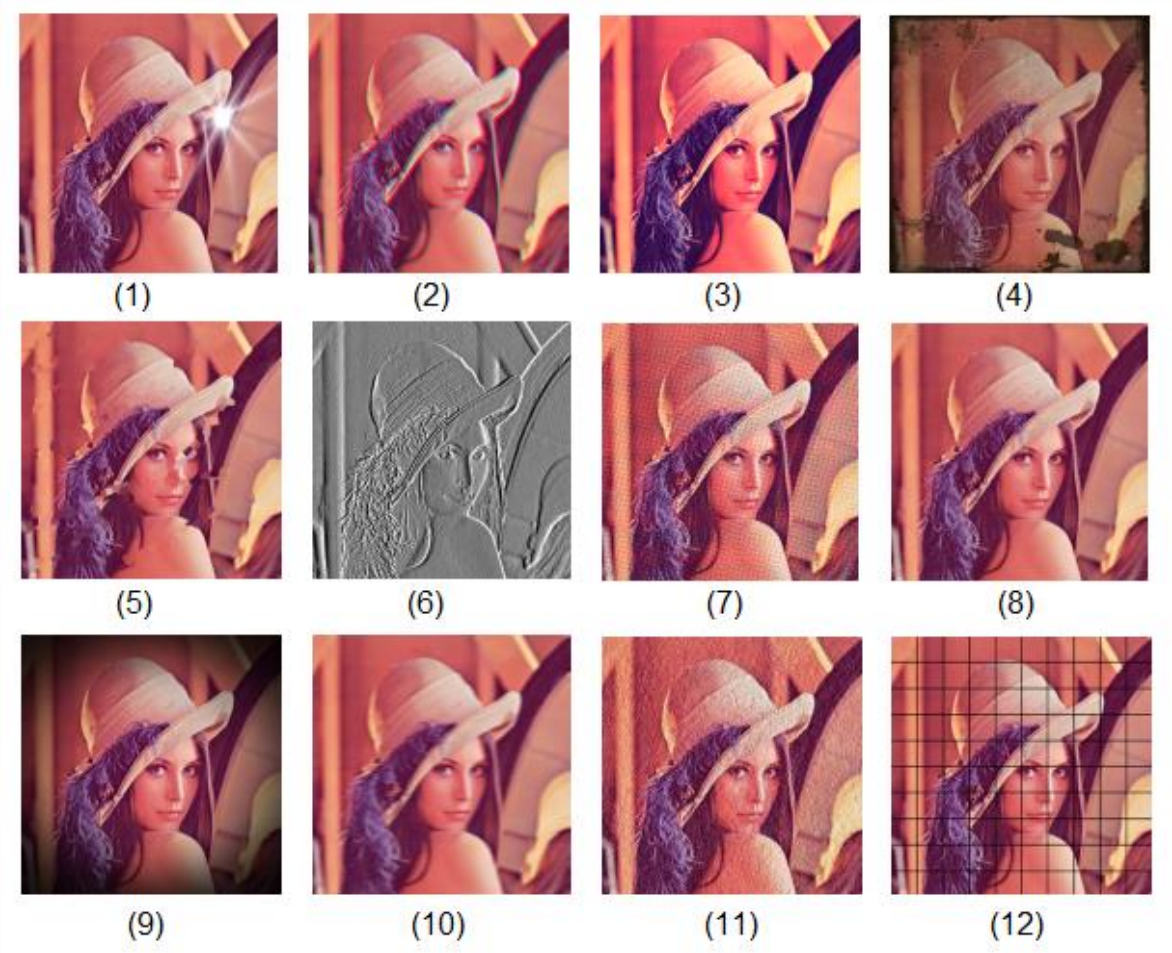



**Figura 4.16.** Filtrado artístico en la imagen de Lena

Los resultados de robustez se muestran en la Tabla 4.2. Como se puede observar, el método de marcado de agua híbrido propuesto en este trabajo de tesis presenta buena robustez ante diversos filtros artísticos, obteniendo tasas de detección en términos de BER mayores que 93% en la salida del detector DFT.

| *Ataque* | *Salida HT* | *Salida DFT* |
|---|---|---|
| (1) Brillo en la lente | *0.53* | 0 |
| (2) Efecto celofán | *0.53* | 0.03 |
| (3) Efecto película | *0.48* | 0 |
| (4) Foto antigua | *0.46* | 0.07 |
| (5) Vidrio | *0.50* | 0.07 |
| (6) Gravado | *0.46* | 0.03 |
| (7) Impresión periódico | *0.50* | 0.03 |
| (8) Jitter | *0.50* | 0.03 |
| (9) Marco tipo viñeta | *0.45* | 0.06 |
| (10) Emborronado por movimiento | *0.46* | 0 |
| (11) Textura | *0.53* | 0.07 |
| (12) Azulejos | *0.54* | 0 |

**Tabla 4.2.** BER obtenida de la imagen Lena después de aplicar filtrado artístico

# Capítulo 5
# Conclusiones generales y trabajo a futuro

## 5.1 Conclusiones generales

En la presente tesis se dio a conocer una técnica de marcado de agua hibrida aplicada a imágenes digitales de color, con el propósito de detectar copias ilegales mediante la autenticación del cliente. Se demostró que el método preserva una alta calidad en la imagen marcada y muy buena robustez contra distorsiones geométricas, incluyendo ataques RST, *affine*, transformación proyectiva, de relación de aspecto y ataques agresivos de recorte, entre otros. Igualmente es robusto ante distintas distorsiones de procesamiento de señal tales como la compresión JPEG, realzado de imagen, adición de ruido, filtrado y ataques combinados.

Basados en los resultados obtenidos se comprobó que la técnica de marcado de agua aplicada a imágenes digitales permitió identificar al propietario de la imagen satisfactoriamente en la mayoría de los casos, a excepción de aquellas imágenes en las cuales se aplicó una combinación de filtros artísticos de Photoshop® tales como molinete, onda, esferizar u algunos otros filtros combinados. Esto debió a que la marca de agua no resistió ataques tan agresivos.

Se mostró que al realizar la inserción, no solo en el dominio espacial sino también en el dominio transformado se logró una mejoría en robustez e imperceptibilidad contra diferentes ataques intencionales o no intencionales tales como rotación, escalamiento, traslación, la compresión de imágenes JPEG, la contaminación de imágenes por ruido Gaussiano e impulsivo, el filtrado, entre otros.

Sin embargo hay que denotar que al querer una marca de agua demasiada robusta se sacrifica imperceptibilidad o al querer demasiada imperceptibilidad se sacrifica robustez, es por ello que en el resultado de esta tesis (al realizar las distintas pruebas ya mencionadas con anterioridad) se encontró un factor de fuerza de inserción donde se pudo balancear tanto el aspecto de robustez como el de imperceptibilidad.

## 5.2 Trabajo Futuro

- Mejorar la técnica de inserción dentro del histograma bidimensional de imágenes de color para adquirir mayor robustez ante procesamiento avanzado de señal.
- Extender la aplicación del método a material de video digital
- Continuar la investigación para adaptar una función criptográfica dentro del esquema de marcado que permita además de detectar la marca de agua, recuperar la información contenida dentro de la misma.

# Referencias


1. Páez Rafael,***"Esteganografía: Ocultando el uso de LSB",*** Marzo 2013, LSB. Recuperado el 06 de octubre de 2015 de http://www.securityartwork.es/2013/03/07/estenografia-ocultando-el-uso-de-lsb.
2. Morales Delgado, Edgar Emilio (2010). "***Marca de agua invisible para imágenes digitales utilizando un índice estructural de similaridad para medir la calidad perceptual de la imagen marcada"***, Universidad Nacional Autónoma de México. Recuperado el 06 de octubre de 2015
3. Cedillo-Hernández Manuel, ,García Ugalde Francisco, Nakano Miyatake Mariko & Pérez-Meana Héctor Manuel***," Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification"***, © Springer-Verlag London 2013
4. ***"Criptografía Caótica"***, Recuperado el 06 de octubre de 2015 de http://www.textoscientificos.com/criptografia/caotica.
5. Martínez Aguilón Erika, ***"Fundamentos de Criptografía"***, Recuperado el 06 de octubre de 2015 de http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/11-concepto-de-criptografia
6. Cedillo Hernández Manuel (2011), ***"Esquemas Robustos De Marca De Agua Aplicados A Imágenes Digitales"***, Instituto Politécnico Nacional. Recuperado el 06 de agosto de 2015
7. Márquez Jorge***, "Procesamiento y Análisis de Señales e Imágenes"***, Recuperado el 06 de octubre de 2015 de http://www.academicos.ccadet.unam.mx/jorge.marquez/cursos/imagenes_neurobiomed/Mediana_filtro.pdf
8. Ramos Rivas Elva (2003), ***"Sistema de pre-procesamiento de imágenes electrocardiográficas en telemedicina"***, Universidad de las Américas Puebla el 06

de octubre de 2015 de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ramos_r_m/capitulo3.pdf

9. Gonzales and Woods***,"Digital Image Processing"***, 3rd. Ed. Recuperado el el 06 de octubre de 2015 de http://alojamientos.us.es/gtocoma/pid/tema1-2.pdf
10. H. Chang and H.H. Chen, ***"Stochastic Color Interpolation for Digital Cameras"***, IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 8, pp. 964-973, Aug 2007.
11. K. N. Plataniotis, A. N. Venetsanopoulos, ***"Color Image Processing and Applications"***, Springer Verlag, Berlin, 2000
12. Saraju P. Mohanty, ***"Digital Watermarking : A Tutorial Review"***, Dept of Comp Sc and Eng. Unversity of South Florida Tampa, 1999
13. García Horta Manuel (2010), ***"Autenticación de Documentos Digitales Usando la Técnica de Marca de Agua"***. Instituto Politécnico Nacional. Recuperado el 06 de octubre de 2015 de http://tesis.ipn.mx/bitstream/handle/123456789/9420/233.pdf?sequence=1
14. Langelaar Gerhard C., Setyawan Iwan, y Lagendijk Reginald L***.,"Watermarking Digital Image and Video Data"***, IEEE signal processing magazine, september 2000
15. - W. Stallings, ***"Fundamentos de seguridad en redes: aplicaciones y estándares"***, Pearson Prentice Hall, Madrid (España) Segunda edición 2004
16. -Death Master, ***"Criptosistemas Informáticos"***,2004. Recuperado el 06 de octubre de 2015 de http://190.90.112.209/http/criptografia/Criptosis.pdf
17. - M. Cedillo-Hernández, F. García-Ugalde, M. Nakano-Miyatake, M. and H. Pérez-Meana, ***"Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification"***, Signal, Image and Video Processing, 2014, vol. 8, no.1, pp. 49-63
18. - C.W. Tang and H.M. Hang, ***"A feature-based robust digital image watermarking scheme"***, IEEE Trans. Signal Process, 2003, vol. 51, no. 4, pp. 950–959.
19. - G. Yuval, ***"How to swindle Rabin"***, Cryptologia, Vol. 3, No. 3, 1979, pp. 187–189.
20. -R. Merkle, ***"One way hash functions and DES***", Advances in Cryptology, Proc. Crypto'89, LNCS 435, G. Brassard, Ed., Springer-Verlag, 1990, pp. 428–446.

21. - C.H. Meyer, M. Schilling, ***"Secure program load with Manipulation Detection Code"***, Proc. Securicom 1988, pp. 111–130.
22. - B. Preneel, R. Govaerts, J. Vandewalle, "Hash functions based on block ciphers: a synthetic approach", Advances in Cryptology, Proc. Crypto'93, LNCS 773, D. Stinson, Ed., Springer-Verlag, 1994, pp. 368–378.
23. - B. den Boer, A. Bosselaers, ***"An attack on the last two rounds of MD4"***, Advances in Cryptology, Proc. Crypto'91, LNCS 576, J. Feigenbaum, Ed., Springer-Verlag, 1992, pp. 194–203.
24. -R.L. Rivest, ***"The MD5 message-digest algorithm"***, Request for Comments (RFC) 1321, Internet Activities Board, Internet Privacy Task Force, April 1992.
25. - B. den Boer, A. Bosselaers, ***"Collisions for the compression function of MD5***", Advances in Cryptology, Proc. Eurocrypt'93, LNCS 765, T. Helleseth, Ed., SpringerVerlag, 1994, pp. 293–304.
26. - S. Vaudenay, ***"On the need for multipermutations: cryptanalysis of MD4 and SAFER"***, Fast Software Encryption, LNCS 1008, B. Preneel, Ed., Springer-Verlag, 1995, pp. 286–297.
27. - R. Anderson***, "The classification of hash functions"***, Proc. of the IMA Conference on Cryptography and Coding, Cirencester, December 1993, Oxford University Press, 1995, pp. 83–95.
28. - H. Dobbertin, ***"RIPEMD with two-round compress function is not collisionfree"***, Journal of Cryptology, to appear.
29. - H. Dobbertin, ***"Cryptanalysis of MD4"***, Fast Software Encryption, this volume.
30. - R.L. Rivest, "The MD4 message digest algorithm", Advances in Cryptology, Proc. Crypto'90, LNCS 537, S. Vanstone, Ed., Springer-Verlag, 1991, pp. 303–311.
31. Ruanaidh, J.Ó., Pun, T. ***"Rotation, scale and translation invariant spread spectrum digital image watermarking"***, Signal Process. 66,303–317 (1998)
32. Bum-Soo, K., Jae-Gark, C., Chul-Hyun, P., Jong-Un, W., Dong-Min, K., Sang-Keun, O., et al. ***"Robust digital image watermarking method against geometrical attacks"***, Real-Time Imaging 9, 139–149 (2003)

33. Ridzon, R., Levicky, D. "***Log-Polar Mapping in Robust Digital Image Watermarking"***, Institute of Electric and Electronics Engineers Computer Society, Brno (2007)
34. Yan, L., Jiying, Z. ***"A new video watermarking algorithm based on 1D DFT and Radon transform"***, Signal Process. 90, 626–639 (2010) 5.
35. Dong, P., Brankov, J.B., Galatsanos, N.P., Yang, Y., Davoine, F. ***"Digital watermarking to geometric distortions",*** IEEE Trans. Image Process. 14(12), 2140–2150 (2005)
36. Cedillo, M., Nakano, M., Perez, H. ***"A robust watermarking technique based on image normalization"***, Rev. Fac. Ing. Univ. Antioquia J. Eng. Fac. Univ. AntioquiaMedellin Colombia 52, 147–160 (2010)
37. Kim, H.S., Lee, H.-K.***"Invariant image watermark using Zernike moments"***, IEEE Trans. Circuits Syst. Video Technol. 13(8), 766–775 (2003)
38. Chareyron, G., Da Rugna, J., Trémeau, A***."Color in image watermarking. In: Al-Haj, A. (ed.) Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications"***, IGI Global, pp. 36–56 (2010). doi:10.4018/978-1-61520-903-3.ch003
39. V. Solachidis and I. Pitas, ***"Circulary Symmetric Watermark Embedding in 2-D DFT Domain"***, in IEEE Trans. Image Process, vol. 10 no. 11, pp 1741-1753 Nov. 2001.
40. Battiato, S., Catalano, D., Gallo, G., Gennaro, R***." Robust watermarking for images based on color manipulation"***,In: Proceedings of the Third InternationalWorkshop on InformationHiding. Springer, vol. 1768, pp. 302–317 (2000)
41. Zhang, X.,Wang, S***."Fragile watermarking scheme using a hierarchical mechanism"***, Signal Process. 89(4), 675–679 (2009)
42. Kougianos, E., Mohanty, P., Mahapatra, R.N***." Hardware assisted watermarking for multimedia"***, Comput. Electr. Eng. 35(2), 339–358 (2009)
43. Coltuc,D., Bolon, P***."Robustwatermarking by histogram specification"***,In: Proceedings of 6th IEEE Conference on Image Processing (ICIP' 99). Kobe, Japan, vol. 2, pp. 236–239 (1999)

44. Chareyron, G., Macq, B. and Tremeau, A*.” Watermarking of color images based on segmentation of the XYZ color space”*, In: CGIV Second European Conference on Color in Graphics, Imaging and Vision, Aachen, Germany, pp. 178–182 (2004)
45. Roy, S., Chang, E.C*.”Watermarking color histogram”*, In Proceedings of IEEE Internaional Conference on Image Processing, Singapore,pp. 2191–2194 (2004)
46. Lin, C.H., Chan, D.Y., Su, H., Hsieh, W.S*.” Histogram oriented watermarking algorithm: color imagewatermarking scheme robust against geometric attacks and signal processing”*, IEE Proc. Vis.Image Signal Proces. 153(4), 483–492 (2006)
47. Xiaolin, J., Yanli, Q., Liping, S., Xiaobo, J*.” An anti-geometric digital watermark algorithm based on histogram grouping and fault-tolerance channel”*,In: Intelligent Science and Intelligent Data Engineering. Lecture Notes in Computer Science (2012). doi:10.1007/978-3-642-31919-8_96
48. Chrysochos, E., Fotopoulos, V., Skodras, A. Xenos,M*.”Reversible imagewatermarking based on histogram modification”*, In: Proceedings of 11th Panhellenic Conference on Informatics with International Participation (PCI), B, pp. 93–104 (2007)
49. Chrysochos, E., Fotopoulos, V., Xenos,M., Skodras, A.N*.” Hybrid watermarking based on chaos and histogram modification”*, Signal Image Video Process. (2012). doi:10.1007/s11760-012-0307-3
50. C.W. Tang and H.M. Hang*, “A feature-based robust digital image watermarking scheme”*, IEEE Trans. Signal Process, 2003, vol. 51, no. 4, pp. 950–95

# Anexo A

# Lista de Publicaciones.

## MEMORIAS DE CONGRESOS INTERNACIONALES

1.- Manuel Cedillo-Hernández, Antonio Cedillo-Hernández, Carlos Aldair Roman-Balbuena, Francisco García-Ugalde, Mariko Nakano-Miyatake and Héctor Manuel Pérez-Meana: *"Customer authentication of digital imaging using hybrid watermarking",* in IEEE International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE) will be held in Cuernavaca, Morelos on November 24-27, 2015.

# ICMEAE

# INTERNATIONAL CONFERENCE ON MECHATRONICS, ELECTRONICS AND AUTOMOTIVE ENGINEERING



## 2015

Cuernavaca, Morelos, México.

Instituto de Ingenieros de Morelos

Universidad Autónoma del Estado de Morelos

IEEE

IIEEM Instituto de Ingenieros Electrónicos y Eléctricos de Morelos A.C

CIICAp

IEEE VTS

| Technical Session:<br>Computer Vision, Computational Intelligence and Human-Computer Interaction | |
|---|---|
| 11:10—11:30 | **Vortex Particle Swarm Optimization in 2D Cases**<br>Helbert Espitia and Jorge Sofrony. |
| 11:30—11:50 | **Customer authentication of digital imaging using hybrid watermarking**<br>Manuel Cedillo-Hernandez, Antonio Cedillo-Hernandez, Francisco Garcia-Ugalde, Carlos Aldair Roman-Balbuena, Mariko Nakano-Miyatake and Hector Perez-Meana. |
| 11:50—12:10 | **A block-wise deformation-based approach for facial expression recognition**<br>Fabiola M. Villalobos-Castaldi, Nicolás Kemper, Laura Ramirez-Sanchez and Esther Rojas-Krugger. |
| 12:10—12:30 | **An efficient content-based video retrieval for large databases**<br>Antonio Cedillo-Hernandez, Manuel Cedillo-Hernandez, , Francisco Garcia-Ugalde, Hector Perez-Meana and Mariko Nakano-Miyatake. |
| 12: 30—12:50 | **Comparative analysis of phase unwrapping in PSP using depth images**<br>Rodrigo Escobar Díaz Guerrreo, Juan Carlos Moya Morales, Juan Manuel Ramos Arreguin, José Emilio Vargas Soto and Jesús Carlos Pedraza Ortega. |
| 12:50—13:10 | **Four Level Wavelet Haar Transform Architecture for Feature Extraction.**<br>Roy Flores-Flores, J. Luis Tecpanecatl-Xihuitl, Ruth M. Aguilar-Ponce and Cesar Torres-Huitzil. |
| 13: 10—13:20 | **Coffee Break** |
| 13:20—13:40 | **Architecture for Real-Time Color Detection on Video Based on the Choquet Fuzzy Integral.**<br>Rosario Ramirez-Lugo, Omar G. Valenzuela-López, J. Luis Tecpanecatl-Xihuitl and Ruth M. Aguilar-Ponce. |
| 13:40—14:00 | **An Approach to Improve Mouth-State Detection to Support the ICAO Biometric Standard for Face Image Validation**<br>Salvador Coronel Castellanos, Ismael Solis Moreno, Jose A. Cantoral Ceballos, Rogelio Alvarez Vargas and Pedro L. Martinez Quintal. |
| 14:00—14:20 | **Image De-Noising Algorithm Based on Intersection Cortical Model and Median Filter**<br>Estela Ortiz Rangel, Manuel Mejía Lavalle, Dante Mújica Vargas and Gerardo Reyes. |
| 14:20—14:40 | **Dimensional Analysis of Geometric Figures through Computer Vision**<br>Marcio Silva |
| 14:40—15:00 | **Hybrid object detection vision-based applied on mobile robot navigation**<br>J-Guadalupe Velasquez, Miguel Granados-Contreras, Agustin Ramirez-Agundis and Francisco Aquino-Robledo. |

which are explained in detail as follows. General diagram of the proposed method is shown Fig. 1.

### A. Watermark Generation

The watermark generation is described as follows: **A)** Register into a database the following customer's identity data: name, an alphanumeric code called Federal Taxpayer's Registry (RFC), birth date, affiliation and a serial number given by the owner of the digital image. The above information is flexible and may be adapted according to the owner's requirements. **B)** Apply the message digest algorithm RIPEMD-160 [3], [4] to the customer's identity data in the previous step. Resulting data are denoted as *MD* and stored into the database.

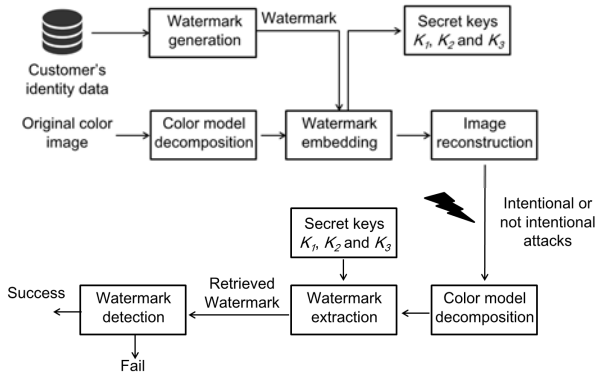



Figure 1. General diagram of the proposed watermarking method.

The proposed method may be easily adapted to the use of other message digest algorithm for example HAVAL [5]. **C)** Split the binary representation of *MD* into two blocks of 80 bits each one and apply an XOR operation between this two blocks, $W_m = bck_k \oplus bck_l$, where $m$, $k = 1, \ldots 80$ and $l = 81, \ldots 160$, *bck* denotes the *k-th* and the *l-th* bits from each block, respectively, and *W* corresponds to the result of the XOR operation. **D)** By its computation the resulting 80 bits are directly dependent on the customer's identity data. In order to preserve the trade-off between payload-robustness-imperceptibility, the payload *L* of the 1D watermark pattern *W* is adjusted from $L$=80 to $L$=64. This adjustment doesn't affects the performance of the proposed method.

### B. Watermark Embedding Process in the Frequency Domain

**1)** Read the original color image $I(x,y)$ and convert its representation from RGB to YCbCr color model space. And isolate the three components respectively. Reason to adopt YCbCr color model is: if the correlated color model such like RGB is used, the modification of one component independently to the others is not necessarily the best choice, because the perceived colors are dependant of the three components together. On the other hand, YCbCr allows obtaining non-correlated components and has the advantage of separating the luminance information from the chrominance information [6]. **2)** Rescale the component *Y* into a size of $N_1 \times N_2$, these dimensions will be stored and considered as a secret key $K_1$ in the detection stage. The resulting component is denoted by $Y_r(x,y)$. **3)** Apply the bi-dimensional DFT denoted as $F(u,v)$ to the component $Y_r(x,y)$ and obtain its magnitude $M(u,v)=|F(u,v)|$ and phase $P(u,v)$ components. **4)** Once the magnitude $M(u,v)$ has been centered, based on the energy distribution, select a pair of radius $r_1$ and $r_2$ around the zero frequency term in $M(u,v)$ and compute its corresponding annular area $A=\pi(r_2^2-r_1^2)$ that should cover a middle frequency band. In order to preserve the robustness respect to JPEG lossy compression and at the same time keep a high imperceptibility [6], [7], the goal then is to find the correct pair of $r_1$ and $r_2$. These radius values will be provided as a secret key $K_2$ in the detection stage. **5)** According to DFT symmetrical properties, it is considered the first and the second quadrants of the upper half part of $M(u,v)$ and it is computed the magnitude difference $d=M_i(u_j,v_j)-M_i(-u_j,v_j)$ into the area *A*, where $i=1,\ldots, L$ denotes an index pointing into the watermark data bits $W_i$, and *j* denotes the coordinates into $M(u,v)$. **6)** Considering a watermark gain factor $\alpha$, modify the middle frequencies coefficients $M'(u,v)$ as is shown Figs. 2 and 3. **7)** In order to produce real values after the DFT magnitude has been modified in the step **6)**, the lower half part of the corresponding middle frequency band should be modified as well in a symmetrical manner. The watermarked component $Y_W(x,y)$ is obtained applying the IDFT to the watermarked magnitude $M'(u,v)$ in conjunction with the corresponding preserved and non-altered original phase $P(u,v)$. Finally the watermarked component $Y_W(x,y)$ is rescaled to the original dimensions of color image.

$$
\begin{array}{l|l}
\textit{if } (W_i = 0) \,\&\, (d \geq -\alpha) \textit{ then} & \textit{if } (W_i = 1) \,\&\, (d \leq \alpha) \textit{ then} \\
\quad M_i'(u_j, v_j) = M_i(u_j, v_j) - (\alpha + d) & \quad M_i'(u_j, v_j) = M_i(u_j, v_j) + (\alpha - d) \\
\quad M_i'(-u_j, v_j) = M_i(-u_j, v_j) + (\alpha + d) & \quad M_i'(-u_j, v_j) = M_i(-u_j, v_j) - (\alpha - d) \\
\textit{end} & \textit{end}
\end{array}
$$

Figure 2. Pseudo-code of the embedding rules in frequency domain.

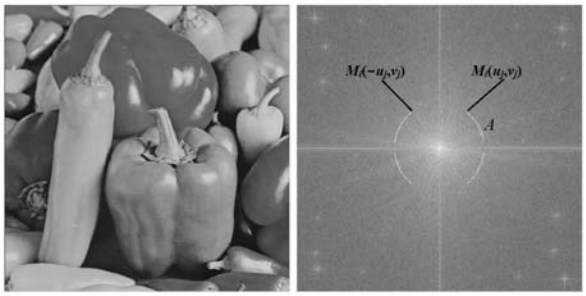



Figure 3. Modification in the frequency domain. a) Original component *Y* of color image. b) Watermarked DFT magnitude of a). For illustrative purposes a bigger value of the watermark gain factor $\alpha$ is used.

### C. Watermark Embedding Process in the Bi-Dimensional Histogram

**1)** Using the chrominance components *Cb*, *Cr*, compute a bi-dimensional color histogram denoted by *H*. **2)** Reshape the 1D watermark sequence *W* in a pattern $W_{rs}$ of size $L=Q_1 \times Q_2$ (where $Q_1$ and $Q_2$ are integers). **3)** Segment the

### A. *Watermark Imperceptibility*

Watermark imperceptibility has been evaluated in terms of the PSNR and SSIM [9] image quality metrics defined by (2) and (3), respectively.

$$PSNR = 10\log 10\left(\frac{Max\ Pixel\ Value}{(MSE_{Y_w} + MSE_{Cb_w} + MSE_{Cr_w})/3}\right), \quad (2)$$

$$SSIM(I_o, I_w) = \frac{(2\mu_{I_o}\mu_{I_w} + C_1)(2\sigma_{I_oI_w} + C_2)}{(\mu_{I_o}^2 + \mu_{I_w}^2 + C_1)(\sigma_{I_o}^2 + \sigma_{I_w}^2 + C_2)}. \quad (3)$$

where $I_o$, $I_w$ are the original and watermarked images, respectively, and $C_1$, $C_2$ are small constant values [9]. Fig. 5 shows (a) original and (b) watermarked color image. As shown in Figs. 6 and 7, a larger value of watermark gain factor $\alpha$ would increase the robustness of the watermark, but the watermark imperceptibility is affected.

To preserve the trade-off between robustness and imperceptibility, based on our experiments, we have considered a watermark gain factor of $\alpha$ = 15000 as a suitable value.


Figure 5. (a) Original and (b) Watermarked test image.

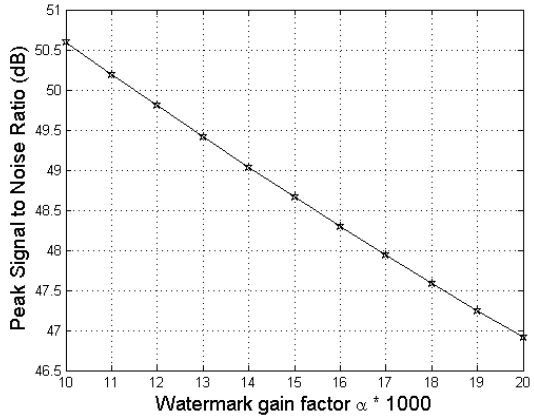



Figure 6. Average PSNR (dB) obtained with variable $\alpha$.

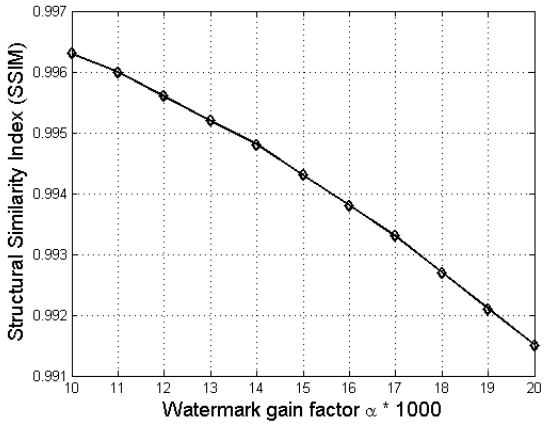



Figure 7. Average SSIM obtained with variable $\alpha$.

### B. *Watermarking Robustness*

To evaluate the watermark robustness of the proposed algorithm, experimental results are classified in geometric, signal processing and combined distortions, as shown in Table 1. In Figs. 8, 9 and 10 shows the average BER of the proposed watermarking method. The detection results are plotted in HT and DFT forms, where HT is the reference to the bi-dimensional histogram modification detector output, and DFT corresponds to the frequency domain detector output. As shown in Fig. 8, the HT detector output get the better performance against geometric distortions with respect to DFT detector output, because, meanwhile the DFT domain presents robustness against Rotation, Scaling and Translation (RST) and cropping attacks, the bi-dimensional histogram domain presents robustness against more geometric distortions such as affine and projective transformations. However, as shown in Figs. 9 and 10, the DFT detector output obtains better performance against signal processing distortions including JPEG compression, enhanced image, adding noise, filtering and combined attacks, respect to HT detector output.

[4] A. Bosselaers, H. Dobbertin,H. and B. Preneel, “The RIPEMD-160 cryptographic hash function”, *Dr.Dobb’s J.*, January 1997, vol. 22, no. 1, pp. 24–28.

[5] Schneier, B., *Applied Cryptography*, 2nd edn. Wiley, New York, 1996

[6] M. Cedillo-Hernández, F. García-Ugalde, M. Nakano-Miyatake, M. and H. Pérez-Meana, “Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification”, *Signal, Image and Video Processing*, 2014, vol. 8, no.1, pp. 49-63

[7] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake and H. Perez-Meana, “Robust digital image watermarking using interest points and DFT domain”, *35th International Conference on Telecommunications and Signal Processing (TSP)*, July 2012, pp. 715-719

[8] C.W. Tang and H.M. Hang, “A feature-based robust digital image watermarking scheme”, *IEEE Trans. Signal Process*, 2003, vol. 51, no. 4, pp. 950–959

[9] Z. Wang, A.C. Bovik, H.R. Sheikh and E.P. Simoncelli, “Image quality assessment: From error measurement to structural similarity”, *IEEE Trans. Image Process*, 2004, vol. 13, no.4, pp.600–612

[10] E. Chrysochos, V. Fotopoulos, M. Xenos and A.N. Skodras, “Hybrid watermarking based on chaos and histogram modification”, *Signal Image Video Process*, 2012, doi:10.1007/s11760-012-0307-3

[11] S. Roy and E.C. Chang, “Watermarking color histogram”, *in Proceedings of IEEE International Conference on Image Processing*, Singapore, 2004, pp. 2191–2194

[12] J. Xiaolin, Q. Yanli, S. Liping and J. Xiaobo, “An anti-geometric digital watermark algorithm based on histogram grouping and fault tolerance channel”, *Intelligent Science and Intelligent Data Engineering, Lecture Notes in Computer Science*, 2012, doi:10.1007/978-3-642-31919-8_96

# Anexo B

# Imágenes Utilizadas

Los experimentos realizados en el esquema propuesto hacen uso de imágenes de con diferente contenido y dimensiones de 1024x768, 800x600 y 512x512 píxeles, todas con una resolución de 24 bits/píxel.. Algunas de estas imágenes se muestran en este anexo y fueron elegidas por ser utilizadas frecuentemente en el área de procesamiento digital de imágenes, y porque visualmente presentan diferentes criterios de complejidad.

Airplane

Peppers

Car

House

Lena

Tifanny

Mandrill

Lake

Tree