**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**
PROGRAMA DE POSGRADO EN CIENCIA E INGENIERIA DE LA COMPUTACIÓN

# MARCADO DE AGUA ROBUSTO EN IMÁGENES DIGITALES PARA PROTEGER LOS DERECHOS DE AUTOR Y AUTENTICACIÓN DE CONTENIDO

**TESIS**
QUE PARA OPTAR POR EL GRADO DE
DOCTORA EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

PRESENTA:
**LAURA JOSEFINA REYES RUIZ**

TUTOR PRINCIPAL
DR. FRANCISCO JAVIER GARCÍA UGALDE
FACULTAD DE INGENIERÍA

MIEMBROS DEL COMITÉ TUTOR
DRA. MARÍA ELENA MARTÍNEZ PÉREZ, INSTITUTO DE INVESTIGACIONES EN MATEMÁTICAS APLICADAS Y EN SISTEMAS
DRA. MARIKO NAKANO MIYATAKE, ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA, UNIDAD CULHUACÁN

CIUDAD UNIVERSITARIA, CD. MX., MAYO 2023

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

**UNAM – Dirección General de Bibliotecas**
**Tesis Digitales**
**Restricciones de uso**

**DERECHOS RESERVADOS ©**
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

# Agradecimientos

Ante todo, agradezco a Dios por brindarme los medios para realizar este trabajo y por las bendiciones que me otorga diariamente.

Mi más sincera gratitud al Dr. Francisco Javier García Ugalde, por su orientación, gran dedicación y enorme apoyo en la realización del presente trabajo de investigación; sin su invaluable ayuda y seguimiento alcanzar este logro no hubiera sido posible.

De la misma manera quiero agradecer a las doctoras Mariko Nakano Miyatake y María Elena Martínez Pérez por el apoyo brindado durante el desarrollo de esta tesis como miembros de mi Comité Tutoral. También a los doctores Oswaldo Ulises Juárez Sandoval y Eduardo Fragoso Navarro por su colaboración en el grupo de trabajo. Así como a la doctora María del Pilar Ángeles por su invaluable apoyo en la revisión del inglés en las publicaciones. De manera especial, agradezco al Dr. Manuel Cedillo Hernández quien hizo aportaciones importantes para que el artículo finalmente fuera publicado.

A mis padres quienes me soportan diariamente, al resto mi familia, a mis amigos y a todas las personas que me han acompañado en este trayecto, por el apoyo que me han brindado.

Esta investigación fue realizada en parte gracias al Programa de Apoyo a Proyectos de Investigación e Innovación Tecnológica (PAPIIT IT-100123) de la UNAM “Marcado de agua robusto en imágenes digitales para proteger los derechos de autor y autenticación de contenido”. Por lo cual agradezco a la DGAPA-UNAM la beca recibida.

Asimismo, agradezco a la Filmoteca de la UNAM por facilitarme las imágenes empleadas para la realización de la presente investigación.

Por último, doy gracias al Consejo Nacional de Ciencia y Tecnología (CONACYT) por el apoyo económico otorgado durante mis estudios de doctorado.

# Acrónimos

| | | |
|---|---|---|
| AV | Atención Visual | *Visual Attention* |
| BER | Relación de Bits Erróneos | *Bit Error Rate* |
| BMP | Imagen de Mapa de Bits | *Bit Mapped Picture* |
| BCR | Relación de Bits Correctos | *Cit Correct Rate* |
| DCI | Iniciativas de Cine Digital | *Digital Cinema Initiatives* |
| DRM | Gestión de los Derechos Digitales | *Digital Rights Management* |
| DCT | Transformada Coseno Discreta | *Discrete Cosine Transform* |
| DFT | Transformada Discreta de Fourier | *Discrete Fourier Transform* |
| DWT | Transformada Wavelet Discreta | *Discrete Wavelet Transform* |
| ED | Distancia Euclidiana | *Euclidean Distance* |
| EV | Valores de Exposición | *Exposure Values* |
| FRC | Control de Velocidad de Fotogramas | *Frame Rate Control* |
| GIF | Formato de Gráficos Intercambiable | *Graphics Interchange Format* |
| HD | Distancia de Hamming | *Hamming Distance* |
| HDR | Alto Rango dinámico | *High Dynamic Range* |
| ICO | Ícono | *Icon* |
| IVW | Marca de Agua Imperceptible Visible | *Imperceptible-Visible Watermarking* |
| JPEG | Conjunto de Grupo de Expertos en Fotografía | *Joint Photographic Expert Group* |
| LSB | Bit Menos Significativo | *Least Significant Bit* |
| MSE | Error del Cuadrado de las Medias | *Mean Squared Error* |
| NC | Correlación Normalizada | *Normalized Correlation* |
| ODG | Gráfico de Documento Abierto | *Open Document Graphic* |
| PSO | Optimización con Enjambre de Partículas | *Particle Swarm Optimization* |
| PSNR | Relación Señal Pico a Ruido | *Peak Signal to Noise Ratio* |
| PNG | Gráficos de Red Portátiles | *Portable Network Graphics* |
| ROI | Región de Interés | *Region of Interest* |
| SSIM | Índice de Semejanza Estructural | *Structural Similarity Index Measure* |
| TIFF | Formato de Archivo de Imagen Etiquetado | *Tagged Image File Format* |
| TV-L1 | Modelo de Variación Total | *Total Variation model* |
| UHD | Ultra Alta Definición | *Ultra High Definition* |
| UVW | Marca de Agua Inadvertida Visible | *Unseen-Visible Watermarking* |
| VQ | Cuantización Vectorial | *Vector Quantization* |
| VIF | Fidelidad de Información Visual | *Visual Information Fidelity* |
| WMF | Meta Archivo de Windows | *Windows Meta File* |

# *Índice*

**Índice** ..... 5
1. Introducción ..... 10
1.1. Marca de agua y por qué usarla ..... 10
1.2. Hipótesis ..... 12
1.3. Objetivos ..... 12
1.4. Organización de la tesis ..... 13
2. Marco teórico y antecedentes ..... 14
2.1. Imágenes digitales ..... 14
2.1.1. Formatos de imágenes digitales ..... 14
2.1.2. Resolución de imágenes ..... 15
2.2. Criptografía, esteganografía y marca de agua ..... 18
2.3. Parámetros del marcado de agua ..... 20
2.4. Clasificación de las técnicas de marcado de agua ..... 21
2.5. Digitalización y transformación digital [9] ..... 23
2.6. Ataques informáticos ..... 23
2.7. Aplicaciones de la marca de agua ..... 26
2.8. Métricas de desempeño de los algoritmos de marcado ..... 27
2.8.1. Robustez ..... 27
2.8.2. Imperceptibilidad ..... 28
2.9. Marca de agua visible ..... 32
2.9.1. Descomposición estructura-textura (*cartoon-texture*) ..... 32
2.9.2. Región de interés (ROI) ..... 34
2.9.3. Súper píxeles (SP) ..... 37
2.10. Marca de agua invisible ..... 41
2.10.1. El método RIPEMD-160 ..... 41
2.10.2. Optimización con un método de enjambre de partículas (PSO). ..... 44
2.11. Protección de la autoría. ..... 45
2.12. Patrimonio cultural ..... 47
3. Algoritmo propuesto ..... 49
3.1. Planteamiento del problema ..... 49
3.2. Parámetros de entrada ..... 50

3.3. Marcado dual ..... 53
3.3.1. Marcado visible ..... 54
3.3.2. Marcado de agua invisible ..... 65
3.3.3. Inspección / Extracción ..... 67
4. Resultados experimentales ..... 69
4.1. Imperceptibilidad ..... 73
4.2. Robustez ..... 74
4.3. Trabajos relacionados ..... 79
5. Conclusiones ..... 81
ANEXO: Publicaciones y participaciones ..... 83
Referencias ..... 86

# Índice de Tablas

Tabla 2.1 Resolución de televisores de pantalla grande. ..... 17
Tabla 2.2 Tipos de HDR en pantallas. ..... 18
Tabla 3.1. Parámetros numéricos para toda $i$ dentro del área de atención visual. ..... 61
Tabla 3.2. Distorsiones consideradas en la función de aptitud objetiva del algoritmo PSO. ..... 67
Tabla 4.1 Encuesta de imperceptibilidad de marca de agua visible. ..... 73
Tabla 4.2. Valores medios de PSNR, SSIM Y VIF ..... 74
Tabla 4.3 Ataques de impresión-escaneo Figura 4.7. ..... 75
Tabla 4.4 Ataques de impresión-escaneo Figura 4.2. ..... 77
Tabla 4.5 Valores promedio de BCT a las distorsiones geométricas. ..... 78
Tabla 4.6 Valores promedio de BCR al procesamiento de señal. ..... 78
Tabla 4.7 Valores promedio de BCR para distorsiones combinadas. ..... 79
Tabla 4.8 Comparación con otros algoritmos de marca de agua dual. ..... 80

# Índice de Figuras

Figura 1.1 Esquema general del marcado de agua en imágenes. ..... 11
Figura 2.1 Comparación de diferentes resoluciones de imagen. ..... 16
Figura 2.2 Comparación entre resolución estática (izquierda) y dinámica (derecha). ..... 16
Figura 2.3 Esquema general de un sistema de encriptación. ..... 19
Figura 2.4 Esquema general de un sistema esteganográfico. ..... 19
Figura 2.5 Esquema general del marcado de agua como sistema de comunicación. ..... 20
Figura 2.6 Clasificación de las técnicas de marcado ..... 21
Figura 2.7 Efectos del ataque impresión-escaneo. (a) Imagen original, (b) histograma original, (c) imagen impresa y escaneada, (d) histograma resultante [12]. ..... 25
Figura 2.8 La información mutua entre C y E cuantifica la información que el cerebro idealmente podría extraer de la imagen de referencia, mientras que la información mutua entre C y F cuantifica la información correspondiente que podría extraerse de la imagen de prueba. [14]..... 31
Figura 2.9 Mapas de saliencia de una imagen de “Pueblito” (23,887) ..... 36
Figura 2.10 Mapas de saliencia de una imagen de “Pueblito” (23,887) reducida. ..... 37
Figura 2.11 Atención visual $\sigma = 8$, a) de la Figura 2.9 y b) de la Figura 2.10. ..... 37
Figura 2.12 Superpíxeles SLIC, con 100 iteraciones y diferentes compacidades $C$. ..... 38
Figura 2.13 Imagen dividida con SLIC en 3403, 232 y 24 superpíxeles. ..... 39
Figura 2.14 Cuadrícula inicial (izquierda) y Rango de búsqueda del SLIC (derecha) ..... 40
Figura 2.15 Superpíxeles SLIC en las iteraciones 2, 4, 6, 8 y 10. ..... 41
Figura 2.16 Ejemplo de la aplicación del método RIPEMD-160. ..... 42
Figura 2.17 Diagrama general de la optimización por el método de enjambre de partículas. ..... 44
Figura 3.1 Diagrama general del algoritmo propuesto. ..... 49
Figura 3.2 Imágenes de muestra del conjunto de datos. (a) Imagen obtenida de la película “Dos monjes”, (b) Imagen obtenida de la película “La mancha de sangre”, 1937, (c) Imagen obtenida de la película “Redes”, 1936, y (d) Imagen obtenida de “Vamonos con Pancho Villa”, película de 1936 (los títulos de las películas están entre comillas y en español). Utilizando un conjunto de datos Fotografías cortesía de Filmoteca, propiedad de Filmoteca UNAM. ..... 50
Figura 3.3 $\boldsymbol{Io}$ Imagen familia inuit. ..... 51
Figura 3.4 Marca binaria $\boldsymbol{W1o}$. ..... 51
Figura 3.5 Marcas de agua binarias cuadradas, tamaño $n \times n = 250 \times 250$ píxeles con fondo blanco (línea superior) y marcas de agua binarias cuadradas, tamaño $n \times n = 21 \times 21$ píxeles con fondo negro (línea inferior). De izquierda a derecha escudo UNAM (a y e), logos de Difusión Cultural (b,f,c, yg) y logo de Filmoteca (d y h). Las imágenes son propiedad de la UNAM. ..... 52
Figura 3.6 Diagrama de bloques del método híbrido de doble marca de agua propuesto. ..... 53
Figura 3.7 Diagrama de bloques del marcado visible camuflado. ..... 54
Figura 3.8 Imagen de estructura $Ie$. ..... 55
Figura 3.9 Imagen de textura $It$ ..... 55
Figura 3.10 Imagen de textura binarizada $\boldsymbol{Itbin}$. ..... 56
Figura 3.11 Mapa de saliencia $AVm$. ..... 57
Figura 3.12 Máscara de atención visual $\boldsymbol{AVmbin}$. ..... 57

Figura 3.13 Pixeles de estructura dentro del área de atención visual $\boldsymbol{IeAV}$. ..... 58
Figura 3.14 Pixeles de textura dentro del área de atención visual $\boldsymbol{ItAV}$..... 59
Figura 3.15 Máscara de súper pixeles $\boldsymbol{SPm}$..... 60
Figura 3.16 $\boldsymbol{IeAV}$ dividida en súper pixeles, $\boldsymbol{SPeAV}$. ..... 60
Figura 3.17 $\boldsymbol{ItAV}$ dividida en súper pixeles, $\boldsymbol{SPtAV}$. ..... 61
Figura 3.18 Súper Pixel elegido..... 63
Figura 3.19 Complemento de $Wo$. ..... 63
Figura 3.20 Imagen marcada $Iw$ y marca incrustada ampliada. ..... 64
Figura 3.21 Llave secreta $K1$. ..... 65
Figura 3.22 Diagrama de bloques del marcado de agua invisible. ..... 65
Figura 3.23 Parámetros en dominio de marca de agua invisible basado en DFT 2D. ..... 66
Figura 4.1 Imágenes originales (1ra columna), Área de atención visual $IeAV$ correspondiente al segundo paso (2da columna), Segmentación aplicando $SPm$ correspondiente al tercer paso (3ra columna) y región de incrustación seleccionada correspondiente al cuarto paso (4ta columna). Fotografías de primera y segunda fila de la película “Redes”, y fotografía de la fila inferior de “El compadre Mendoza” (los títulos de las películas están entre comillas y en español). Las fotografías usadas son cortesía de Filmoteca y propiedad de Filmoteca UNAM..... 69
Figura 4.2 Imágenes con marca de agua, utilizando una fotografía de la película “Vámonos con Pancho Villa”, cortesía de Filmoteca, propiedad de Filmoteca UNAM. ..... 70
Figura 4.3 Selección del segundo (amarillo) y tercer (rojo) SP. ..... 71
Figura 4.4 Marcas incrustadas, segundo SP a la izquierda y tercer SP a la derecha. ..... 71
Figura 4.5 Imagen con dos marcas visibles camufladas. ..... 72
Figura 4.6 Imagen con múltiples marcas camufladas, utilizando una fotografía de la película “Vámonos con Pancho Villa”, cortesía de Filmoteca, propiedad de Filmoteca UNAM. ..... 72
Figura 4.7. Marca original (a) y atacadas (b-ar), imagen inuit. ..... 75
Figura 4.8. Marca original (a) y fotografiadas (b-c), imagen inuit. ..... 76
Figura 4.9 Marcas de agua extraídas de la imagen que se muestra en la Figura 4.2 (a) Marca de agua sin ataques y (b-ac) marcas de agua atacadas. ..... 76

# 1. Introducción

"La memoria más fuerte será aquella basada en imágenes".
–Ramón Campayo

En este capítulo se presenta un panorama general del trabajo investigación realizado dentro del área del marcado de agua en imágenes digitales.

## 1.1. Marca de agua y por qué usarla

En esta sección se proporciona una descripción general de la marca de agua aplicada a imágenes digitales: se enlistan algunos términos estándar básicos del marcado de agua, las propiedades de la marca de agua y sus aplicaciones. Una explicación más detallada de estos temas se proporciona en el Capítulo 2. También se expone la motivación del presente trabajo de investigación.

*Términos estándar* empleados en el marcado de agua digital:

- **Ima**ge**n Portadora** (*Cover image*). Es la imagen original usada en el marcado de agua. También llamada imagen original.
- **Imagen marcada**. Es la imagen portadora después de la incrustación de la marca.
- **Marca**. Puede ser una señal simple que consiste en una secuencia pseudoaleatoria, una imagen o un mensaje de varios bits codificados en un dominio de transformación.
- **Incrustación**. También conocido como proceso de marcado, es el proceso en el que se introduce la marca en la imagen portadora.
- **Extracción**. Es el proceso en el que la marca se recupera a partir de la imagen marcada. Este proceso puede ser simplemente de revelado o identificación visual.
- **Esquema del (algoritmo/sistema de) marcado**. Elemento gráfico que representa tanto el proceso de incrustación y de extracción. En la Figura 1.1 se observa el más simplificado de los esquemas de marcado.

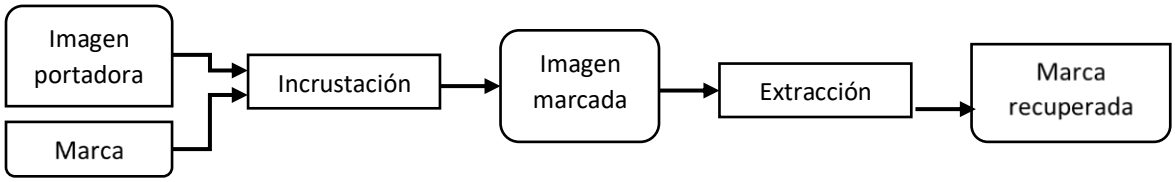



*Figura 1.1 Esquema general del marcado de agua en imágenes.*

- **Ataques o distorsiones**. Son los cambios sufridos por la imagen marcada. Éstos pueden ser no intencionales, como la compresión JPEG, el cambio de formato, o procesamiento de imagen común como el cambio en el nivel de brillo, o el aumento de nitidez; o intencionales como las operaciones geométricas y de recorte. Aunque también se les denomina ataques no necesariamente se refieren a intenciones maliciosas.

Las *propiedades* fundamentales de una marca de agua digital son las siguientes:

- **Robustez**. Se refiere a su capacidad para soportar distorsiones o ataques.
- **La carga útil de datos (*payload*)**. Es el tamaño del mensaje embebido, es decir, el tamaño de una marca de agua incrustada. Se puede expresar en porcentaje, respecto al tamaño de la imagen.
- **Capacidad**. Es la cantidad de información de marca de agua en una imagen. Si se incorporan varias marcas de agua en una imagen, la capacidad de la marca de agua de la imagen es la suma de la carga útil de datos de todas las marcas de agua individuales.
- **Imperceptibilidad**. Es la característica de ocultar la marca de agua para no degradar la calidad visual de la imagen portadora.
- **Costo computacional**. Es la medida de los recursos computacionales requeridos para llevar a cabo la incrustación o extracción de la marca. Se puede medir usando el tiempo de procesamiento para una configuración de computadora dada.

La marca de agua se puede usar para diversas *aplicaciones* de protección, dentro de los cuales se encuentran [1]:

- Prueba de la Propiedad intelectual.
- Copyright.
- Rastreo de copias (*fingerprinting*).
- Autenticación de contenido.

Otras *aplicaciones* relacionadas pueden ser:

- Entrega de información.
- Indexación.
- Seguridad médica.
- Ocultamiento de datos.

Los rápidos avances tecnológicos, el abaratamiento de dispositivos y la gran difusión de los medios digitales plantean grandes retos para la demostración de Propiedad y las leyes de Propiedad intelectual debido a que facilitan la creación, modificación y distribución de documentos digitales. Esto a su vez ha provocado que los medios digitales tengan considerable impacto en la sociedad actual y en la cultura.

La gestión de derechos digitales, DRM por sus siglas en inglés, se ha vuelto un área de investigación muy activa para solventar los desafíos actuales para la protección de los archivos digitales. El presente trabajo se centra en la protección de imágenes en tonos de gris, cuyas características particulares se describen en el siguiente capítulo.

## 1.2. Hipótesis

Es posible desarrollar un algoritmo específico de marcado dual (una marca visible camuflada y una invisible) que sea lo suficientemente robusto para resistir el ataque de impresión-escaneo, para proteger las imágenes digitalizadas (fotografías y posters) de las películas de la época de oro del cine mexicano (facilitadas por la Filmoteca de la UNAM).

## 1.3. Objetivos

Dado el crecimiento de los medios digitales, la mayoría de los sistemas de marcado de agua digital existentes fallarían ante un ataque de impresión y escaneo (*print-scan attack*) [2], el objetivo principal del algoritmo propuesto en esta investigación es ser robusto respecto a este tipo de ataque, para asegurar el buen uso de imágenes del patrimonio cinematográfico mexicano.

La marca de agua visible que se presenta debe ser imperceptible a simple vista por cualquiera que desconozca su existencia para evitar ataques directos dirigidos a marcas visibles, debido a que dentro de los usos que se otorgan a terceros de las imágenes del patrimonio cultural se incluyen las reimpresiones.

Fortalecer el algoritmo de marcado propuesto mediante una marca de agua invisible en el dominio de la frecuencia, que aporte datos adicionales, como información acerca del propietario de la imagen y/o del concesionario. Obteniendo de esta manera una marca de agua dual, o híbrida.

## 1.4. Organización de la tesis

Las partes restantes de esta tesis están organizadas de la siguiente manera. En el capítulo 2 se enumeran y explican los principales conceptos y herramientas utilizadas en el marcado de agua en imágenes digitales y en el desarrollo del algoritmo propuesto.

En el capítulo 3 se describe el algoritmo propuesto, mostrando visualmente el desarrollo con una imagen de prueba.

En el capítulo 4 se presentan los resultados obtenidos de la base de datos usada, la resistencia de la marca a los ataques y comparación del desempeño del algoritmo propuesto con otros similares.

Finalmente, en el capítulo 5 presentamos algunos comentarios finales y sugerimos varias direcciones de trabajo futuras para ampliar este trabajo de tesis.

# 2. Marco teórico y antecedentes

## 2.1. Imágenes digitales

Una imagen digital o gráfico digital es un arreglo bidimensional para preservar la información de una imagen a partir de una matriz numérica.

### 2.1.1. Formatos de imágenes digitales

Las imágenes digitales se pueden almacenar en diversos formatos, cambiar de uno a otro es muy común dependiendo del uso que se le quiera dar a la imagen. A continuación, se listan algunos de los formatos más importantes de imágenes digitales más usados.

- JPEG ("*Joint Photographic Expert Group*"): es un sistema de compresión de imágenes, cuyo uso es muy extendido en Internet y presenta una pérdida mínima de resolución.
- PNG ("*Portable Network Graphics*"): emplea algoritmos de compresión y permite transparencias.
- GIF ("*Graphics Interchange Format*"): permite hasta 256 colores y capas para animaciones.
- BMP ("*BitMaP*"): soporta 24 bits (16.7 millones de colores, por lo que la capacidad de los archivos es muy elevada). El mapa de bits es el formato más utilizado en informática.
- TIFF ("*Tagged Image File Format*"): maneja los datos de las imágenes combinadas con etiquetas.
- ODG ("*Open Document Graphic*"): imagen generada con la suite *OpenOffice* o *StarOffice*.
- WMF ("*Windows Meta File*"): formato de imágenes de Microsoft® basado en sistema vectorial.
- ICO ("*Icon*"): imágenes pequeñas de uso común para el entorno de *Microsoft® Windows* y *Microsoft® Internet Explorer* 8. [1]

[1] https://es.wikipedia.org/wiki/Imagen_digital

Los formatos de imágenes digitales, en su gran mayoría, poseen una cabecera que comprende algunos atributos (tipo de codificación, dimensiones de la imagen, etc.), generalmente es seguida de los datos de la imagen. Cada formato posee una estructura particular de los atributos y de los datos de la imagen.

## *2.1.2. Resolución de imágenes*

En general la resolución de una imagen es una indicación de la cantidad de detalles que puede observarse en la misma. La resolución de la imagen determina si ésta es estática o dinámica, en el primer caso se trata de una imagen matricial (en las que se centra el presente trabajo), en el segundo caso se trata de un gráfico vectorial.

**Resolución estática**

Una imagen con resolución estática o imagen matricial (rasterizado), pierde calidad cuando se despliega ampliada como se puede observar en la Figura 2.2 Existen dos convenciones muy aceptadas y de uso extendido acerca de la resolución estática de una imagen:

- La primera es describir la resolución con dos números enteros, donde el primero es la cantidad de columnas de pixeles y el segundo la cantidad de renglones de pixeles.
- La segunda es describir el número total de píxeles en la imagen.

"Técnicamente hablando, 4K representa una resolución horizontal de 4,096 pixeles, establecida por *Digital Cinema Initiatives* (DCI). No todas las películas tienen la misma proporción de imagen; por lo que no se especifica la resolución vertical de la forma del rectángulo en la pantalla" [1].

La Figura 2.1 muestra el número relativo de pixeles en cada una de las resoluciones más populares, cabe mencionar que esta figura no es una representación visual exacta. "De mayor a menor: 4K Cinema, en proporción 1.78:1 (negro); UHD (blanco); 2K Cinema, en proporción 1.78:1 (verde); Full HD 1080p (rojo); 720p (azul)" [1].

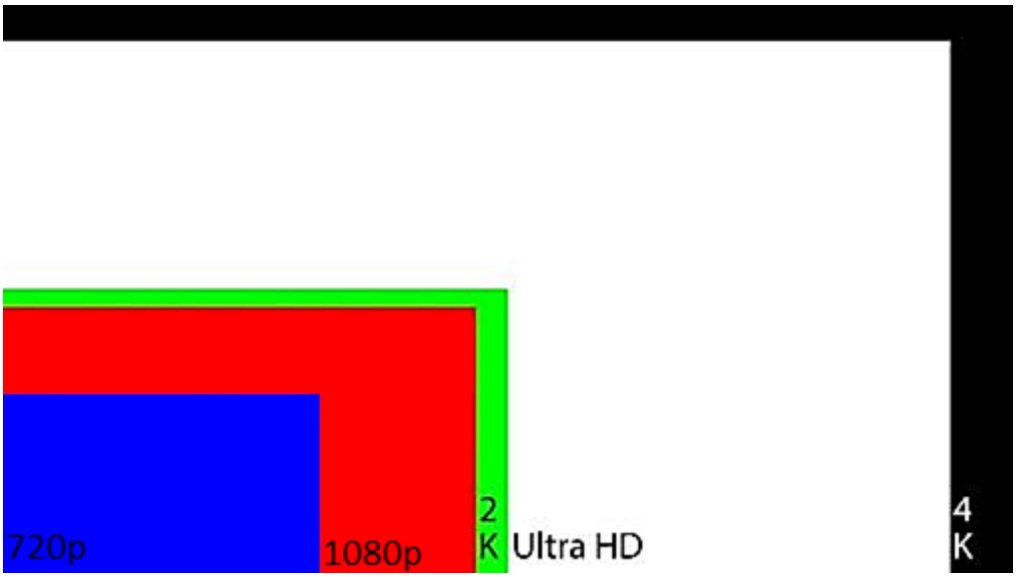



*Figura 2.1 Comparación de diferentes resoluciones de imagen.*[2]

**Resolución dinámica**

Una imagen vectorial con resolución dinámica está formada por objetos geométricos dependientes, cada uno de los cuales está definido por atributos matemáticos. Su ventaja principal radica en que puede ampliarse sin sufrir pérdida de calidad como se puede apreciar en la Figura 2.2.

*Figura 2.2 Comparación entre resolución estática (izquierda) y dinámica (derecha).*[3]

[2] https://www.cnet.com/es/noticias/1080p-2k-uhd-4k-8k-que-significan-resolucion-televisores/
[3] https://kevurugames.com/blog/vector-vs-raster-graphics-the-complete-guide-to-pros-cons-and-applications/

Los dispositivos electrónicos como los televisores listados en la Tabla 2.1, los monitores de computadora, celulares, etc. Convierten las imágenes vectoriales a imágenes rasterizadas (mapa de bits) para su despliegue.

*Tabla 2.1 Resolución de televisores de pantalla grande.*[4]

| Nombre de resolución | Pixeles Horizontales x Verticales | Otros nombres | Dispositivos |
|---|---|---|---|
| 8K | 7,680 x 4,320 | ninguno | Televisores conceptuales |
| "Cinema" 4K | 4,096 x [sin especificar] | 4K | Proyectores |
| UHD | 3,840 x 2,160 | 4K, Ultra HD, Definición Ultra Alta | Televisores |
| 2K | 2,048 x [sin especificar] | ninguno | Proyectores |
| WUXGA | 1,920 x 1,200 | Widescreen Ultra Extended Graphics Array | Monitores, proyectores |

**Alto rango dinámico HDR**

El Alto Rango Dinámico, HDR por sus siglas en inglés (*High Dynamic Range)*, es un concepto que se originó en el ámbito fotográfico, se refiere a un conjunto de técnicas que facilitan una mejora en el *rango dinámico de luminancias* entre los sectores más claros y los más oscuros de una imagen [2].

El HDR fue creado en la década de los 30, por el fotoquímico estadounidense Charles Wales Wyckoff, con el objetivo de que sus fotografías poseyeran un mayor rango dinámico al existente en ese momento [2].

Una fotografía en HDR, produce una imagen muy parecida a la captada por el ojo humano, debido a que tienen una diferencia más acentuada de iluminación por zona que otros formatos. La adaptación constante del ojo humano al rango lumínico del entorno, favorece que las personas vean las múltiples variantes de las condiciones de luz [2].

Las imágenes en HDR pueden representar con mayor fidelidad las intensidades de luz del mundo real gracias a su rango dinámico amplio. El rango dinámico se mide empleando los diferentes valores de exposición (EV) entre las zonas más claras y las más oscuras de la imagen, cada aumento del EV provoca un incremento de la cantidad de luz. Una imagen en HDR, generalmente se obtiene combinando varias fotos tradicionales usando la técnica llamada *bracketing* [2].

El rango dinámico de un televisor depende de la diferencia de la intensidad entre las zonas más oscuras y las más iluminadas de las imágenes. El brillo que es capaz de ofrecernos el televisor no es el único factor que afecta el rango dinámico, también el

[4] Ídem

número de niveles de luminosidad con diferente intensidad que consigue reproducir. Entre mayor sea el número de niveles del televisor más información será capaz de recuperar, tanto en las zonas oscuras como en las zonas luminosas [3].

La calidad de un televisor HDR depende de tres factores: su capacidad de entrega de brillo, su relación de contraste y el espacio de color que es capaz de reproducir. Por ejemplo, un panel de 8 bits puede reproducir 256 tonos y los televisores que los utilizan son capaces de reproducir hasta 16.7 millones de colores diferentes. Los paneles de 10 bits son capaces de reproducir cada color básico en 1,024 tonos distintos y logran representar un espacio de aproximadamente 1,073 millones de tonos diferentes [3]. En la Tabla *2.2* se listan los tipos de pantalla existentes que utilizan HDR, así como su profundidad de color y el tipo de licencia.

Sin embargo, existe una técnica que puede simular una reproducción del color más amplia en los paneles de 8 bits. Mediante un procesado que utiliza técnicas FRC (*Frame Rate Control*) se puede simular un espacio de color más amplio manipulando píxeles adyacentes de colores diferentes para provocar la sensación de que estamos viendo un tercer color que, en realidad, no forma parte del espacio de color original del panel de 8 bits [3].

*Tabla* 2.2 Tipos *de HDR en pantallas.*

| Tipo | Profundidad de color | Tipo de estándar |
|---|---|---|
| HDR10 | 10 bits | Abierto |
| HDR10+ | 10 bits | Abierto |
| Dolby Vision | 12 bits | Propietario |

## 2.2. Criptografía, esteganografía y marca de agua

Por la seguridad que aportan, estas tres disciplinas están estrechamente relacionadas, ya que son parte de los procesos de protección de la información y pueden utilizarse combinadas. Los esquemas mostrados a continuación son generales por lo que pueden presentar variantes.

**Criptografía**

La criptografía es la técnica y el arte de crear mensajes codificados con procedimientos o claves secretas con el objeto de que no pueda ser descifrado salvo por

la persona a quien está dirigido o que conozca la clave, para garantizar que terceras personas no puedan conocer el contenido del mensaje cifrado.

El objetivo es convertir el mensaje (texto en claro) en algo ininteligible sin la llave de cifrado (texto cifrado). No se ocupa de ocultar el envío del mensaje en sí. Una vez desencriptado el mensaje pierde toda protección. En la *Figura 2.3* se muestra el esquema general que representa un sistema de encriptación.

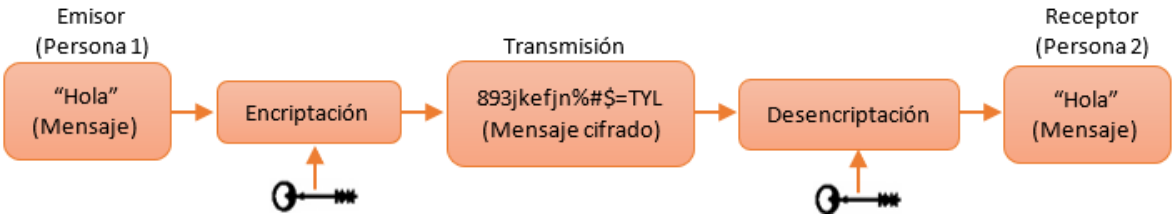



*Figura 2.3 Esquema general de un sistema de encriptación.*

**Esteganografía**

La esteganografía es la aplicación de técnicas que permiten ocultar mensajes dentro de otros llamados portadores o cubiertas para ser enviados de modo que pase desapercibida la existencia del mensaje oculto. La no distorsión de la portadora no es ninguna prioridad para esta disciplina. En la *Figura 2.4* se muestra el esquema general que representa un sistema de esteganográfico.

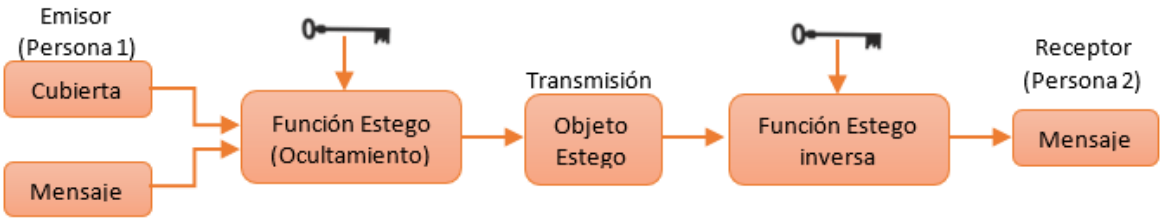



*Figura 2.4 Esquema general de un sistema esteganográfico.*

**Marca de agua digital**

Como en los billetes de banco, sólo que ahora de manera digital, la marca de agua (*digital watermarking*) es la aplicación de técnicas para incrustar una marca a una señal portadora, dando prioridad a la preservación de la señal portadora tratando de causarle la menor distorsión posible.

Al igual que las marcas de agua físicas tradicionales, las marcas de agua digitales a menudo solo son perceptibles bajo ciertas condiciones [4].

El marcado de agua visto como un sistema de comunicación consiste principalmente de tres partes: Transmisor, canal y receptor [5].

En el esquema de la *Figura* 2.5 se muestran los elementos básicos del sistema de marcado de agua, en este esquema las flechas punteadas indican que dicho elemento es prescindible. $M$ es la marca, $P$ es la señal portadora sin marcar, $P_M$ es la señal marcada, $P'_M$ es la señal marcada después de haber sido atacada) ya sea de manera intencional, o no intencional), $M'$ es la marca recuperada después de los ataques y $K_1$ es una llave, o clave, que puede usarse para la incrustación y/o la extracción/revelado de la marca.

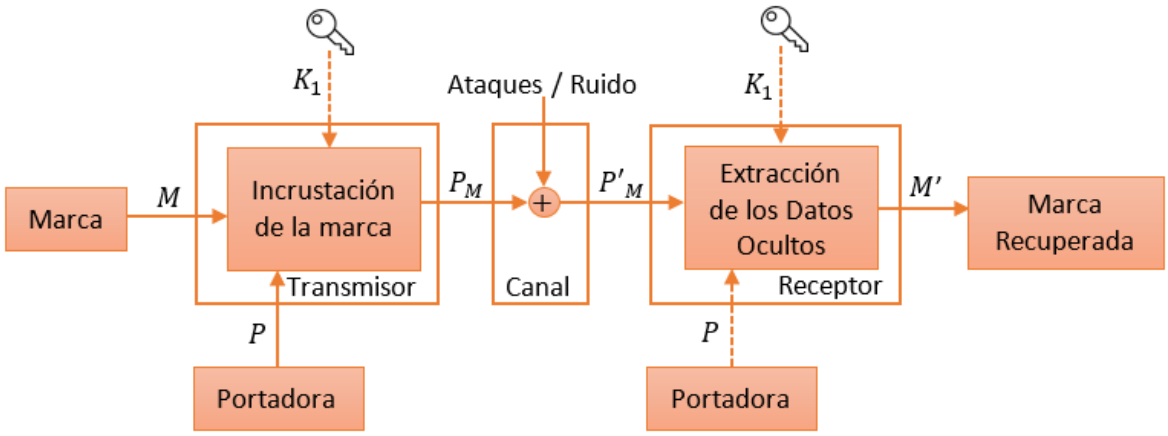



*Figura 2.5 Esquema general del marcado de agua como sistema de comunicación.*

## 2.3. Parámetros del marcado de agua

La fórmula general del marcado de agua es la que se muestra en la ecuación (2.1):

$$\alpha P + \beta M = P_M \tag{2.1}$$

Donde $\alpha + \beta = 1$, $\alpha$ y $\beta$ son los factores de fuerza de inserción, $P$ es la señal portadora sin marcar, $M$ es la marca, y $P_M$ es la señal marcada.

En la ecuación (2.1) se observa que uno de los principales parámetros de las marcas de agua es la fuerza de inserción que es directamente proporcional a la robustez de la marca. El segundo parámetro es la imperceptibilidad, que es inversamente proporcional a la robustez, es decir, directamente proporcional a la calidad resultante de la señal portadora marcada.

En cualquier algoritmo de marcado se debe encontrar la mejor proporción entre robustez, e imperceptibilidad, con el objetivo de que la marca sea suficientemente resistente sin dañar a la señal portadora.

Adicionalmente, cada algoritmo particular puede tener parámetros adicionales, tales como codificación, dispersión, llaves de incrustación, entre otros.

## 2.4. Clasificación de las técnicas de marcado de agua

Las diversas técnicas de marcado [6] se pueden clasificar considerando diferentes características de los algoritmos empleados [5], [7]. En la *Figura* 2.6 se muestra una clasificación de las técnicas de marcado y en los puntos subsecuentes se detallan las propiedades de los cuales derivan las clasificaciones.

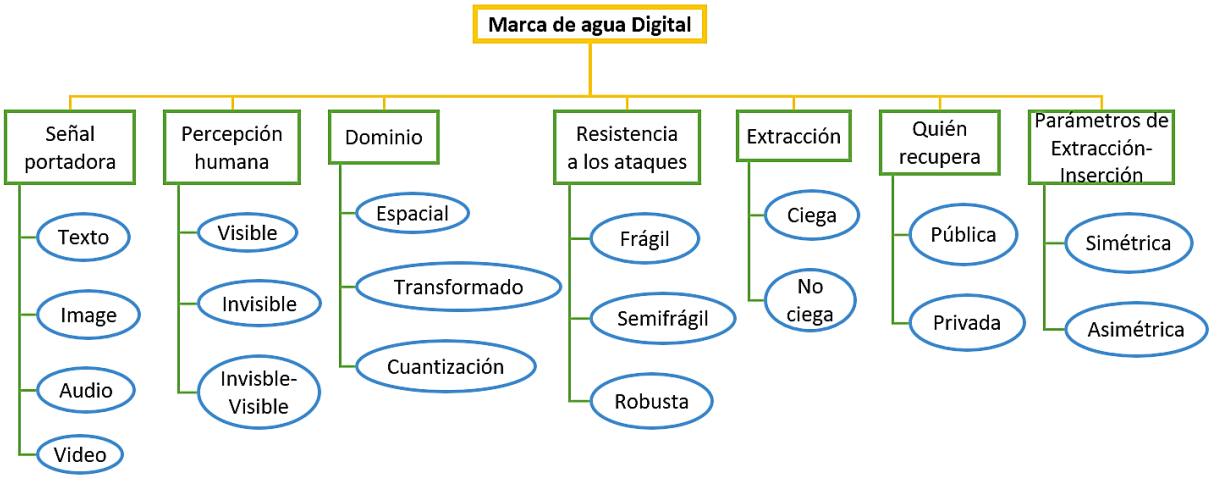



*Figura 2.6 Clasificación de las técnicas de marcado*

**Dependiendo de la señal portadora**

La incrustación de la marca puede llevarse a cabo en diferentes tipos de señales:

a) Texto. Documentos escritos.
b) Imágenes. Archivos pictográficos.
c) Audio. Archivos de sonido.
d) Video. Archivos audiovisuales.

El presente trabajo se centra en el marcado de imágenes digitales, por lo que en adelante se referirá como imagen a la señal portadora.

**Dependiendo de la percepción humana**

Los sentidos por los que percibimos el entorno tienen sus limitaciones, dependiendo del alcance de la visión humana la marca puede clasificarse como:

a) Visible. Se percibe a simple vista sin ayuda externa, no obstante, puede camuflarse para que no sea evidente.
b) Invisible. Se requiere un procesamiento externo para poder ver la marca.

c) Invisible-Visible. Se requiere un mínimo procesamiento para revelar la marca. Se consideran dos tipos principales IVW (*Imperceptible-Visible Watermark*) y UVW (*Unseen-Visible Watermark*); en el primer caso se aprovechan las capacidades de procesamiento de imágenes de los dispositivos de visualización (Hardware) y en el segundo caso se aprovechan las funciones de procesamiento de imágenes integradas en los dispositivos de visualización (Software). [8]

**Dependiendo el dominio de inserción**

Los diferentes dominios que se pueden usar para llevar a cabo la incrustación de la marca son:

a) Espacial. En el caso de las imágenes se refiere a los pixeles directamente. Uno de los métodos más antiguos es el del bit menos significativo (LSB, por sus siglas en inglés).
b) Transformado. La imagen portadora es convertida mediante alguna de las transformadas disponibles, tales como: coseno (DCT), wavelet (DWT), Fourier (DFT), etc.
c) Cuantización. La imagen portadora se cuantifica aplicando el conjunto de vectores elegidos, uno de los métodos más usados es la cuantización vectorial (VQ).

**Dependiendo de la resistencia a los ataques**

Las imágenes marcadas pueden ser propicias a experimentar diversos ataques, dependiendo del tipo de aplicación es deseable que la resistencia de la marca varíe.

a) Robusta. La marca tiene una fuerte resistencia a la mayoría de los ataques.
b) Semi-frágil. La marca tiene una fuerte resistencia solamente a algunos tipos de ataques, mientras que es frágil a otros.
c) Frágiles. La marca no es resistente a los ataques; generalmente se usan para detectar la manipulación de las imágenes marcadas.

**Dependiendo del proceso de extracción o revelado**

El proceso de extracción puede requerir cierto tipo de información, dependiendo de esto las marcas se clasifican en:

a) No ciega. Para obtener la marca se requieren los datos originales, la imagen original y/o la marca original.

b) Ciega. Para la extracción de la marca no se requiere de los datos originales.

**Dependiendo de quién puede recuperar la marca**

La información que la marca pueda proporcionar al usuario es un factor importante para determinar quién pueda recuperar dicha marca:

a) Pública. Cualquiera puede extraer o revelar la marca incrustada.
b) Privada. Solamente los usuarios autorizados pueden extraer la marca.

**Dependiendo de los parámetros de inserción y extracción**

El algoritmo de marcado se puede clasificar en:

a) Simétrico. La extracción usa los mismos parámetros que la incrustación.
b) Asimétrico. La extracción usa parámetros diferentes a los de la incrustación.

## *2.5. Digitalización y transformación digital [9]*

El término de digitalización se utiliza con dos significados. El primero es la transformación de la versión análoga o formato físico a una versión digital (bits) (digitization, en inglés). El segundo (digitalization, en inglés) se refiere a trasmutar las interacciones, las comunicaciones, las funciones comerciales en lo más digital posible; en este sentido la digitalización conduce al uso de tecnologías digitales y de datos para un negocio digital.

La transformación digital, requiere de la digitalización y abarca todos los aspectos de los negocios, independientemente de si se trata de un negocio digital o no.

## *2.6. Ataques informáticos*

Un ataque se puede definir como cualquier manipulación que altere una imagen, incluyendo las operaciones normales de procesamiento de imágenes, como la compresión, los filtrados y el cambio de contraste, que se consideran ataques no intencionales.

Los ataques a la imagen también pueden ser intencionales como las distorsiones geométricas (recorte, rotación, escalamiento, etc.)

Existen también ataques directos a la marca como el promedio estadístico mediante el cual un atacante puede estimar la marca de agua y entonces retirarla de la imagen marcada restando la marca estimada; o el remarcado que consiste en marcar una imagen ya marcada y reclamarla como propia.

A continuación, se presenta una clasificación no exhaustiva de los tipos de ataques [1].

**Ataques simples**

Los ataques simples pretenden dañar la marca insertada manipulando la imagen marcada pero no intentan identificar ni aislar la marca. Algunos ejemplos de este tipo de ataques son la compresión con pérdida de información, la adición de ruido, el filtrado lineal y no lineal, la adición de un *offset*, los recortes, la conversión analógica, la cuantización de los píxeles y la corrección gamma [1].

**Ataques de sincronización**

Los ataques de sincronización pretenden imposibilitar la recuperación de la marca sin dañarla, y provocando la desincronización del detector. Fundamentalmente son distorsiones geométricas como las rotaciones, los desplazamientos espaciales, la inserción o eliminación de píxeles o áreas, los recortes, los *zooms*, etc. [1]

**Ataques de ambigüedad**

Los ataques de ambigüedad pretenden crear confusión mediante la creación de falsas imágenes marcadas, u originales falsos. Un ejemplo de este tipo de ataque es el ataque de inversión, el cual introduce una o varias marcas nuevas en la imagen para tratar de impedir que se pueda identificar cuál es la marca legítima y original [1].

**Ataques de supresión**

Los ataques de supresión pretenden analizar la imagen marcada con el objetivo de aislar la marca y eliminarla. Ejemplos de este tipo de ataques son ciertas operaciones de filtrado no lineal, los ataques por colisión, o los ataques dirigidos concretamente a un esquema de marcado particular, explotando los puntos débiles ya conocidos de dicho esquema [1].

**Impresión-Escaneo (print-scan attack)**

El proceso de impresión-escaneo es un complejo compuesto de varios ataques. La dificultad al enfrentar este problema se puede resumir en tres puntos [10]:

- Aleatoriedad. El resultado siempre es diferente uno de otro.
- Dependencia humana. Cada persona opera los equipos de manera diferente.
- Ambigüedad. Los procesos de impresión y de escaneo no pueden separarse uno del otro y las distorsiones siempre pertenecen a ambos.

La calidad de la impresión depende del tipo y antigüedad de la impresora [11], en el proceso de impresión: la distribución no uniforme del tóner o la inyección tinta desigual puede producir distorsiones geométricas; la conversión a medio tono genera una variación de los valores de los pixeles; la suciedad de los rodillos adiciona ruido; cuando la resolución de la impresora (puntos por pulgada, dpi) es menor a la resolución de la imagen digital, la imagen resulta deteriorada.

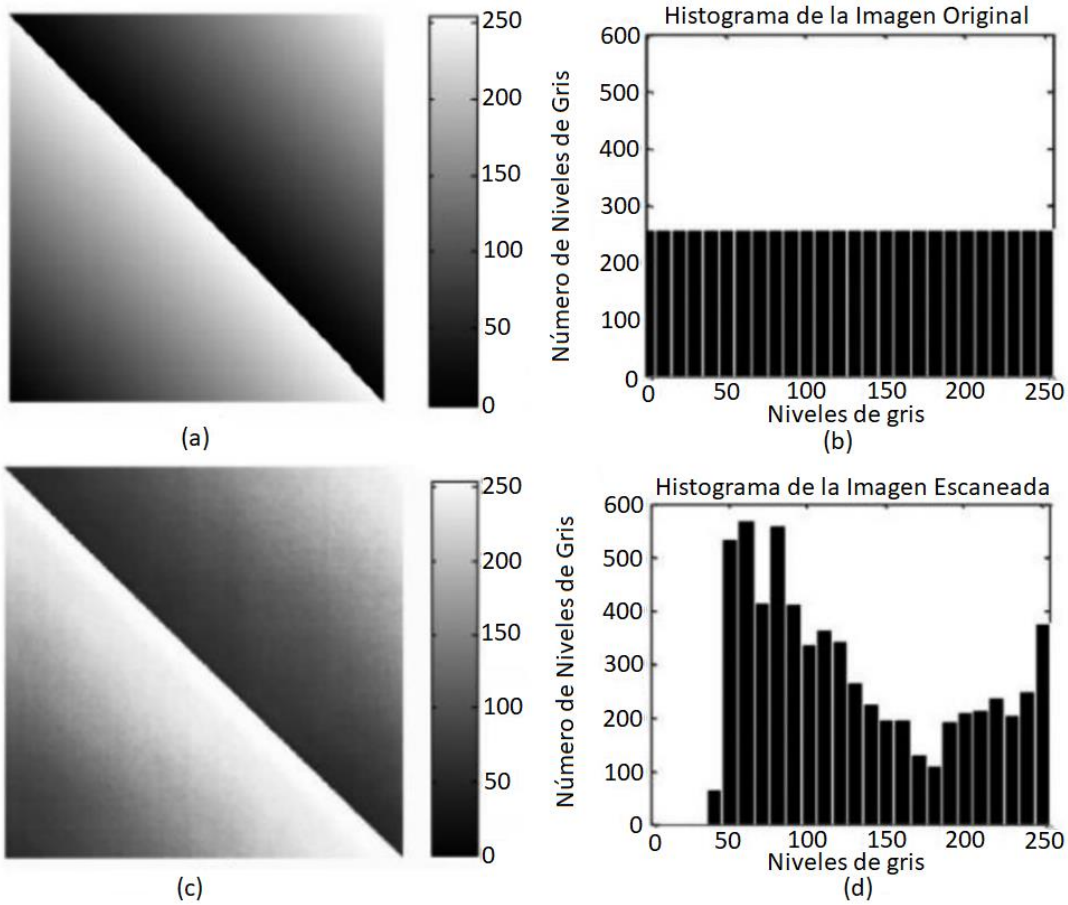



*Figura 2.7 Efectos del ataque impresión-escaneo. (a) Imagen original, (b) histograma original, (c) imagen impresa y escaneada, (d) histograma resultante* [12].

La calidad del escaneo depende en parte de la configuración del escáner, en el proceso de escaneo: suele ser muy difícil colocar la imagen correctamente sin ningún desplazamiento lo que induce consecuentemente rotación y recorte; la distorsión de escalamiento por otra parte resulta de la configuración incorrecta de la resolución del escáner; además, la suciedad del escáner adiciona ruido. En la Figura 2.7 se puede apreciar los efectos de la impresión y escaneo en el histograma de en una imagen en tonos de gris.

## 2.7. Aplicaciones de la marca de agua

Las marcas de agua pueden utilizarse para diferentes propósitos, algunos de los más comunes se listan a continuación.

**Integración de información**

Las marcas destinadas a este propósito incrustan información en la imagen, debido a que adjuntar datos extra a las imágenes puede ser muy deseable, a diferencia de la información almacenada en el encabezado de una imagen la marca de agua guarda la información en el gráfico en sí, por lo que dicha información no se perdería si la imagen llega a cambiar de formato.

**Protección de derechos de propiedad intelectual**

Las marcas de agua pueden usarse para proteger los derechos de propiedad intelectual, las destinadas a este propósito son robustas; algunas de las marcas de agua pueden ser detectadas por las máquinas y desencadenar un proceso que interrumpa la copia.

**Demostración de propiedad**

La demostración de propiedad generalmente se realiza incrustando logos o marcas en las imágenes que indiquen quienes son los legítimos propietarios de una imagen.

**Rastreo de copias**

Las marcas usadas para el rastreo de copias se individualizan para cada copia de la imagen, de esta manera la información proporcionada por cada marca corresponde a una copia particular y facilita su rastreo.

**Autenticación de contenido**

Las marcas destinadas a este propósito generalmente son frágiles, ya que su propósito es verificar que la imagen no haya sido manipulada.

## 2.8. Métricas de desempeño de los algoritmos de marcado

Las métricas se emplean para determinar el valor de los dos principales parámetros de las marcas de agua: robustez e imperceptibilidad. Más adelante se hace una división de las métricas en estas dos categorías.

En las ecuaciones de las medidas de desempeño $M$ representa a la imagen utilizada como marca original, $M'$ representa a la imagen de la marca recuperada, $I$ representa a la imagen usada como portadora antes de ser marcada, e $I'$ representa a la imagen empleada como portadora después de ser marcada. $X$ y $Y$ son las dimensiones de cada imagen respectivamente.

### 2.8.1. Robustez

Como se puede observar en la sección **2.4**, la resistencia de una marca a los ataques establece su grado de robustez. Para determinar el valor de la robustez se compara la marca original $M$ con la marca recuperada $M'$.

**Distancia hamming (HD)**

En el caso de que las imágenes fueran idénticas entonces $HD(M,M') = 0$, por el contario si las imágenes fueran totalmente diferentes $HD(M,M') = \mathrm{X} \times \mathrm{Y}$, que sería el valor máximo que esta medida puede alcanzar. Si la distancia de Hamming, ecuación (2.2), se normaliza respecto al tamaño de la imagen, entonces el valor normalizado de $HD(M,M')$ se encontrará entre 0 y 1.

$$HD(M,M') = \sum_{i}^{X} \sum_{j}^{Y} [M(i,j) \neq M'(i,j)] \tag{2.2}$$

**Bit error rate (BER)**

Debido a que el mayor valor normalizado que puede adoptar $HD(M,M') = X \times Y$, es 1, el valor máximo de $BER(M,M') = 100\%$, es decir, siempre oscila entre 0 y 1, donde 0 correspondería a dos marcas de agua iguales y 1 a dos marcas de agua totalmente

diferentes, es decir con ningún bit de coincidencia. El cálculo del Bit Error Rate se realiza mediante la ecuación (2.3).

$$BER(M, M') = \frac{HD(M, M')}{X \times Y} \times 100 \tag{2.3}$$

**Bit correct rate (BCR)**

Al ser el complementario del $BER$, si $BCR(M, M') = 100\%$ significa que las marcas de agua son iguales y si $BCR(M, M') = 0\%$ significa que las marcas de agua son totalmente diferentes. El cálculo del Bit Correct Rate se realiza mediante la ecuación (2.4).

$$BCR(M, M') = \left(1 - \frac{HD(M, M')}{X \times Y}\right) \times 100 \tag{2.4}$$

**Correlación normalizada (NC)**

En esta medida si $NC(I, I') = 1$, quiere decir que las marcas de agua son idénticas; siempre y cuando $\sum_i^X \sum_j^Y (M(i,j)^2) \neq 0$. En esta medida si $NC(I, I') = 1$, quiere decir que las marcas de agua son idénticas; siempre y cuando $\sum_i^X \sum_j^Y (M(i,j)^2) \neq 0$. El cálculo de la Correlación Normalizada se realiza mediante la ecuación (2.5).

$$NC(M, M') = \frac{\sum_i^X \sum_j^Y \left(\left(M(i,j)\right) \times \left(M'(i,j)\right)\right)}{\sum_i^X \sum_j^Y (M(i,j)^2)} \tag{2.5}$$

## *2.8.2. Imperceptibilidad*

La imperceptibilidad se mide comparando la imagen original $I$ y la imagen marcada antes de ser atacada $I'$, este parámetro nos proporciona información acerca de la distorsión sufrida por la imagen debido a la incrustación de la marca de agua.

**Distancia euclidiana (ED)**

El mejor resultado sería $ED(I, I') = 0$, en cuyo caso las imágenes comparadas serían idénticas. Entre más elevado sea su valor, dado que no tiene un límite superior, más distintas son las imágenes comparadas. El cálculo de la Distancia Euclidiana se realiza mediante la ecuación (2.6).

$$ED(I, I') = \sum_i^X \sum_j^Y \left(\left(I(i,j)\right) - \left(I'(i,j)\right)\right)^2 \tag{2.6}$$

**Error del cuadrático medio (MSE)**

Al igual que en el caso anterior, el mejor resultado sería $MSE(I,I')=0$. El cálculo del Error de Cuadrático Medio se realiza mediante la ecuación (2.7).

$$MSE(I,I')=\frac{ED(I,I')}{X\times Y} \tag{2.7}$$

**Relación señal pico a ruido (PSNR)**

$I_{max}=255$, es el máximo valor de intensidad que puede tomar cualquier pixel de la imagen de 8 bits.

Si las imágenes fueran idénticas $PSNR(I,I')=\infty$, por lo que entre menor sea su valor la distorsión de $I'$ es mayor. El cálculo de la Relación Señal Pico a Ruido se realiza mediante la ecuación (2.8).

$$\begin{aligned}PSNR(I,I') &= 10\times\log_{10}\frac{(I_{max})^2}{MSE(I,I')}=20\times\log_{10}\frac{I_{max}}{\sqrt{MSE(I,I')}}\\ &= 20\log_{10}I_{max}-10\log_{10}MSE(I,I')\end{aligned} \tag{2.8}$$

**Medida del índice de semejanza estructural (*Structural similarity index measure*, SSIM)**

La Semejanza Estructural, ecuación (2.9), considera tres parámetros: luminancia, contraste y estructura de la imagen [4]. "La información estructural es la que representa el arreglo de los objetos presentes en la escena y es independiente del contraste y de la iluminación" [4].

$$SSIM(I,I')=[l(I,I')]^{\alpha}\cdot[c(I,I')]^{\beta}\cdot[s(I,I')]^{\gamma} \tag{2.9}$$

Cumple con las siguientes características:

Simetría $SSIM(I,I')=SSIM(I',I)$

Límite $SSIM(I,I')\leq 1$

Máximo único $si\ I=I'\ SSIM(I,I')=1$

El valor medio de la intensidad de una imagen está dado por la ecuación (2.10):

$$\mu_I=\frac{1}{X\times Y}\sum_{i}^{X}\sum_{j}^{Y}I(i,j) \tag{2.10}$$

La luminancia se calcula con la ecuación (2.11):

$$l(I,I')=\frac{2\mu_I\mu_{I'}+c_1}{\mu_I^2+\mu_{I'}^2+c_1} \tag{2.11}$$

La desviación estándar está representada por las ecuaciones (2.12) y (2.13).

$$\sigma_I = \left( \frac{1}{(X \times Y) - 1} \sum_{i}^{X} \sum_{j}^{Y} (I(i,j) - \mu_I)^2 \right)^{\frac{1}{2}} \tag{2.12}$$

$$\sigma_{II'} = \frac{1}{(X \times Y) - 1} \sum_{i}^{X} \sum_{j}^{Y} (I(i,j) - \mu_I)(I'(i,j) - \mu_{I'}) \tag{2.13}$$

La comparación del contraste está dada por la ecuación (2.14):

$$c(I, I') = \frac{2\sigma_I \sigma_{I'} + c_2}{\sigma_I{}^2 + \sigma_{I'}{}^2 + c_2} \tag{2.14}$$

La función de similitud estructural está dada por la ecuación (2.15):

$$s(I, I') = \frac{\sigma_{II'} + c_3}{\sigma_I \sigma_{I'} + c_3} \tag{2.15}$$

Los parámetros $c_1$, $c_2$ y $c_3$ se utilizan para evitar que haya divisiones entre cero, $c_1 = (K_1 L)^2$, $c_2 = (K_2 L)^2$, donde $L$ es el rango dinámico de la imagen. Para una imagen, 8 bits entonces $L = 255$. $K_1 \ll 1$, $K_2 \ll 1$ y $c_3 = \frac{c_2}{2}$. En el presente trabajo se escogieron los valores $K_1 = 0.01$ y $K_2 = 0.03$, por consiguiente $c_1 = 0.065025$ y $c_2 = 0.585225$. Considerando $\alpha = \beta = \gamma = 1$ [13] se obtiene la ecuación (2.16):

$$\begin{aligned} SSIM(I, I') &= [l(I, I')] \cdot [c(I, I')] \cdot [s(I, I')] \\ &= \frac{2\mu_I \mu_{I'} + c_1}{\mu_I^2 + \mu_{I'}^2 + c_1} \cdot \frac{2\sigma_I \sigma_{I'} + c_2}{\sigma_I{}^2 + \sigma_{I'}{}^2 + c_2} \cdot \frac{\sigma_{II'} + \frac{c_2}{2}}{\sigma_I \sigma_{I'} + \frac{c_2}{2}} \\ &= \frac{(2\mu_I \mu_{I'} + c_1)(2\sigma_{II'} + c_2)}{(\mu_I^2 + \mu_{I'}^2 + c_1)(\sigma_I^2 + \sigma_{I'}^2 + c_2)} \end{aligned} \tag{2.16}$$

La función de Matlab© ssim$(I, I')$ (índice de similaridad estructural). Primero utiliza una máscara gaussiana W de desviación estándar 1.5 de 11x11, y de esta manera, le da más peso al pixel central.

Calcular SSI localmente. El valor medio de la intensidad de una imagen está dado por la ecuación (2.17):

$$\mu_I = \sum_{i=1}^{N} w_i I_i \tag{2.17}$$

La desviación estándar está dada por las ecuaciones (2.18) y (2.19).

$$\sigma_I = \left( \sum_{i=1}^{N} w_i (I_i - \mu_I)^2 \right)^{\frac{1}{2}} \tag{2.18}$$

$$\sigma_{II'} = \sum_{i=1}^{N} w_i (I_i - \mu_I)\,(I'_i - \mu_{I'}) \tag{2.19}$$

El promedio del índice [5] está dada por la ecuación (2.20):

$$MSSIM(WI, WI) = \frac{1}{M} \sum_{j=h1}^{M} SSIM\left(WI_j, WI'_j\right) \tag{2.20}$$

Donde $WI$ y $WI$ se refieren a las ventanas de las imágenes original y marcada y $M$ es el número de ventanas locales de la imagen

**Fidelidad de información visual (*Visual information fidelity*, VIF)**

Como se sabe en la literatura [14], el valor VIF, ecuación (2.21), refleja distorsiones perceptivas con mayor precisión que la métrica PSNR. El rango de valores de VIF es [0, 1], y un valor más cercano a 1 representa una mejor fidelidad con respecto a la imagen original.

$$VIF = \frac{\sum_{t \in channels} I(\vec{C}^{R,t}; \vec{F}^{R,t} | s^{R,t})}{\sum_{t \in channels} I(\vec{C}^{R,t}; \vec{E}^{R,t} | s^{R,t})}. \tag{2.21}$$

Donde $I(\vec{C}^{R,t}; \vec{F}^{R,t} | s^{R,t})$ representa la información que idealmente podría ser extraída por el cerebro en la imagen de referencia, y $I(\vec{C}^{R,t}; \vec{E}^{R,t} | s^{R,t})$ representa la información que idealmente podría ser extraída por el cerebro en la imagen de prueba. $\vec{C}^{R,t}$ representa los $R$ elementos del campo aleatorio $C_t$ que describe los coeficientes de la subbanda $t$, y así sucesivamente. En la Figura 2.8 se muestra gráficamente como se obtienen los elementos para calcular la VIF.

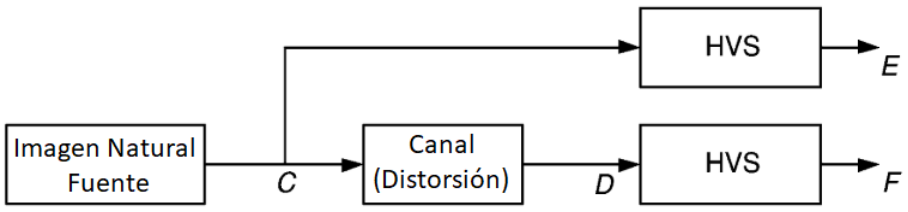



*Figura 2.8 La información mutua entre C y E cuantifica la información que el cerebro idealmente podría extraer de la imagen de referencia, mientras que la información mutua entre C y F cuantifica la información correspondiente que podría extraerse de la imagen de prueba.* [14]

## 2.9. Marca de agua visible

### 2.9.1. Descomposición estructura–textura (cartoon–texture)

Existen diferentes modelos de descomposición de una imagen en varias imágenes. En el modelo de Estructura-Textura, una imagen $I$ de entrada se descompone en una imagen de estructura $I_e$ y una imagen de textura $I_t$, ambas de tamaño $M \times N$, que se puede expresar como en la ecuación (2.22):

$$I = I_e + I_t \tag{2.22}$$

Entre las posibles aplicaciones, este tipo de descomposición puede emplearse tanto para la selección de características[15], para inserción de marcas de agua [16], [17] o para la eliminación de ruido [18]. La descomposición de la imagen en estructura y textura está formulado como un problema de optimización [19] dado por la expresión (2.23):

$$\min_{I_e}\{\|s(I_e)\|_A | \|t(I_e, I)\|_B | \leq \sigma\} \tag{2.23}$$

Donde $\| \|_A$ y $\| \|_B$ son normas cualesquiera, $s(\ )$ y $t(\cdot, \cdot)$ son funciones cualesquiera, y $\sigma$ es un valor constante, que se usa como una condición de restricción de la optimización.

Se hace $s(I_e)$ como el gradiente de diferencia intermedio $s(I_e) = \nabla(I_e)$, $t(I_e, I)$ como $I_t = t(I_e, I) = I - I_e$ y las normas $\| \|_A$ y $\| \|_B$ como la $norma - L1$; de esta manera la ecuación (2.23) se convierte en un modelo de variación total L1 (TV-L1).

**Modelo de variación total L1 (TV-L1)**

El modelo de Variación Total L1 (TV-L1), es considerado uno de los modelos más eficientes para resolver el problema de optimización dado por la ecuación (2.23) [16] que se puede rescribir como en la expresión (2.24):

$$\min_{I_e}\left\{\int_\Omega |\nabla(I_e)| + \int_\Omega \lambda |I - I_e|\right\} \tag{2.24}$$

Donde $\Omega$ es la región de la imagen entera y $\lambda$ es el multiplicador de Lagrange.

En la forma discreta la ecuación (2.24) se reescribiría como en la expresión (2.25):

$$\min_{I_e}\{\|\nabla(I_e)\|_1 + \lambda\|I - I_e\|_1\} \tag{2.25}$$

El gradiente $\nabla(I_e)$, ecuación (2.26), se calcula con la diferencia entre un píxel adyacente y el pixel actual:

$$\nabla(I_e) = \begin{cases} (\nabla I_e)^y_{i,j} = \begin{cases} I_e(i+1,j) - I_e(i,j) & \text{si } i < M \\ 0 & \text{si i} = M \end{cases} \\ (\nabla I_e)^x_{i,j} = \begin{cases} I_e(i,j+1) - I_e(i,j) & \text{si } j < N \\ 0 & \text{si j} = N \end{cases} \end{cases} \tag{2.26}$$

$\|\nabla(I_e)\|_1$ se define como en la ecuación (2.27):

$$\|\nabla(I_e)\|_1 = \sum\nolimits_{i,j} \sqrt{\left((\nabla I_e)^x_{i,j}\right)^2 + \left((\nabla I_e)^y_{i,j}\right)^2} \tag{2.27}$$

Para resolver el problema de minimización aplicamos los siguientes operadores en cada iteración [20].

Operador proximal inicial $\mathrm{p}_0$ está dado por la ecuación (2.28):

$$p_0 = \begin{cases} (\mathrm{p}_0)^y_{i,j} = \begin{cases} I(i+1,j) - I(i,j) & \text{si } i < M \\ 0 & \text{si i} = M \end{cases} \\ (p_0)^x_{i,j} = \begin{cases} I(i,j+1) - I(i,j) & \text{si } j < N \\ 0 & \text{si j} = N \end{cases} \end{cases} \tag{2.28}$$

Operador sigma está dado por las ecuaciones (2.29) y (2.30).

$$p_n^\sigma = (p_{n-1})\big(\sigma \times \nabla(I_e)\big) \tag{2.29}$$

$$p_n = \frac{p_n^\sigma}{\max\left(1, \sqrt{\left(\left(p_n^\sigma\right)^x\right)^2 + \left(\left(p_n^\sigma\right)^y\right)^2}\right)} \tag{2.30}$$

Operador de divergencia discreto está expresado en la ecuación (2.31):

$$div_n(i,j) = \begin{cases} p_n^y(i,j) & \text{si } i = 1 \\ p_n^y(i,j) - p_n^y(i-1,j) & \text{si } i < i < M \\ -p_n^y(i-1,j) & \text{si } i = M \end{cases} + \begin{cases} p_n^x(i,j) & \text{si } j = 1 \\ p_n^x(i,j) - p_n^x(i,j-1) & \text{si } i < j < N \\ -p_n^x(i,j-1) & \text{si } j = N \end{cases} \tag{2.31}$$

Operador *tao está expresado en la ecuación* (2.32):

$$p_n^\tau(i,j) = \begin{cases} (I_e^{n-1}(i,j) + (\tau \times div_n) - (\lambda\tau)) & \text{si}(I_e^{n-1}(i,j) + (\tau \times div_n) - I(i,j)) > (\lambda\tau) \\ (I_e^{n-1}(i,j) + (\tau \times div_n) + (\lambda\tau)) & \text{si}(I_e^{n-1}(i,j) + (\tau \times div_n) - I(i,j)) < -(\lambda\tau) \\ I(i,j) & \text{si}(\lvert(i,j) + (\tau \times div_n) - I\rvert(i,j)) \leq (\lambda \times \tau) \end{cases} \quad (2.32)$$

Para calcular la imagen de estructura en la iteración $n$, se emplea la ecuación (2.33):

$$I_e^n = p_n^\tau + (\theta \times (p_n^\tau - I_e^{n-1})) \quad (2.33)$$

El algoritmo TV-L1 se resume como

1) Fijar los parámetros: constante de Lagrange $\lambda$; número de iteraciones $it$; pasos del esquema iterativo $\sigma$ y $\tau$; paso de extrapolación $\theta$, que converge cuando $\theta = 1$ y $\tau\sigma L^2 \leq 1$, donde $L^2 = \|\nabla\|^2 \leq 8$. En el presente trabajo de manera empírica se escogieron los valores $L^2 = 8$, $\tau = 0.02$, $\sigma = \frac{1}{L^2 \times \tau} = 6.25$, con lo que se cumplen las inecuaciones.
2) Imagen de entrada $I$ normalizada.
3) Calcular el operador proximal inicial $p_0$
4) for $n = 1, \ldots, it$
    a. Calcular $\nabla(I_e^{n-1})$, para la primera iteración $I_e^{n-1} = I$.
    b. Calcular los factores proximales.
    c. Calcular el operador de divergencia
    d. Calculamos $I_e^n$
5) end for

## *2.9.2. Región de interés (ROI)*

La región de interés (ROI) es una zona delimitada de la imagen, seleccionada para su posterior análisis, esta selección puede hacerse manual o automáticamente. Existen diversos métodos automáticos para extraer la ROI que varían dependiendo de la naturaleza de las imágenes a procesar, por ejemplo, en imágenes médicas suele ser específico de cada caso [21], [22].

**Atención visual**

El mapa de saliencia [23] es un área que llama la atención visual [24], [25], y es un método usado para extraer la ROI en imágenes de uso general.

El método empleado en [26] para obtener un mapa de saliencia se detalla a continuación.

Si consideramos a cualquier imagen como una composición de primer plano y fondo, se podría expresar mediante la ecuación (2.34):

$$I = f + b \tag{2.34}$$

Donde $f$ es el primer plano, mientras $b$ es el fondo que es débilmente soportado en el dominio de la transformada discreta coseno DCT, es decir, que $b$ tiene solo una pequeña cantidad de componentes distintos de cero en el dominio transformado. Entonces se puede aislar aproximadamente $f$ como en la ecuación (2.35):

$$\bar{I} = sign(DCT(I)) \tag{2.35}$$

Se puede formar un mapa de saliencia $m$, dado por la expresión (2.36):

$$m = g * (\bar{I} \odot \bar{I}) \tag{2.36}$$

Donde $g$ es un filtro de difuminación, $*$ es la operación de convolución, $\odot$ es el operador del producto de Hadamard. En el presente trabajo $g$ es un filtro gaussiano, de las mismas dimensiones que $I$, y desviación estándar $\sigma$.

En la Figura 2.9 se muestran los mapas de saliencia obtenidos con valores de sigma crecientes, cuyo tamaño es 3226x4038 pixeles, donde $\sigma$ es el valor de la desviación estándar para el filtro usado. En blanco se destaca las áreas sobresalientes.

En la Figura 2.10 se muestran los mapas de saliencia obtenidos de la misma imagen reducida a 200x250 pixeles. Comparando ambas figuras se puede percibir que la resolución de la imagen cambia el mapa de saliencia resultante.

En la Figura 2.11 se muestra el área de atención visual en blanco, obtenida de la binarización, con un umbral de 0.6, obtenida de los mapas de saliencia con $\sigma = 8$, mostrados en la Figura 2.9 y la Figura 2.10.

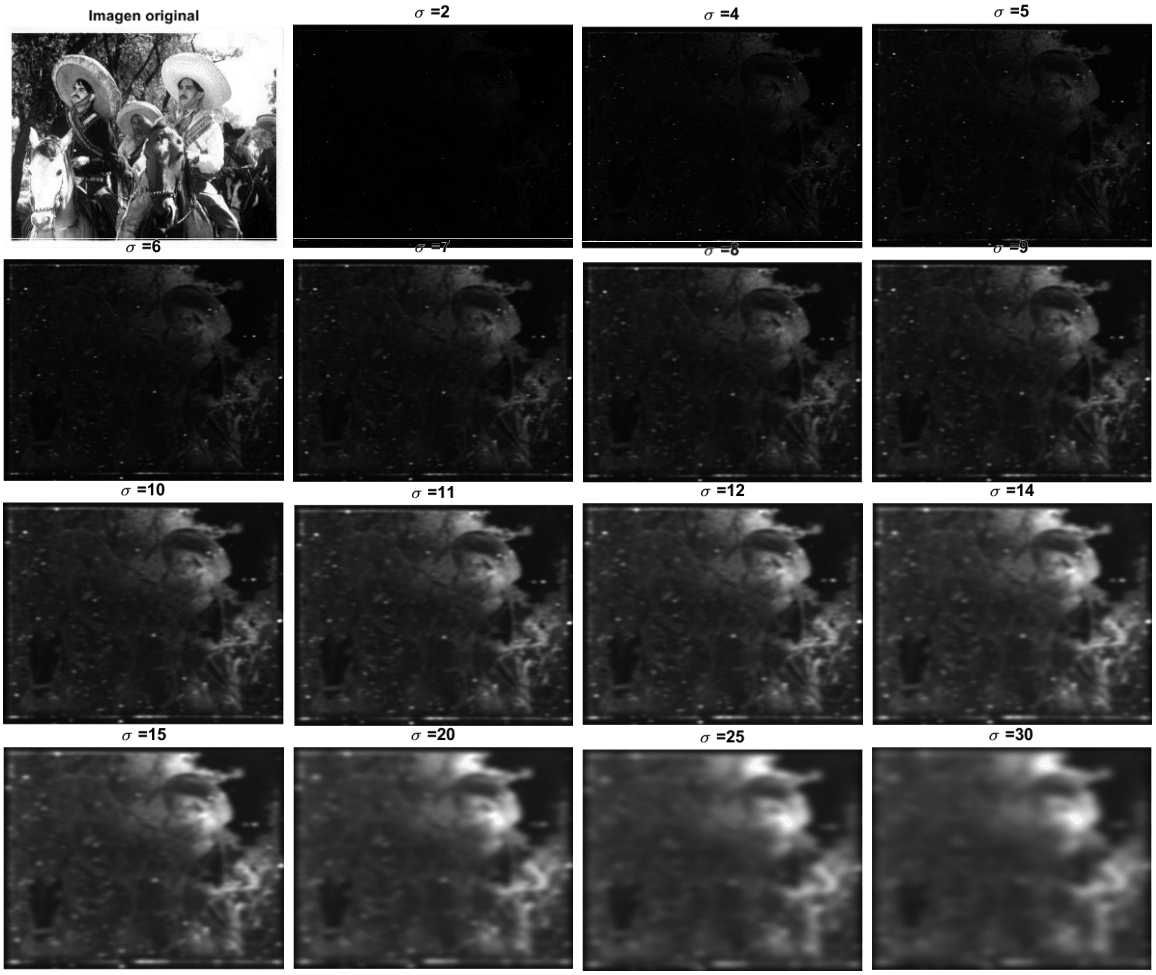
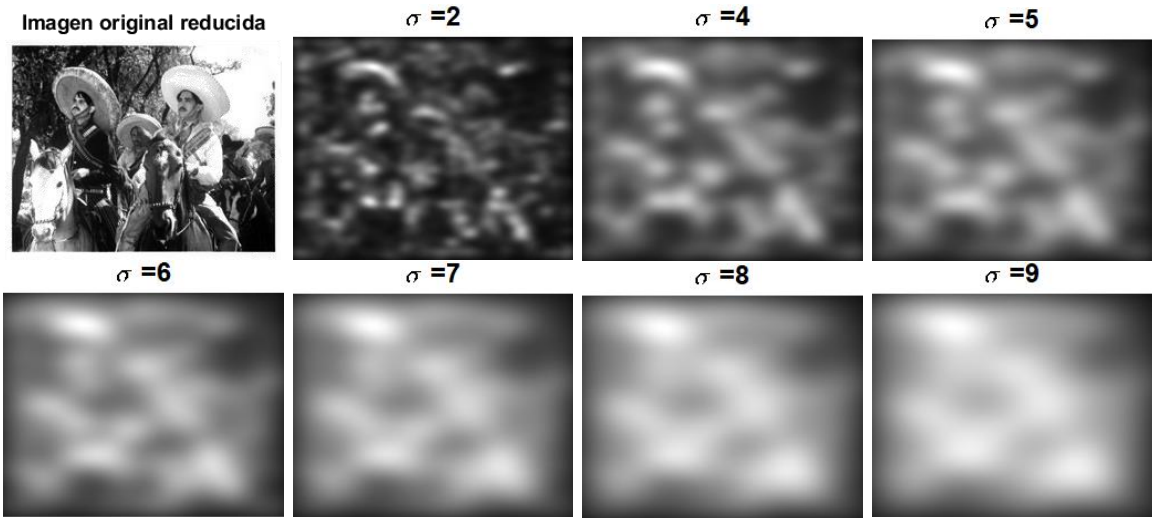



*Figura 2.9 Mapas de saliencia de una imagen de "Pueblito" (23,887)*



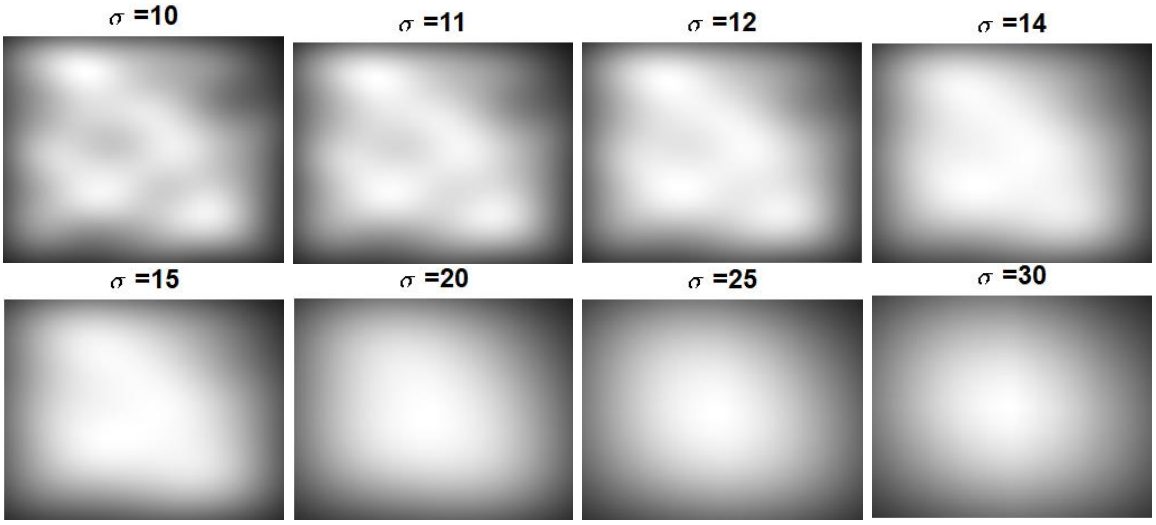
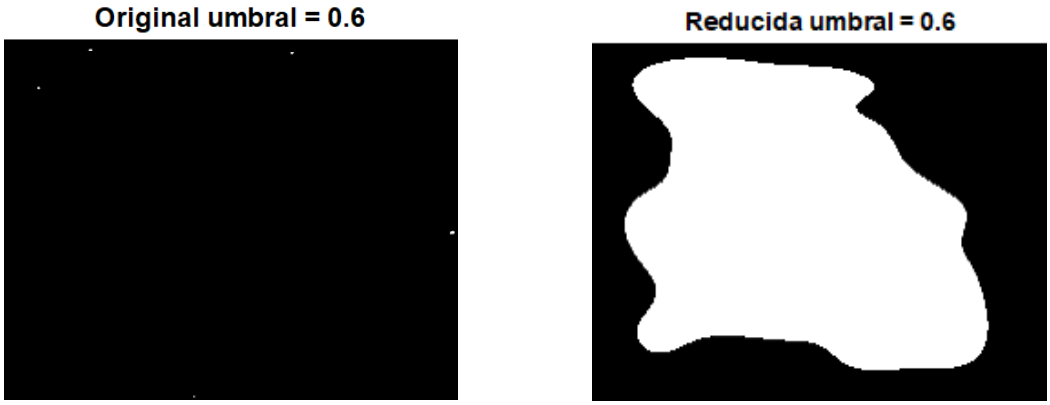



*Figura 2.10 Mapas de saliencia de una imagen de "Pueblito" (23,887) reducida.*




*a)* *b)*

*Figura 2.11 Atención visual $\sigma = 8$, a) de la Figura 2.9 y b) de la Figura 2.10.*

Entre más grande el umbral menor es la región blanca, para un valor demasiado pequeño (0.01), todo resulta en blanco. En la Figura 2.11, el umbral y sigma=8 se eligió para conservar aproximadamente el 50% de los pixeles de la imagen y para obtener una sola región de ser posible.

## *2.9.3. Súper píxeles (SP)*

Los algoritmos de Súper Pixeles o Superpíxeles (SUPERPIXEL) agrupan píxeles en regiones perceptualmente significativas y se han convertido en componentes clave de muchos algoritmos de visión computacional tales como segmentación de imagen [27], [28], reconocimiento de objetos [29], [30], clasificación [31], [32] y seguimiento [33].

Los algoritmos para generar Superpíxeles se pueden clasificar en términos generales en dos grandes grupos: basados en aumentación de gradiente ([34]–[36]) y basados en grafos ([37]–[40]).

Una propuesta más eficiente en términos de la memoria requerida, que exhibe una mejor adherencia de límites y una mejora en el desempeño de los algoritmos de segmentación es la llamada SLIC (*Simple Linear Iterative Clustering*) [41]. En términos de tiempo de procesamiento, el algoritmo SLIC también es el más rápido comparado con otros métodos [42].

El principal parámetro del algoritmo SLIC es $K$ que es el número de superpíxeles deseado. Los otros parámetros son el número de iteraciones; la compacidad (*compactness*), que es una cantidad numérica que representa el grado en que una forma es compacta, cuando su valor sea más cercano a cero, tendrá una forma del superpíxel más irregular, y mientras que entre más grande sea su valor la forma del superpíxel será más cuadrada, como se puede ver en la Figura 2.12. Y por último el método, en el cual se elige si la compacidad se mantiene constante (`slic`) o se va ajustando en cada iteración (`slic0`).

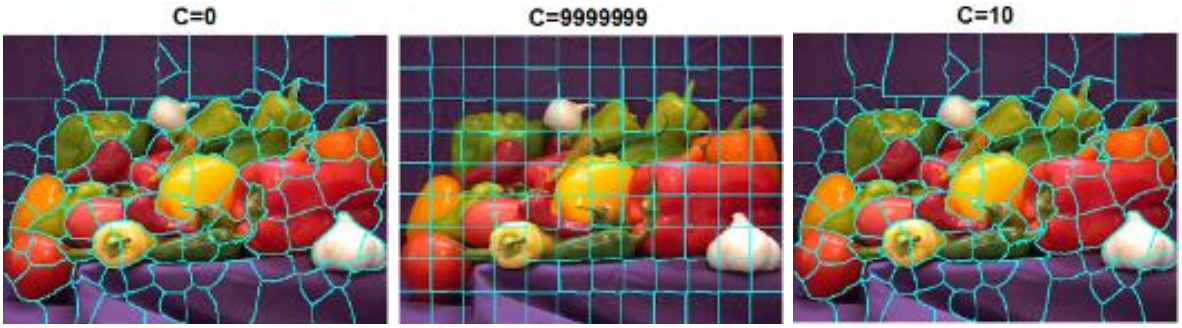



*Figura 2.12 Superpíxeles SLIC, con 100 iteraciones y diferentes compacidades `C`.*

En la Figura 2.13 se puede observar una imagen segmentada con diferentes números de superpíxeles con los valores empíricamente predeterminados (iteraciones=10, compactness=10, método=slic0) de la función *superpixels* de Matlab©.

*Figura 2.13 Imagen dividida con SLIC en 3403, 232 y 24 superpíxeles.*

El algoritmo de SLIC se inicializa con la imagen en el espacio de color CIELab y con $K$ centroides equidistantes formando una cuadrícula regular con un intervalo $S$, como se muestra en la Figura 2.14. Para evitar que los centroides pertenezcan a los pixeles del borde, el centroide se mueve dependiendo del gradiente en una vecindad del centro de 3x3.

El cálculo del gradiente está dado por la ecuación (2.37):

$$G(x_i, y_i) = |I(x_i + 1, y_i) - I(x_i - 1, y_i)|^2 + |I(x_i, y_i + 1) - I(x_i, y_i - 1)|^2 \qquad (2.37)$$

El siguiente paso, que se lleva a cabo en cada iteración, es asignar cada pixel $I(x_i, y_i)$ de la imagen $I$ a un centroide delimitando su región de búsqueda como se muestra en la Figura 2.14.

Para delimitar la distancia se utilizan las ecuaciones (2.38) a (2.41)de distancia en el espacio de color CIELab.

Distancia de color dada por la ecuación (2.38):

$$d_c = \sqrt{(l_j - l_i)^2 + (a_j - a_i)^2 + (b_j - b_i)^2} \qquad (2.38)$$

Donde $l$ representa la luminosidad, $a$ representa las coordenadas rojo/verde ($+a$ indica rojo y $-a$ indica verde), $b$ representa las coordenadas amarillo/azul ($+b$ indica amarillo y $-b$ indica azul).

Distancia espacial dada por la ecuación (2.39):

$$d_c = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \tag{2.39}$$

Donde $x$ y $y$ representa las coordenadas cartesianas de los pixeles en una imagen digital.

Al combinar las distancias de color y la espacial se obtiene la ecuación (2.40):

$$D' = \sqrt{\left(\frac{d_c}{N_c}\right)^2 + \left(\frac{d_s}{N_s}\right)^2} \tag{2.40}$$

Donde $N_c$ y $N_s$ son los valores máximos correspondientes para la normalización de las distancias. Donde $N_s$ está limitada por el rango de búsqueda $S$, dado por la ecuación (2.41)

$$N_s = S = \sqrt{\frac{N}{K}} \tag{2.41}$$

Donde $N$ es el número total de pixeles en una imagen, $K$ es el número de superpíxeles deseado, $S$ es el ancho o alto inicial del superpíxel.

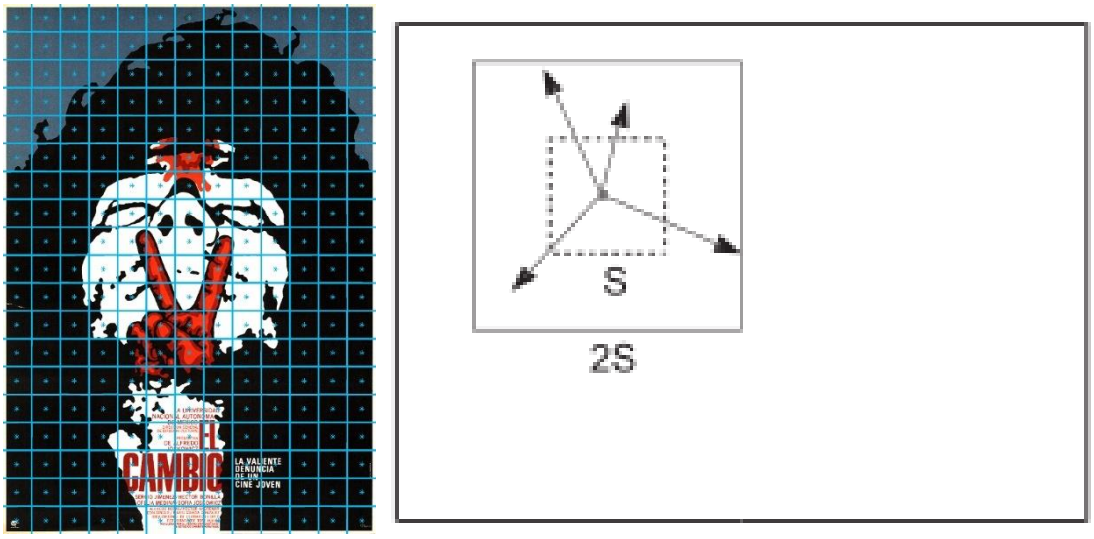



*Figura 2.14 Cuadrícula inicial (izquierda) y Rango de búsqueda del SLIC (derecha)*

En la Figura 2.15 se muestra la evolución del algoritmo, empleando una imagen de 3463x4213 pixeles, el valor de $K$ elegido es de 256 superpíxeles, la división inicial es de 270 superpíxeles y después de 10 iteraciones el número de superpíxeles se mantuvo

en 270. La compacidad se inició con un valor de 10 y dado que se utilizó el método slic0, ésta se fue ajustando en cada iteración.

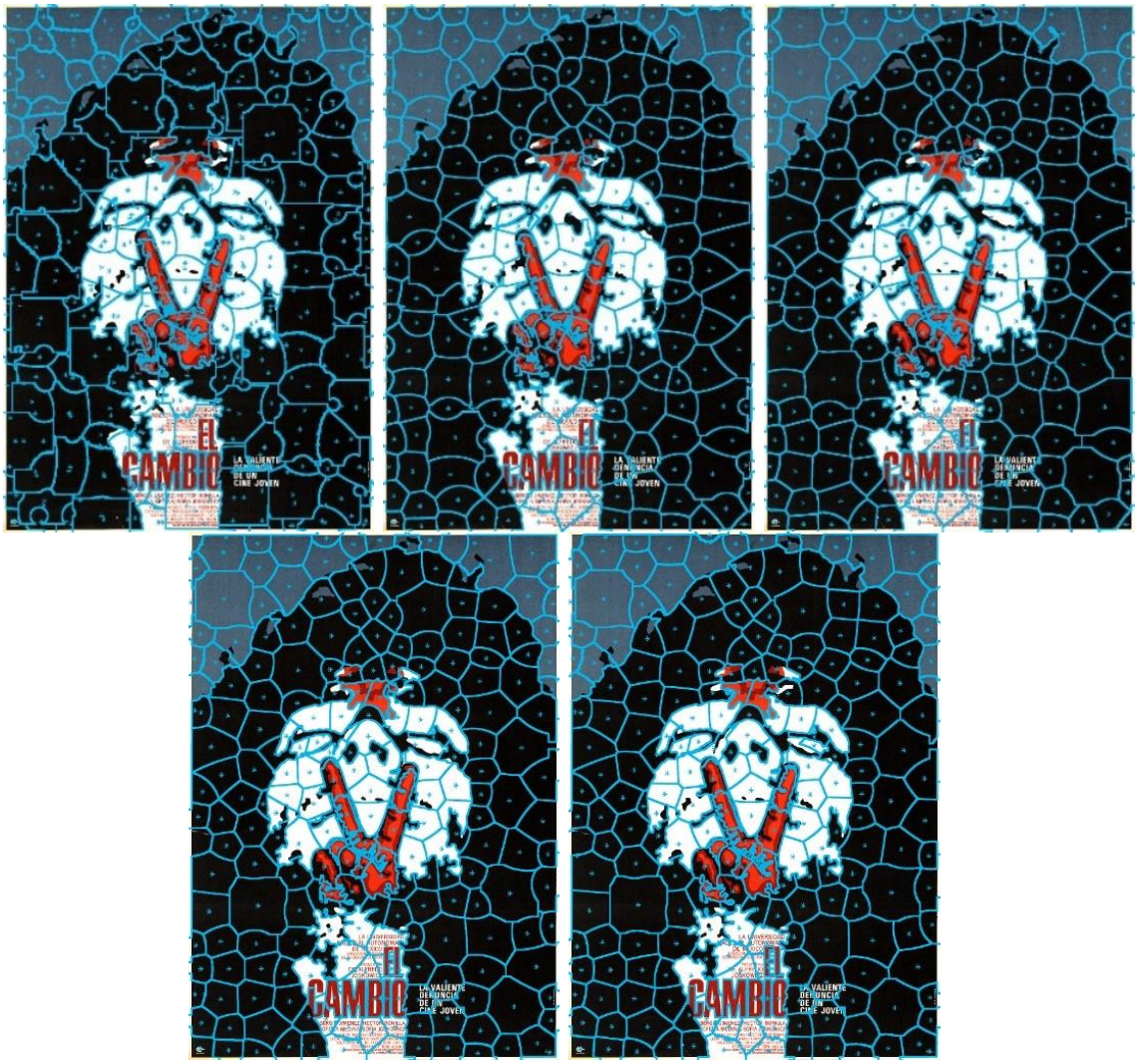


*Figura 2.15 Superpíxeles SLIC en las iteraciones 2, 4, 6, 8 y 10.*

# 2.10. Marca de agua invisible

## 2.10.1. El método RIPEMD–160

El método RIPEMD-160 es una función criptográfica de tipo *hash* iterativa unidireccional que opera con palabras de 32 bits. La función toma como entrada una variable de encadenamiento de 5 palabras y un bloque de mensaje de 16 palabras y los asigna a una nueva variable de encadenamiento. Todas las operaciones se definen en

palabras de 32 bits. En la Figura 2.16 se muestra un ejemplo de lo que se obtiene aplicando el método RIPEMD-160.

*Figura 2.16 Ejemplo de la aplicación del método RIPEMD-160.*

RIPEMD es el acrónimo de RACE *Integrity Primitives Evaluation Message Digest*, es decir, Evaluación de las Primitivas de Integridad del Resumen del Mensaje. Adicionalmente, RACE es el acrónimo de ***R**esearch and Development in **A**dvanced **C**ommunications Technologies in **E**urope*.

Se parte de que el mensaje después del relleno consta de *t* bloques de 16 palabras que se denotarán con $X_i[j]$, con $0 \leq i \leq t-1$ y $0 \leq j \leq 15$. El símbolo $\boxplus$ denota la suma en módulo $2^{32}$ y $rol_s$ denota un desplazamiento cíclico a la izquierda (rotación) sobre las posiciones *s*. A continuación, se proporciona el pseudocódigo para RIPEMD-160 [43]:

*Funciones no lineales a nivel de bit: exor, mux, -, mux, -*

$$\begin{aligned}
f(j,x,y,z) &= x \oplus y \oplus z && (0 \leq j \leq 15)\\
f(j,x,y,z) &= (x \wedge y) \vee (\neg x \wedge z) && (16 \leq j \leq 31)\\
f(j,x,y,z) &= (x \vee \neg y) \oplus z && (32 \leq j \leq 47)\\
f(j,x,y,z) &= (x \wedge z) \vee (y \vee \neg z) && (48 \leq j \leq 63)\\
f(j,x,y,z) &= x \oplus (y \vee \neg z) && (64 \leq j \leq 79)
\end{aligned} \tag{2.42}$$

*Constantes sumadas (hexadecimal)*

$$\begin{aligned}
K(j) &= 00000000_X && (0 \leq j \leq 15)\\
K(j) &= 5A827999_X && (16 \leq j \leq 31) && \lfloor 2^{30} \cdot \sqrt{2} \rfloor\\
K(j) &= 6ED9EBA1_X && (32 \leq j \leq 47) && \lfloor 2^{30} \cdot \sqrt{3} \rfloor\\
K(j) &= 8F1BBCDC_X && (48 \leq j \leq 63) && \lfloor 2^{30} \cdot \sqrt{5} \rfloor\\
K(j) &= A953FD4E_X && (64 \leq j \leq 79) && \lfloor 2^{30} \cdot \sqrt{7} \rfloor\\
K'(j) &= 50A28BE6_X && (0 \leq j \leq 15) && \lfloor 2^{30} \cdot \sqrt[3]{2} \rfloor\\
K'(j) &= 5C4DD124_X && (16 \leq j \leq 31) && \lfloor 2^{30} \cdot \sqrt[3]{3} \rfloor\\
K'(j) &= 6D703EF3_X && (32 \leq j \leq 47) && \lfloor 2^{30} \cdot \sqrt[3]{5} \rfloor\\
K'(j) &= 7A6D76E9_X && (48 \leq j \leq 63) && \lfloor 2^{30} \cdot \sqrt[3]{7} \rfloor\\
K'(j) &= 00000000_X && (64 \leq j \leq 79)
\end{aligned} \tag{2.43}$$

*Selección de la palabra del mensaje*

$$
\begin{aligned}
r(j) &= j \qquad (0 \le j \le 15)\\
r(16..31) &= 7,4,13,1,10,6,15,3,12,0,9,5,2,14,11,8\\
r(32..47) &= 3,10,14,4,9,15,8,1,2,7,0,6,13,11,5,12\\
r(48..63) &= 1,9,11,10,0,8,12,4,13,3,7,15,14,5,6,2\\
r(64..79) &= 4,0,5,9,7,12,2,10,14,1,3,8,11,6,15,13\\
r0(0..15) &= 5,14,7,0,9,2,11,4,13,6,15,8,1,10,3,12\\
r0(16..31) &= 6,11,3,7,0,13,5,10,14,15,8,12,4,9,1,2\\
r0(32..47) &= 15,5,1,3,7,14,6,9,11,8,12,2,10,0,4,13\\
r0(48..63) &= 8,6,4,1,3,11,15,0,5,12,2,13,9,7,10,14\\
r0(64..79) &= 12,15,10,4,1,5,8,7,6,2,13,14,0,3,9,11
\end{aligned}
\tag{2.44}
$$

*Cantidad para girar a la izquierda (rol)*

$$
\begin{aligned}
s(0..15) &= 11,14,15,12,5,8,7,9,11,13,14,15,6,7,9,8\\
s(16..31) &= 7,6,8,13,11,9,7,15,7,12,15,9,11,7,13,12\\
s(32..47) &= 11,13,6,7,14,9,13,15,14,8,13,6,5,12,7,5\\
s(48..63) &= 11,12,14,15,14,15,9,8,9,14,5,6,8,6,5,12\\
s(64..79) &= 9,15,5,11,6,8,13,12,5,12,13,14,11,8,5,6\\
s'(0..15) &= 8,9,9,11,13,15,15,5,7,7,8,11,14,14,12,6\\
s'(16..31) &= 9,13,15,7,12,8,9,11,7,7,12,7,6,15,13,11\\
s'(32..47) &= 9,7,15,11,8,6,6,14,12,13,5,14,13,13,7,5\\
s'(48..63) &= 15,5,8,11,14,14,6,14,6,9,12,9,12,5,15,8\\
s'(64..79) &= 8,5,12,9,12,5,14,6,8,13,6,5,15,13,11,11
\end{aligned}
\tag{2.45}
$$

*Valores iniciales en hexadecimal*

$h_0 = 67452301_{\mathrm{X}}; h_1 = EFCDAB89_{\mathrm{X}}; h_2 = 98BADCFE_X; h_3 = 10325475_{\mathrm{X}}; h_4 = C3D2E1F0_{\mathrm{X}};$

$for\ i\ = 0: t-1$

$A = h_0; B = h_1; C = h_2; D = h_3; E = h_4;$

$A' = h_0; B' = h_1; C' = h_2; D' = h_3; E' = h_4;$

$for\ j\ = 0: 79$

$T = rol_{s(j)}\big(A \boxplus f(j,B,C,D) \boxplus X_i[r(j)] \boxplus K(j)\big) \boxplus E;$

$A = E; E = D; D = rol_{10}(C); C = B; B = T;$

$T' = rol_{s'(j)}\left(A' \boxplus f(79-j,B',C',D') \boxplus X_i\left[r'^{(j)}\right] \boxplus K'(j)\right) \boxplus E';$

$A' = E'; E' = D'; D' = rol_{10}(C'); C' = B'; B' = T';$

$end$

$end$

## *2.10.2. Optimización con un método de enjambre de partículas (PSO).*

"El método de enjambre de partículas (*Particle Swarm Optimization*, PSO) es un método de optimización heurística orientado a encontrar los mínimos o los máximos globales. Su funcionamiento está inspirado en el comportamiento que tienen las parvadas, o los bancos de peces en los que, el movimiento de cada individuo (dirección, velocidad, aceleración, etc.), resulta de la combinación de las decisiones individuales de cada uno, pero correlacionado con el comportamiento del resto" [44].

En términos generales el algoritmo de la optimización por enjambre requiere una función objetivo y un criterio de parada. Éste empieza con la creación de un enjambre inicial donde se conoce la posición y velocidad de cada partícula; después se evalúa la posición de cada partícula con la función objetivo; finalmente se actualiza la posición y velocidad de cada partícula [45]. En la Figura 2.17 se muestran las etapas del algoritmo de optimización mediante el método de enjambre de partículas.

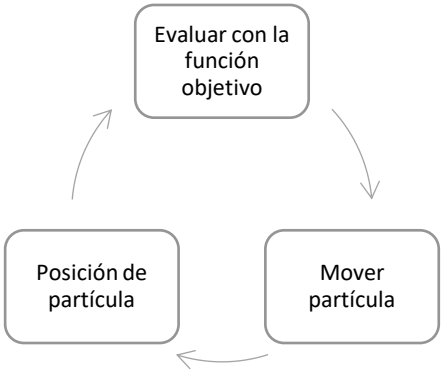



*Figura 2.17 Diagrama general de la optimización por el método de enjambre de partículas.*

La actualización de la velocidad de cada partícula se realiza mediante la ecuación

$$v_i\,(t+1) = \omega v_i(t) + r_1 C_1 (p_i(t) - x_i\,(t)) + r_2 C_2\,(g(t) - x_i\,(t)) \qquad (2.46)$$

Donde:

$v_i\,(t+1)$ = Velocidad de la partícula $i$ en el momento $t+1$.

$v_i(t)$ = Velocidad de la partícula $i$ en el momento $t$.

$\omega$ = Coeficiente de inercia, reduce o aumenta la velocidad de la partícula.

$C_1$ = coeficiente cognitivo.

$C_2$ = coeficiente social.

$r_1\ y\ r_2$ = vectores de valores aleatorios entre 0 y 1 de longitud igual al vector de velocidad.

$p_i(t)$ = mejor posición en la que ha estado la partícula $i$ hasta el momento.

$x_i\ (t)$ = posición de la partícula $i$ en el momento $t$.

$g(t)$ = posición de todo el enjambre en el momento $t$, el mejor valor global.

La actualización de la posición de cada partícula se realiza mediante la ecuación

$$v_i\ (t+1) = x_i(t) + v_i(t+1) \tag{2.47}$$

Para controlar el coeficiente de inercia

$$\omega_t = (\omega_{max} - \omega_{min})\frac{t_{max} - t}{t_{max}} + \omega_{min} \tag{2.48}$$

Donde:

$\omega_t$ = Coeficiente de inercia en la iteración $t$.

$\omega_{max}$ = Coeficiente de inercia máximo. Valor con el que se inicia el algoritmo (0.9 recomendado).

$\omega_{min}$ = Coeficiente de inercia mínimo. Valor que se alcanza en la última iteración (0.4 recomendado).

$t_{max}$ = Número máximo de iteraciones.

## 2.11. Protección de la autoría.

Existen varios conceptos que están estrechamente relacionados con la protección de la autoría y que pueden confundirse muy fácilmente. Con el propósito tener claros estos conceptos a continuación se definen brevemente los principales.

**Derecho moral**

"El derecho moral es el derecho intrínseco de todo autor a ser reconocido como tal, a decidir el momento de la divulgación y evitar deformaciones, o mutilaciones, de su obra, entre otros. Es imprescriptible, inalienable, inembargable e irrenunciable" [46].

**Derecho de autor (*Copyright*)**

"El derecho de autor o copyright es el conjunto de normas y principios jurídicos que certifican los derechos patrimoniales y morales que la ley confiere a los autores, por

el simple hecho de la creación de una obra musical, artística, didáctica o científica, ya sea que esté publicada o sea inédita" [47].

El derecho de autor reconoce al creador del trabajo y su derecho natural sobre su trabajo. El derecho moral es parte del derecho de autor. Es el derecho a exigir el respeto a la integridad de la obra y a la no alteración de la misma (Ministerio de Cultura) [48].

**Propiedad intelectual**

La propiedad intelectual hace referencia a un bien económico y/o cultural que puede incluir tanto productos intangibles como productos tangibles, es reconocida en las legislaciones de mayoría de los países y es susceptible de ser explotada económicamente por los dueños legales de dicha propiedad. Jurídicamente la propiedad intelectual, es todo aquello que se encuentra protegido por las leyes de propiedad intelectual, por lo que cualquier producción intelectual que no se encuentre explícitamente dentro de la legislación correspondiente no puede considerarse propiedad intelectual dentro del marco jurídico. De esta manera, los derechos de propiedad intelectual salvaguardan los intereses de los creadores al darles prerrogativas en relación con sus creaciones [49].

**Derecho patrimonial, o derecho de reproducción**

El derecho patrimonial es la potestad que tiene el autor para explotar por sí mismo su obra, al igual que dar la autorización o prohibición, de la explotación a terceros en cualquier forma dentro de los límites que establece la Ley Federal del Derecho de Autor. A diferencia del derecho moral, este derecho se puede transferir por escrito, es temporal y necesariamente oneroso [46].

Según el diccionario *copyright* es "el derecho exclusivo de una persona de reproducir, publicar, o vender su trabajo de autoría original (como un trabajo literario, musical, dramatúrgico, artístico, o arquitectónico, etc.)" [50].

**El copyright varía según la legislación de los diferentes países:**

En los EEUU el *copyright* es una forma de protección de la propiedad intelectual provista por las leyes de ese país. La protección de derechos de autor está disponible para trabajos de autoría original que sean fijados en una forma tangible, sin importar que sean publicados, o no. Las categorías de trabajos que pueden ser protegidos por las leyes del *copyright* incluyen pinturas, trabajos literarios, espectáculos en vivo, fotografías, películas y software. [47]

En España el *copyright* abarca exclusivamente los derechos patrimoniales de un trabajo, es decir, los derechos estrictamente económicos, porque se considera al trabajo como un producto de consumo, de modo que su dueño pueda traspasar su propiedad a otro mediante una transacción comercial, un regalo, una herencia, etc. [48]

En México el *copyright* (derecho de autor) es el registro que concede el Estado a todos los creadores de obras artísticas y literarias, en virtud del cual el autor goza de derechos tanto de tipo personal, también conocido como derecho moral, como derechos económicos, que constituyen un derecho patrimonial [46].

## 2.12. Patrimonio cultural

La inclusión en la definición de patrimonio cultural ha evolucionado a lo largo del tiempo, desde lo tangible basándose en criterios objetivos hasta lo intangible basándose en criterios subjetivos.

Cronológicamente se han ido añadiendo conceptos a la definición de patrimonio cultural. Monumentos históricos, alrededores[5], sitios, patrimonio rural, jardines y paisajes históricos, ciudades históricas, folclore y cultura tradicional, patrimonio cultural sumergido, patrimonio vernáculo construido, patrimonio cultural intangible.

La definición de monumento histórico aplica tanto a las grandes obras de arte, como a las obras más modestas del pasado que han alcanzado importancia con el paso del tiempo [51].

"El patrimonio cultural es la herencia cultural propia del pasado de una comunidad, mantenida hasta la actualidad y transmitida a las generaciones presentes"[6]. En la actualidad incluye tanto lo material, como lo inmaterial[7].

**Conservación del patrimonio cultural**

La conservación y la restauración son dos actividades que están íntimamente relacionadas, ambas están dedicadas para procurar la permanencia de patrimonio de la humanidad. La conservación implica el resguardo en determinadas condiciones del patrimonio para mantenerlo en buen estado, mientras que la restauración involucra una reparación, o arreglo, del patrimonio.

[5] Considera no solamente el monumento sino también los alrededores y el medio ambiente donde se encuentra situado.
[6] http://whc.unesco.org/en/about/
[7] www.unesco.org/culture/ich/index.php?pg=00022

Se debe considerar que no todas las comunidades le dan el mismo peso al patrimonio material ni lo conservan y restauran de la misma manera. En África este tipo de patrimonio representa apenas un 20%. En Japón no hay interés alguno en conservar el material original de los monumentos, se da preferencia al conocimiento vinculado a su creación [51], muchos monumentos se reconstruyen en su totalidad cada cierto tiempo con materiales nuevos siguiendo las técnicas originales.

Las nuevas tecnologías se han ido incorporando a ambas actividades [52]. En particular en el caso de las fotografías existe un reto tecnológico implícito, su potencial comunicativo y expresivo está definido, y limitado, por su gran vulnerabilidad al deterioro y la fragilidad de los materiales que las constituyen [53]. La digitalización es un medio que se puede emplear tanto para la conservación como para la restauración de las fotografías y otros medios impresos.

En la presente investigación se trabajó con fotografías y carteles de cine digitalizados para su conservación y su posterior transmisión a generaciones presentes, y futuras.

# 3. Algoritmo propuesto

En el algoritmo mostrado en la Figura 3.1, las imágenes son protegidas mediante la incrustación de marcas de agua, una marca visible y una invisible, con el objetivo de poder detectar usos no permitidos de las imágenes. La estrategia de marcado de agua digital está definida de la manera que una marca visible camuflada, resistente a los procesos de impresión y escaneo, puede identificarse mediante la inspección visual directa para posteriormente detectar la existencia de la marca de agua invisible y detectar un uso no deseado de las imágenes.

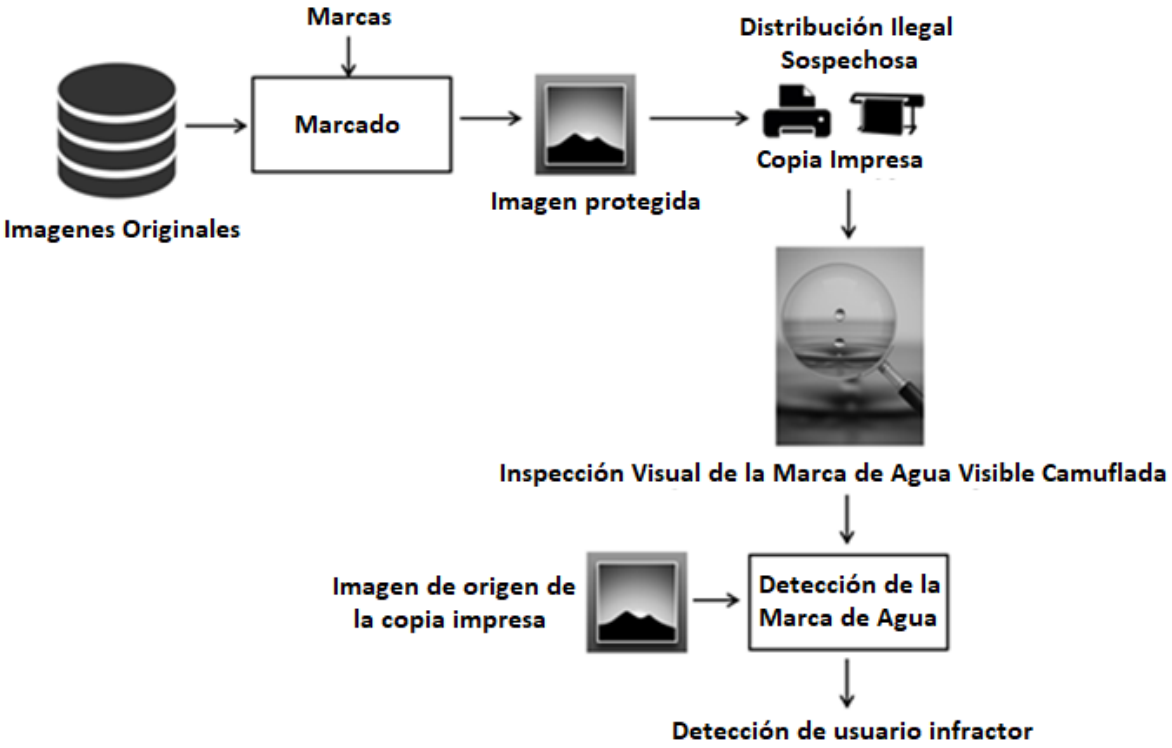



*Figura 3.1 Diagrama general del algoritmo propuesto.*

## 3.1. Planteamiento del problema

El propósito del algoritmo propuesto es proteger imágenes pertenecientes al patrimonio cultural del cine mexicano, para demostrar la propiedad y rastreo de copias distribuidas bajo permisos específicos, resistiendo a uno de los ataques que constituye uno de los mayores retos tecnológicos, como es la impresión y escaneo. La marca propuesta es una marca dual, conformada por una marca en el dominio espacial, visible camuflada, robusta, ciega y asimétrica, y una marca invisible en el dominio de Fourier.

Las imágenes objetivo son imágenes digitalizadas a partir de formatos físicos antiguos, fotografías y carteles de cine. La base de datos utilizada está conformada por 923 las imágenes digitales que están en escala de grises ($2^8$) y 11 en color, en formato TIFF.

Las imágenes son de gran resolución con dimensiones $M \times N$; $\min_I(M) = 1509$, pertenece a una imagen de 1509x1962; $\min_I(N) = 1952$, pertenece a una imagen de 3133x1952; $\max_I(M) = 6798$ y $\max_I(M) = 8409$ pertenecen a la misma imagen de dimensiones 6798x8409. Lo que implica que la base de imágenes es heterogénea y está conformada de imágenes en posición tanto horizontal como vertical y cuyos tamaños varían entre 1500 y 8000 pixeles aproximadamente.

Adicionalmente el contenido de las imágenes es también bastante heterogéneo, como se puede observar en la Figura 3.2, pudiendo ser retratos, paisajes, escenarios citadinos, multitudes y hasta incluir animales. Lo cual dificulta aprovechar el contenido para desarrollar el algoritmo de marcado.

(a) (b) (c) (d)

*Figura 3.2 Imágenes de muestra del conjunto de datos. (a) Imagen obtenida de la película "Dos monjes", (b) Imagen obtenida de la película "La mancha de sangre", 1937, (c) Imagen obtenida de la película "Redes", 1936, y (d) Imagen obtenida de "Vamonos con Pancho Villa", película de 1936 (los títulos de las películas están entre comillas y en español). Utilizando un conjunto de datos Fotografías cortesía de Filmoteca, propiedad de Filmoteca UNAM.*

## 3.2. Parámetros de entrada

Como se puede apreciar en la Figura 3.1, las entradas del algoritmo propuesto son las imágenes originales (sin marcar), y las marcas de agua escogidas.

**Imagen original $I_o$**

En el punto 3.1 se describieron las características del conjunto de imágenes utilizadas, que consta de más de 900 imágenes pertenecientes al cine mexicano

proporcionadas por la Filmoteca de la UNAM. La imagen empleada para ilustrar el desarrollo del marcado visible camuflado se muestra en la Figura 3.3; es una imagen en escala de grises, en formato TIFF, cuyas dimensiones en pixeles son $I_{tam} = [M, N] = [2872, 3751]$.

*Figura 3.3 $\boldsymbol{I_o}$ Imagen familia inuit.*[8]

**Marca visible $\boldsymbol{W1}$**

La marca visible empleada puede ser cualquier imagen binaria cuadrada, de tamaño $n \times n$. La marca debe ser una imagen con significado contextual, para fines prácticos se eligió la letra "F" (de filmoteca), mostrada en la Figura 3.4.

*Figura 3.4 Marca binaria $\boldsymbol{W1_o}$.*

[8]https://es.wikipedia.org/wiki/Archivo:Inupiat_Family_from_Noatak,_Alaska,_1929,_Edward_S._Curtis_(restored).jpg

El escudo de la UNAM, los logos de Difusión Cultural, y el logo de la Filmoteca (Figura 3.5). También fueron aplicadas como marcas visibles camufladas para la obtención de los resultados del capítulo 4.

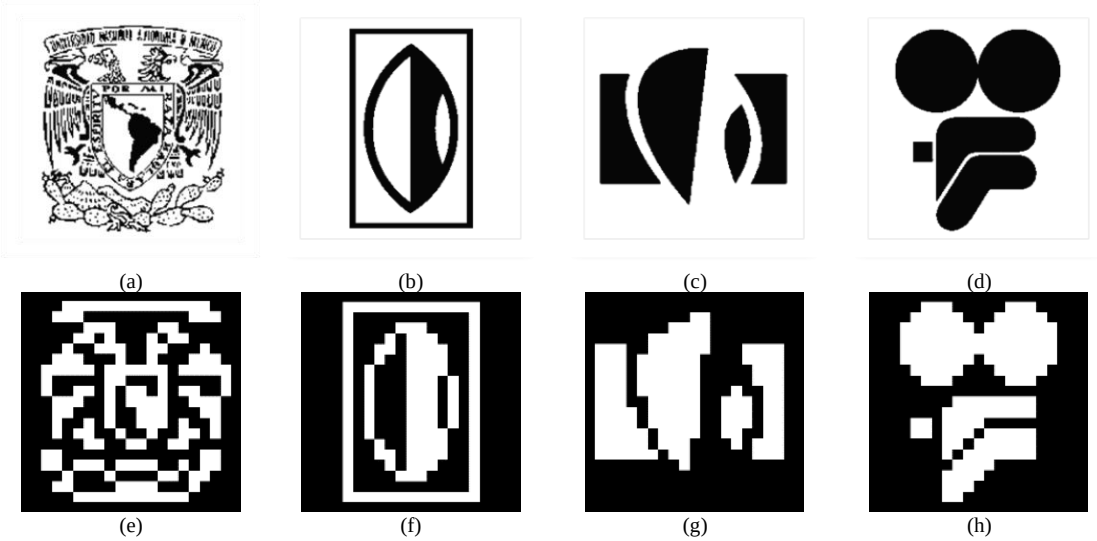



*Figura 3.5 Marcas de agua binarias cuadradas, tamaño $n \times n = 250 \times 250$ píxeles con fondo blanco (línea superior) y marcas de agua binarias cuadradas, tamaño $n \times n = 21 \times 21$ píxeles con fondo negro (línea inferior). De izquierda a derecha escudo UNAM (a y e), logos de Difusión Cultural (b,f,c, yg) y logo de Filmoteca (d y h). Las imágenes son propiedad de la UNAM.*

**Tamaño de la marca visible**

El valor de $n$ se ajusta proporcionalmente con el tamaño de $\boldsymbol{I_o}$, de acuerdo a la ecuación [54] (3.1):

$$n = \left\lfloor \frac{\Delta}{0.125} \right\rfloor \tag{3.1}$$

Donde:

$$\begin{aligned} r_M &= \max(I_{tam})/\max(D_t) \\ r_m &= \min(I_{tam})/\min(D_t) \\ \Delta &= \max(r_M, r_m) \end{aligned} \tag{3.2}$$

En la ecuación (3.2), $D_t = [719, 529]$ son las dimensiones en pixeles del formato "revista" también conocido como "*digest*", que en su versión impresa con una resolución de 96 puntos por pulgada (dpi) corresponden a un área de 14 × 19 cm. Se toma como referencia el formato *digest* debido a que es el tamaño más pequeño conveniente de impresión de uso extendido mundialmente.

En concordancia con el formato *digest* se usa una marca de tamaño 8x8 [54]; el valor de 0.125 de la ecuación (3.1) se debe al tamaño de la marca de referencia, $8^{-1}$. En el caso de la imagen $I_o$ de la Figura 3.3, $I_{tam} = 2872 \times 3751$ y $n = 41$.

**Marca invisible $W2$**

La marca invisible es un mensaje de 160 bits generado mediante una función criptográfica de *hash*, que se forma con datos del usuario y/o propietario y los datos numéricos correspondientes a la llave secreta $K1$, obtenidos de la incrustación de la marca visible.

## 3.3. Marcado dual

La marca dual propuesta en el presente trabajo está conformada por dos etapas principales de marcado, recuadro azul de la Figura 3.6; una inspección visual para detección de la marca visible $W1$, recuadro naranja de la Figura 3.6; una extracción para la recuperación de la marca invisible $W2$; y la determinación de un uso no permitido, recuadro rosa de la Figura 3.6.

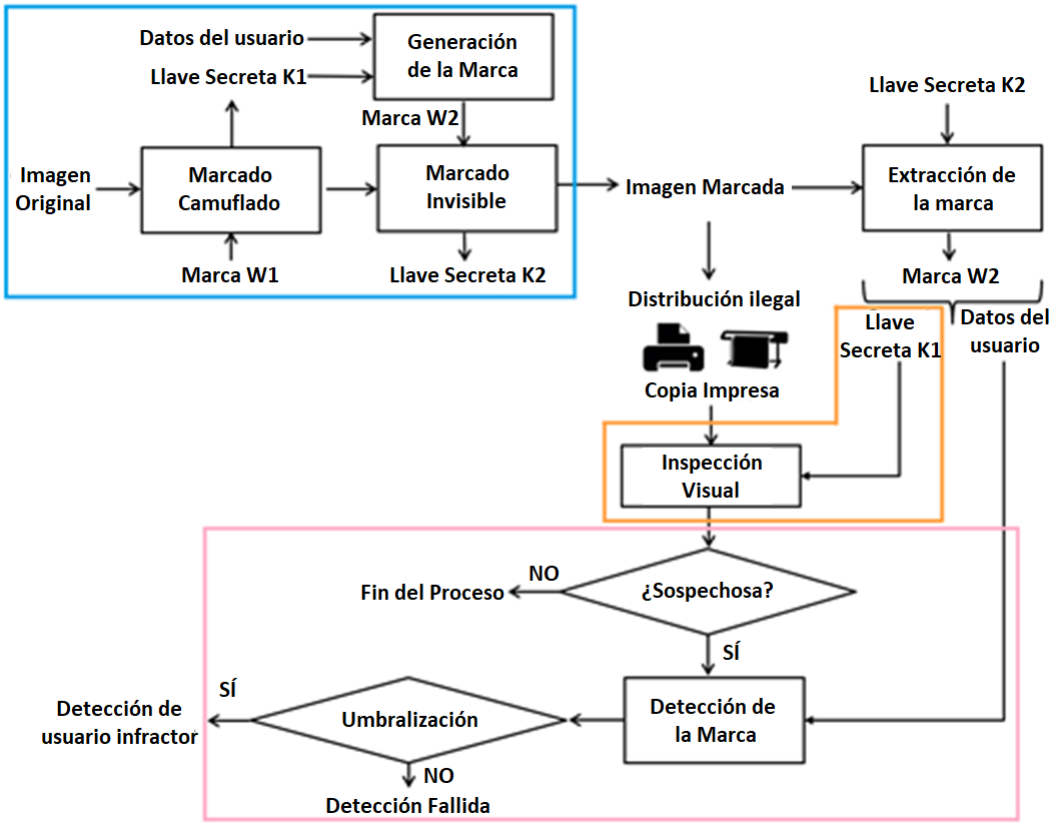



*Figura 3.6 Diagrama de bloques del método híbrido de doble marca de agua propuesto.*

## 3.3.1. Marcado visible

En la Figura 3.7 se muestra el diagrama de bloques del algoritmo de marcado visible camuflado.

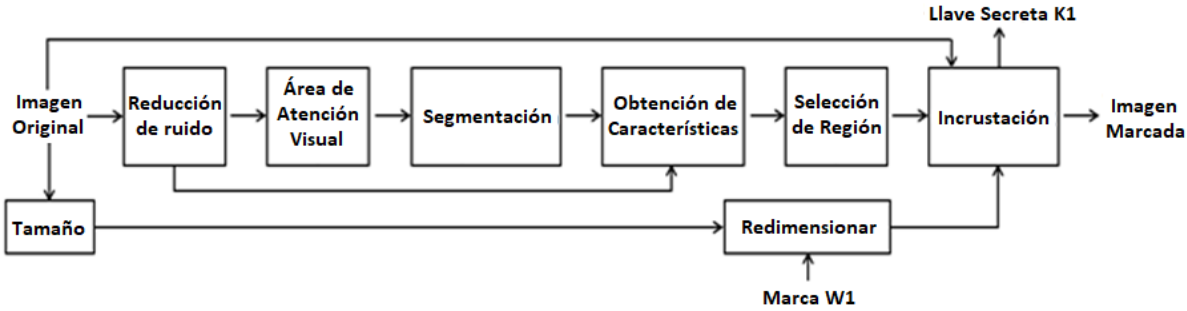



*Figura 3.7 Diagrama de bloques del marcado visible camuflado.*

**Reducción de ruido (TV-L1)**

Mediante el modelo de variación total L1, TV-L1 [19], se descompone a la imagen original en una imagen de estructura $I_e$ y una imagen de textura $I_t$. Dicha descomposición es favorable ya que reduce el ruido de las imágenes, lo cual es deseable debido a la naturaleza de las imágenes de nuestra base de datos.

La función TV-L1 se aplica a $I_o$ con los parámetros determinados de manera empírica $\lambda = 0.1$ y el número de iteraciones $it = 10$. En la Figura 3.8 se muestra la $I_e$ y en la Figura 3.9 se muestra la $I_t$ resultantes.

Para efectos prácticos se usan los valores binarizados de la imagen de textura, $\boldsymbol{I_t}$. Donde, el umbral de binarización para la imagen de textura se obtiene con el método de Otsu [55], y como se explicó anteriormente corresponde al valor del umbral que optimiza los dos segmentos en términos de la varianza. La Figura 3.10 muestra la binarización de la imagen de textura mostrada en la Figura 3.9.

*Figura 3.8 Imagen de estructura $I_e$.*

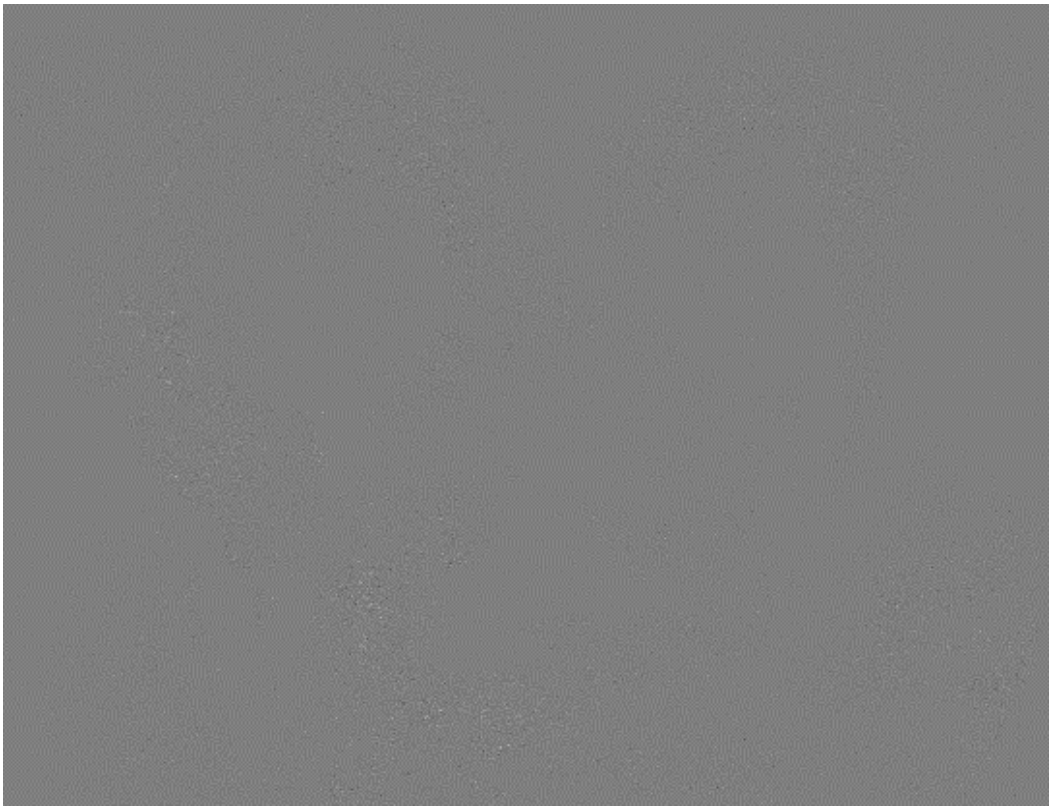


*Figura 3.9 Imagen de textura $I_t$.*

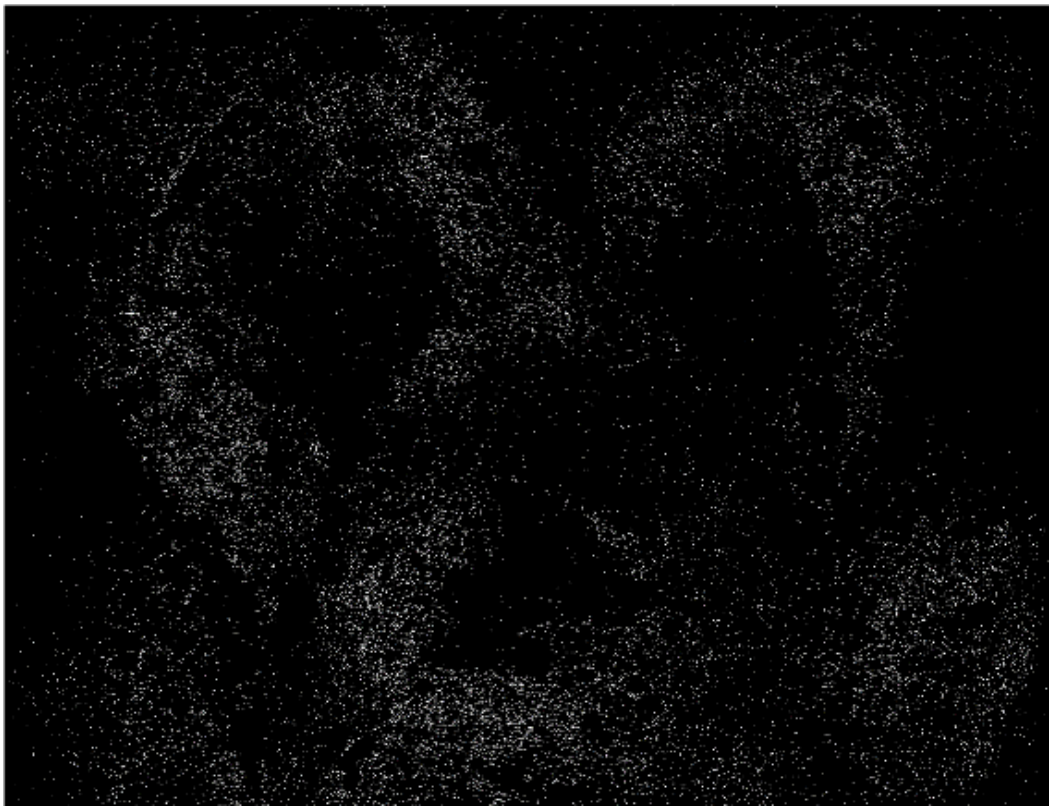


*Figura 3.10 Imagen de textura binarizada* $\boldsymbol{I_{t_{bin}}}$.

**Área de atención visual (AV)**

El mapa de saliencia $AV_m$ destaca las zonas de la imagen que llaman la atención visual humana. Para obtener $AV_m$ se aplica la función de saliencia AV, utilizando el método descrito en [26], con $\sigma = 7$. En la Figura 3.11 se muestra el mapa de saliencia obtenido.

Para crear la máscara de atención visual $\boldsymbol{AV_{m_{bin}}}$, se binariza el mapa de saliencia $AV_m$, con un umbral de 0.3, determinado empíricamente. En la Figura 3.12 la región blanca representa el área de atención visual de la imagen de la Figura 3.3.

La ventaja del área de atención visual es que, en términos de un ataque intencional, tiene menos probabilidades de sufrir recortes, lo que le proporciona robustez al algoritmo.

*Figura 3.11 Mapa de saliencia $AV_m$.*

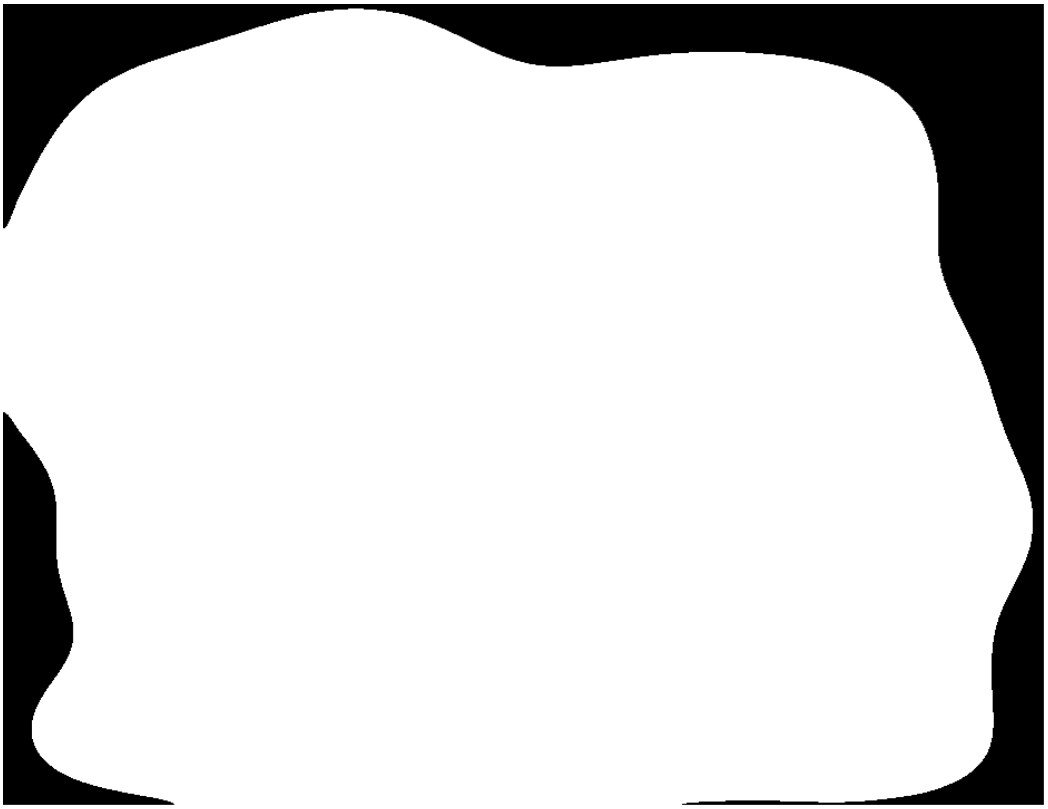


*Figura 3.12 Máscara de atención visual $\boldsymbol{AV_{m_{bin}}}$.*

Los **pixeles** de imagen de estructura **dentro del área de atención visual** $\boldsymbol{I_{eAV}}$ y los pixeles de imagen de textura dentro del área de atención visual $\boldsymbol{I_{tAV}}$, se obtienen mediante las ecuaciones (3.3) y (3.4), respectivamente. Asimismo, el resultado visual se muestra en la Figura 3.13 y la Figura 3.14.

$$I_{eAV} = \boldsymbol{AV_{m_{bin}}} \times I_e \tag{3.3}$$

$$I_{tAV} = \boldsymbol{AV_{m_{bin}}} \times I_t \tag{3.4}$$

*Figura 3.13 Pixeles de estructura dentro del área de atención visual* $\boldsymbol{I_{eAV}}$.

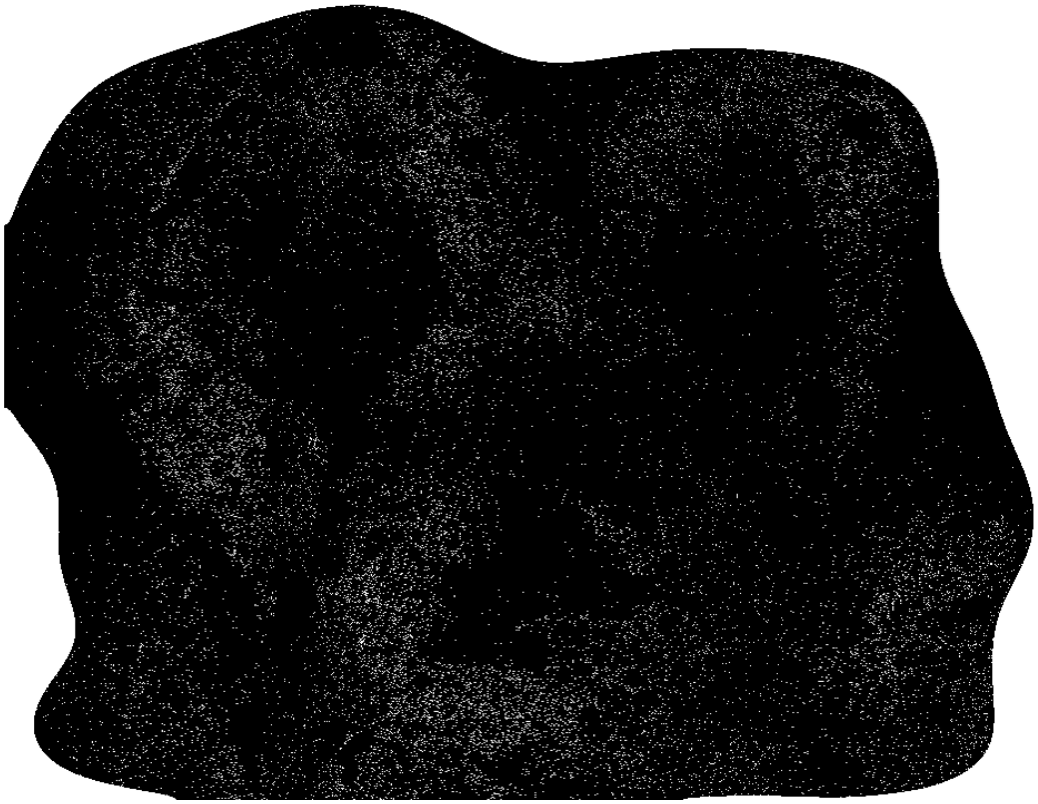


*Figura 3.14 Pixeles de textura dentro del área de atención visual $\boldsymbol{I_{tAV}}$.*

**Segmentación**

La función superpíxeles SP, que usa el algoritmo SLIC (*Simple Linear Iterative Clustering*) [41], segmenta la imagen en $k$ súper pixeles que reúnen pixeles cercanos con características similares. El número de súper pixeles $k$ lo vinculamos con las dimensiones de la imagen portadora, $M \times N$, y de la marca, $n \times n$, como indica la ecuación (3.5) para asegurar regiones de buen tamaño para la incrustación de la marca.

$$k = \frac{(M \times N)}{\lfloor n \times 2 \rfloor^2} \tag{3.5}$$

La división del área de atención visual usando SP da como resultado la máscara de superpíxeles $\boldsymbol{SP_m}$, mostrada en la Figura 3.15 con 1344 súper píxeles. Al aplicar la máscara $\boldsymbol{SP_m}$ a $\boldsymbol{I_{eAV}}$ y a $\boldsymbol{I_{tAV}}$, se obtiene una división de los pixeles, $\boldsymbol{SP_{eAV}} = \boldsymbol{SP_m}(\boldsymbol{I_{eAV}})$ y $\boldsymbol{SP_{tAV}} = \boldsymbol{SP_m}(\boldsymbol{I_{tAV}})$, dentro del área de atención visual como muestra en la Figura 3.16 y la Figura 3.17, respectivamente.

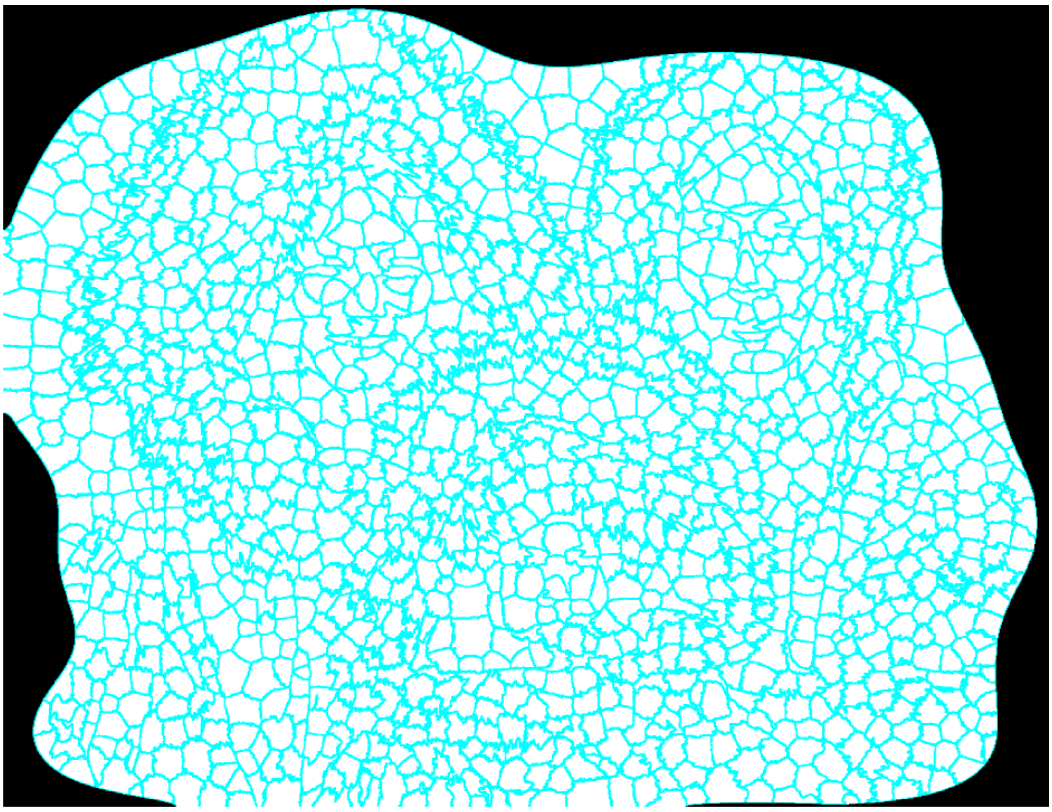


*Figura 3.15 Máscara de súper pixeles $\boldsymbol{SP_m}$.*

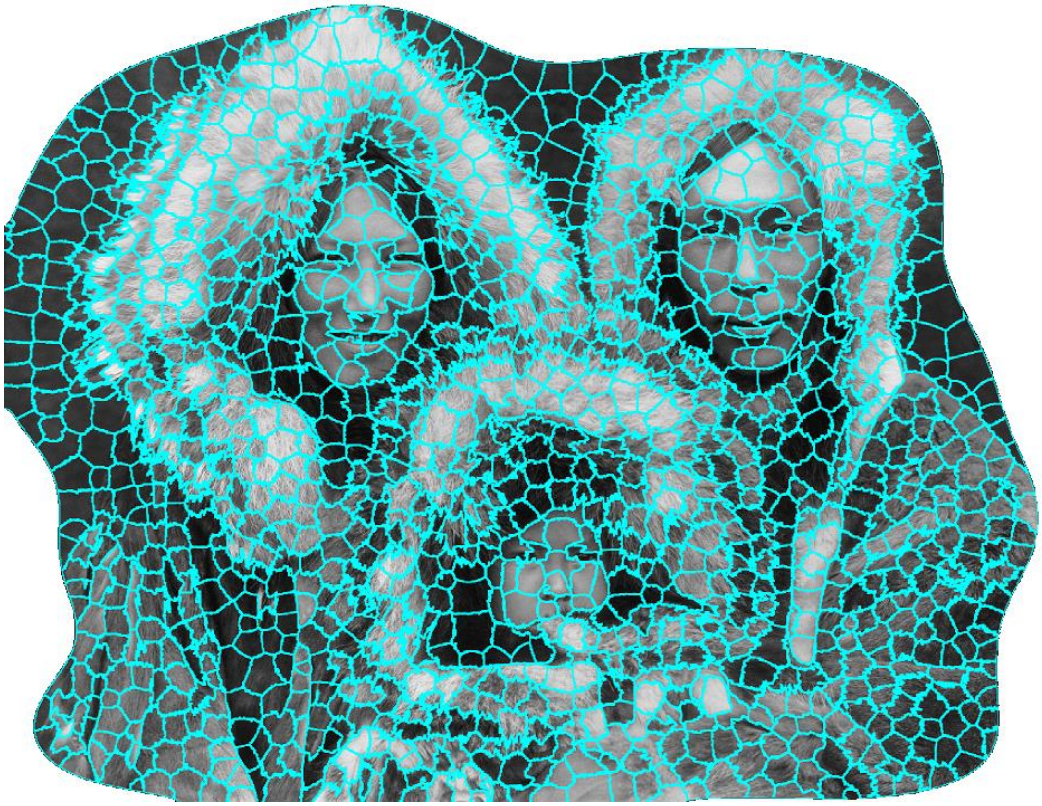


*Figura 3.16 $\boldsymbol{I_{eAV}}$ dividida en súper pixeles, $\boldsymbol{SP_{eAV}}$.*

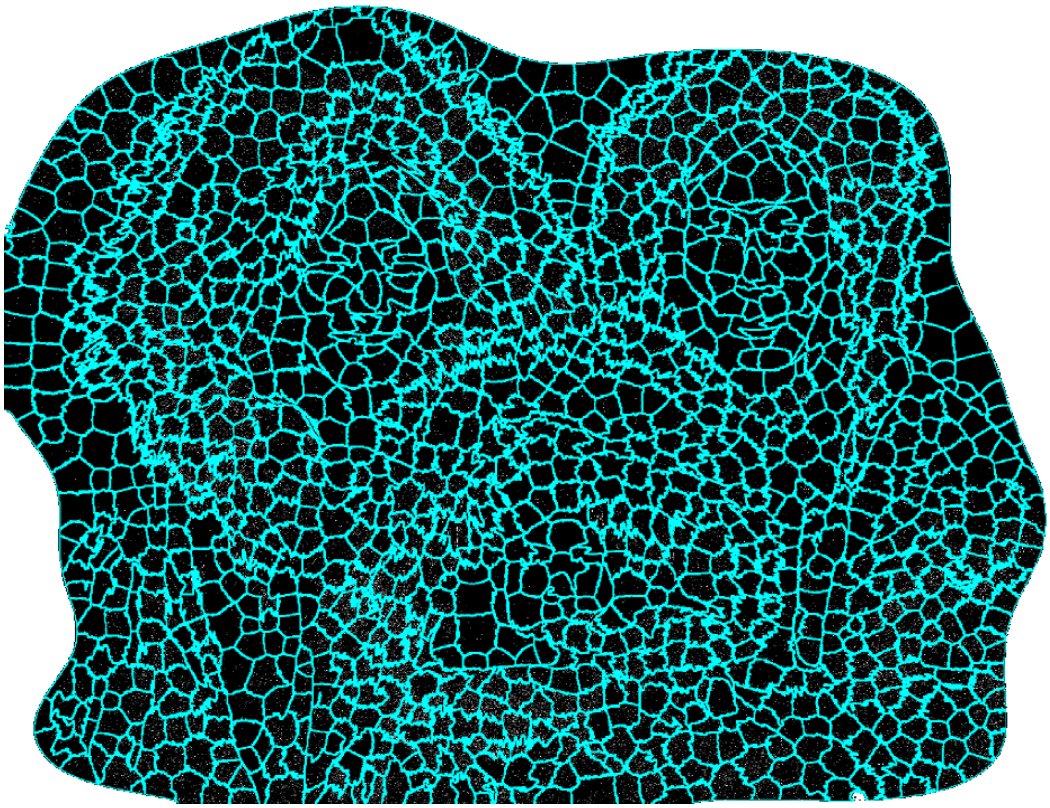


*Figura 3.17 $\boldsymbol{I_{tAV}}$ dividida en súper pixeles, $\boldsymbol{SP_{tAV}}$.*

**Vectores de características ($\boldsymbol{V_c}$)**

A partir de los súper pixeles de las imágenes de estructura $\boldsymbol{SP_{eAV}}$ y textura $\boldsymbol{SP_{tAV}}$, obtenemos parámetros numéricos que conforman el vector de características $\boldsymbol{V_c}$ de cada súper pixel representado por la ecuación (3.6):

$$V_c = [SP_{tam}, SP_{ent}, SP_{var}, SP_{sum}, SP_{prom}] \tag{3.6}$$

Los métodos para obtener los parámetros numéricos del i-ésimo SP se listan en la Tabla 3.1. Donde $SP_{tam}$ es el número de pixeles, $SP_{ent}$ es la entropía, $SP_{var}$ es la varianza, $SP_{sum}(i)$ es el promedio de los pixeles blancos de la imagen de textura binarizada [0,255], y $SP_{prom}$ es el valor promedio de gris.

*Tabla 3.1. Parámetros numéricos para toda $i$ dentro del área de atención visual.*

| Tamaño | Textura | Tonos de gris |
|---|---|---|
| $SP_{tam}(i) = numel(SP_{eAV}(i))$ | $SP_{ent}(i) = H(SP_{tAV}(i))$<br>$SP_{var}(i) = \sigma^2(SP_{tAV}(i))$<br>$SP_{sum}(i) = \overline{SP_{tAV}(i))}$ | $SP_{prom}(i) = \mu(SP_{eAV}(i))$ |

**Selección del SP**

Una vez obtenidos los vectores de características $\boldsymbol{V_c}$ de cada SP se descartan los súper pixeles que se encuentren dentro de los rangos señalados en (3.7):

$$\begin{gathered} SP_{tam}(i) < (n \times 1.5)^2 \\ SP_{sum}(i) \leq 35 \ \| \ SP_{sum}(i) \geq 105 \\ SP_{prom}(i) \leq 60 \ \| \ SP_{prom}(i) \geq 190 \end{gathered} \tag{3.7}$$

En primera instancia se eliminan los SP demasiado pequeños, es decir aquellos cuya área sea menor a 2.25 veces del área de la marca que se insertará.

El siguiente parámetro de eliminación es uno de los valores de textura $SP_{num}$, que es el promedio de pixeles blancos dentro de cada SP, debido a que dicho parámetro se toma de la imagen de textura binarizada, si el valor es muy bajo, o muy alto, significa que la textura es demasiado lisa y no nos sirve para camuflar la marca, por lo que empíricamente y midiendo las características de regiones óptimas se eligió eliminar todos los SP que tuvieran un valor por debajo de 35, o por arriba de 105.

De igual manera se procedió con el valor de promedio de gris, ya que, si su valor es muy alto, o muy bajo, no es óptimo para la inserción de la marca.

Por último, se ordenan los vectores de mayor a menor, de forma separada para los valores de $SP_{var}$ y $SP_{ent}$, posteriormente se intersecan y se elige el primer SP listado como el óptimo. En la Figura 3.18 se muestra el súper pixel seleccionado en rojo.

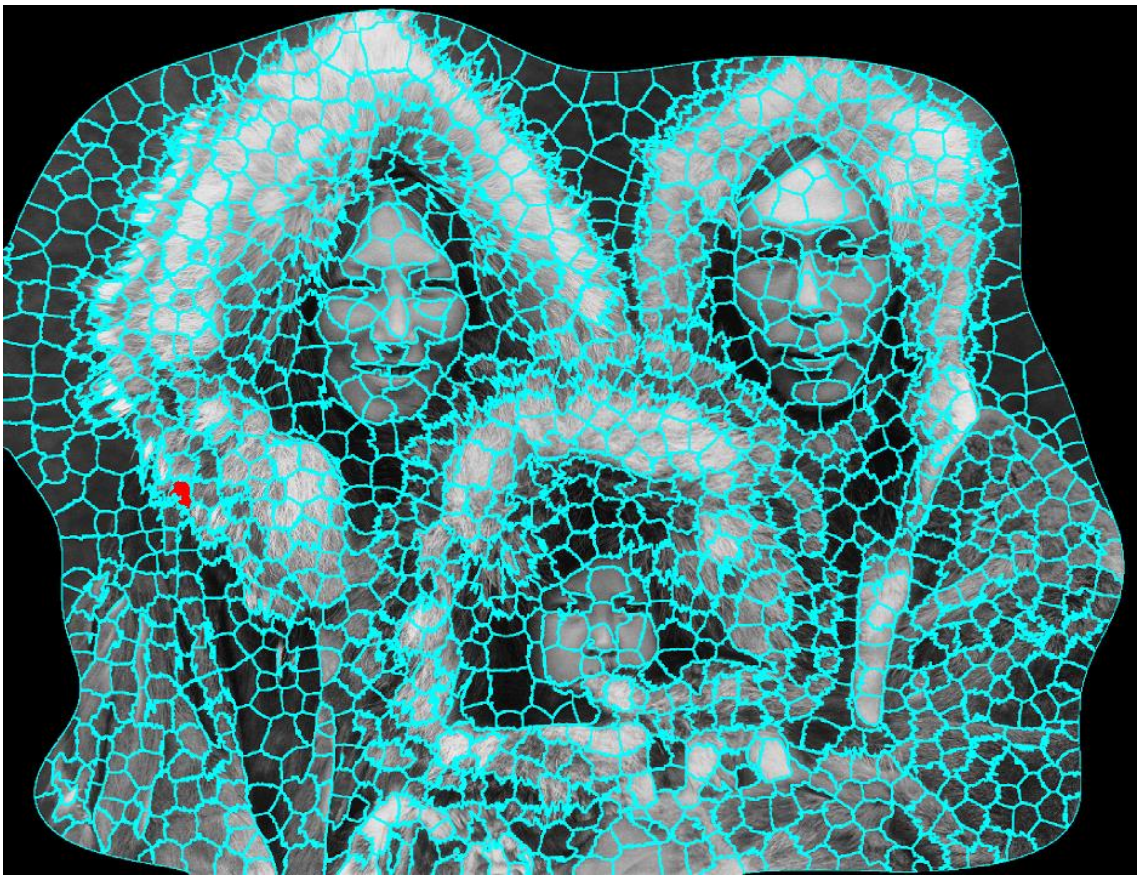


*Figura 3.18 Súper Pixel elegido.*

**Incrustación**

Antes de proceder a la incrustación, se hace un último ajuste a la marca, dependiendo del valor del $SP_{prom}$ elegido, se decide si usar la marca original mostrada en la Figura 3.4, o su complemento mostrado en la Figura 3.19; con el propósito de favorecer a la robustez, está selección se hace siguiendo la ecuación (3.8).

*Figura 3.19 Complemento de $W_o$.*

$$W_o = \begin{cases} W_N \rightarrow (\overline{\boldsymbol{W_N}} \leq \overline{\boldsymbol{W_B}} \,\&\, \overline{SP_s} \in [127.5,\ 255]) \parallel (\overline{\boldsymbol{W_N}} > \overline{\boldsymbol{W_B}} \,\&\, \overline{SP_s} \in [0,\ 127.5) \\ W_B \rightarrow (\overline{\boldsymbol{W_N}} \leq \overline{\boldsymbol{W_B}} \,\&\, \overline{SP_s} \in [0,\ 127.5) \parallel (\overline{\boldsymbol{W_N}} > \overline{\boldsymbol{W_B}} \,\&\, \overline{SP_s} \in [127.5,\ 255]) \end{cases} \tag{3.8}$$

Como umbral se seleccionó el punto medio de los valores que puedan tomar los pixeles de la imagen.

Entonces se encuentra el centroide del SP elegido y se hace coincidir con el centro de la marca, la incrustación se lleva a cabo usando la ecuación (3.9).

$$I_w = \alpha \times I_o + \beta \times W_o \tag{3.9}$$

Donde $\alpha = 0.85$ y $\beta = 0.15$, valores seleccionados empíricamente con la finalidad de proporcionar suficiente fuerza de incrustación de la marca (robustez) conservando un buen camuflaje (imperceptibilidad).

**Imagen marcada $I_w$.**

Una vez hecha la incrustación, la marca de agua debe pasar inadvertida por cualquier observador que ignoré su existencia. En la Figura 3.20 se muestra la imagen marcada $I_w$ con el método descrito junto con la ampliación de la marca incrustada.

Los valores obtenidos de las métricas usadas para este ejemplo son: SSIM=0.99995 y PSNR=58.25374. Lo que indica que la imperceptibilidad de la marca es muy buena.

*Figura 3.20 Imagen marcada $I_w$ y marca incrustada ampliada.*

**Llave secreta $K1$**

En el caso de la marca visible camuflada, se obtiene la llave secreta $K1$ que indica la ubicación de la marca $W1$. La llave secreta $K1$ puede ser visual, una imagen reducida en formato JPG con un recuadro señalando la ubicación; y/o numérica, una coordenada cartesiana que indica en porcentaje la ubicación de la marca, tomando como origen la esquina superior izquierda, como se muestra en la Figura 3.21.

*Figura 3.21 Llave secreta $K1$.*

## 3.3.2. Marcado de agua invisible

En la Figura 3.22 se muestra el diagrama de bloques del algoritmo de marcado invisible.

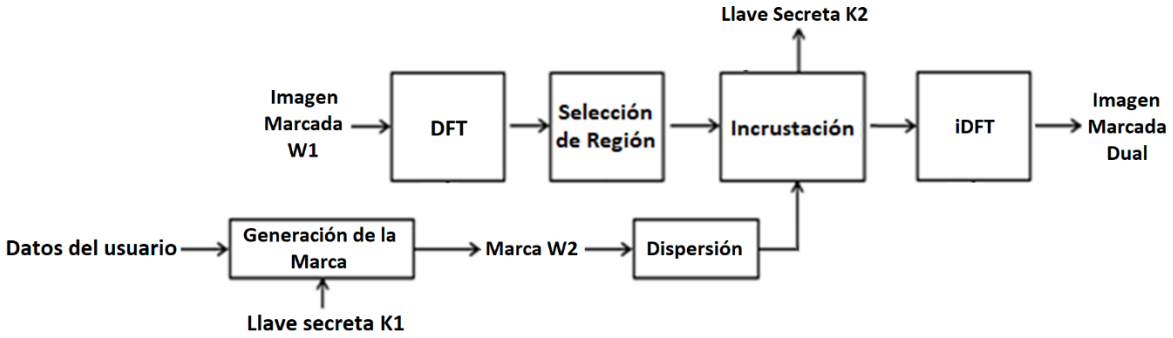



*Figura 3.22 Diagrama de bloques del marcado de agua invisible.*

**Generación de la marca $W2$**

La marca de agua invisible se genera considerando un conjunto de datos, UD, que se asocia al usuario autorizado de la imagen digital. Esta UD está conformada de manera enunciativa, pero no limitativa, del nombre completo del usuario, fecha de préstamo, empresa solicitante, identificadores, tales como, el registro federal de contribuyentes y el registro único de población, entre otros. El proceso de generación de la marca $W2$ es el siguiente:

1) Obtener el resumen criptográfico de UD aplicando el algoritmo RIPEMD-160 [56], [57] cuyo resultado binario se almacena en MD (*Message-Digest Algorithm*).
2) Dividir MD en 2 partes de 80 bits cada una, y para aumentar la robustez, aplicar la operación *or*-exclusiva entre ambas partes. El resultado de esta operación se concatena con la representación binaria de la clave secreta numérica $K1$, y de esta manera, la cadena de bits resultante constituye la marca de agua $W2$. Así, en el proceso de extracción cuando se recupere $W2$, los primeros 80 bits se utilizarán para la detección de la posible infracción de uso, mientras que el resto de bits de $W2$ pertenecen a la clave secreta $K1$.

**Selección de Región**

La imagen es transformada al dominio de la frecuencia mediante la Transformada Discreta de Fourier (**DFT**), donde se aplica el algoritmo de Optimización con Enjambre de Partículas (PSO) [45], este último se utiliza para encontrar los valores optimizados de los parámetros clave en este dominio para la selección de la región de inserción de marca de agua invisible basado en DFT-2D (Figura 3.23), un par de radios $r_1$ y $r_2$ y el área anular $A = \pi(r_2^2 - r_1^2)$.

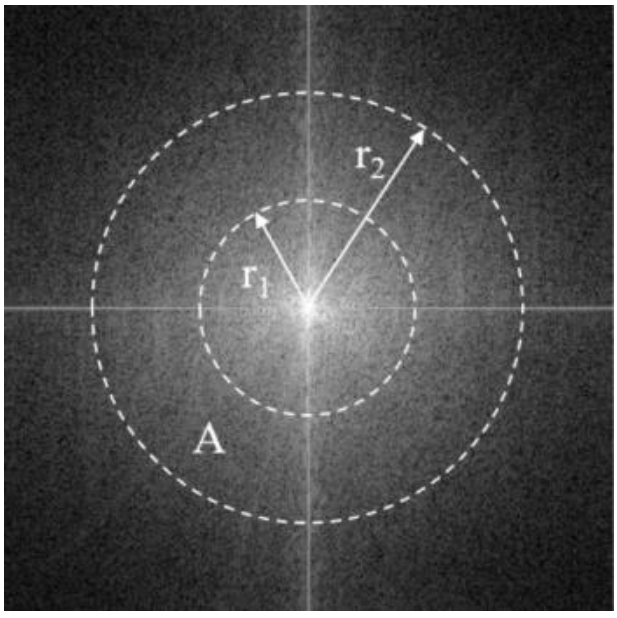



*Figura 3.23 Parámetros en dominio de marca de agua invisible basado en DFT 2D.*

En términos generales, la marca de agua invisible basada en PSO [58], determina los valores óptimos de los radios homocéntricos $r_1$ y $r_2$ utilizados para definir una región de inserción. Por su parte, la función de aptitud objetiva del algoritmo PSO utiliza el criterio *Bit Correct Rate* (BCR) [59], así como la métrica *Visual Information Fidelity* (VIF) [14]. Las imágenes a proteger tienen una profundidad de 8 bits por píxel, y para la ejecución de la función de aptitud objetiva son considerados los procesos de señal definidos en la Tabla 3.2 [58].

*Tabla 3.2. Distorsiones consideradas en la función de aptitud objetiva del algoritmo PSO.*

| **Ataque** | **Tolerancia** |
|---|---|
| Filtro promedio | 5x5 ventana |
| Ajuste de tamaño | Factor 0.6 |
| Compresión JPEG | Factor de calidad 30 |

**Incrustación**

Dentro de la magnitud del DFT seleccionada de la imagen a proteger, la marca se incrusta con el valor óptimo del factor de fuerza de inserción $\alpha$. Para aumentar la robustez del método, el algoritmo de marca de agua implementa la técnica de **espectro disperso** conocida como espectro disperso de secuencia directa (DS-CDMA) [60]. A su vez se obtiene la llave secreta $K2$.

**Imagen marcada y llave secreta K2**

Después de la incrustación de la marca invisible, $W2$, se aplica la transformada inversa de Fourier (**iDFT**) para obtener la imagen marcada con las dos marcas de agua (visible e invisible), llamada dual.

## *3.3.3. Inspección / Extracción*

En el caso de la marca visible camuflada, no existe un proceso de extracción o revelado como tal. Simplemente se debe conocer la marca, y su ubicación para hacer la inspección visual correspondiente, o con ayuda de una amplificación de tipo *zoom*, verificar la existencia de la marca.

En el caso de la marca invisible, el proceso de extracción utiliza las mismas operaciones que en la incrustación; se aplica la DFT a la imagen marcada dual y con la llave secreta $K2$ se extrae la marca $W2$, de ésta última se obtiene los datos de usuario

$UD$ y la llave secreta $W1$; con $UD$. Empleando los $UD$ y un umbral se puede realizar un proceso de detección de infracción de uso.

# 4. Resultados experimentales

El algoritmo se aplicó a toda la base de imágenes proporcionada por la filmoteca de la UNAM, para probar su funcionamiento. En la Figura 4.1 se muestran las diferentes etapas del marcado visible para tres imágenes, en la última columna se señaliza la región seleccionada para la incrustación de la marca de agua visible-camuflada.

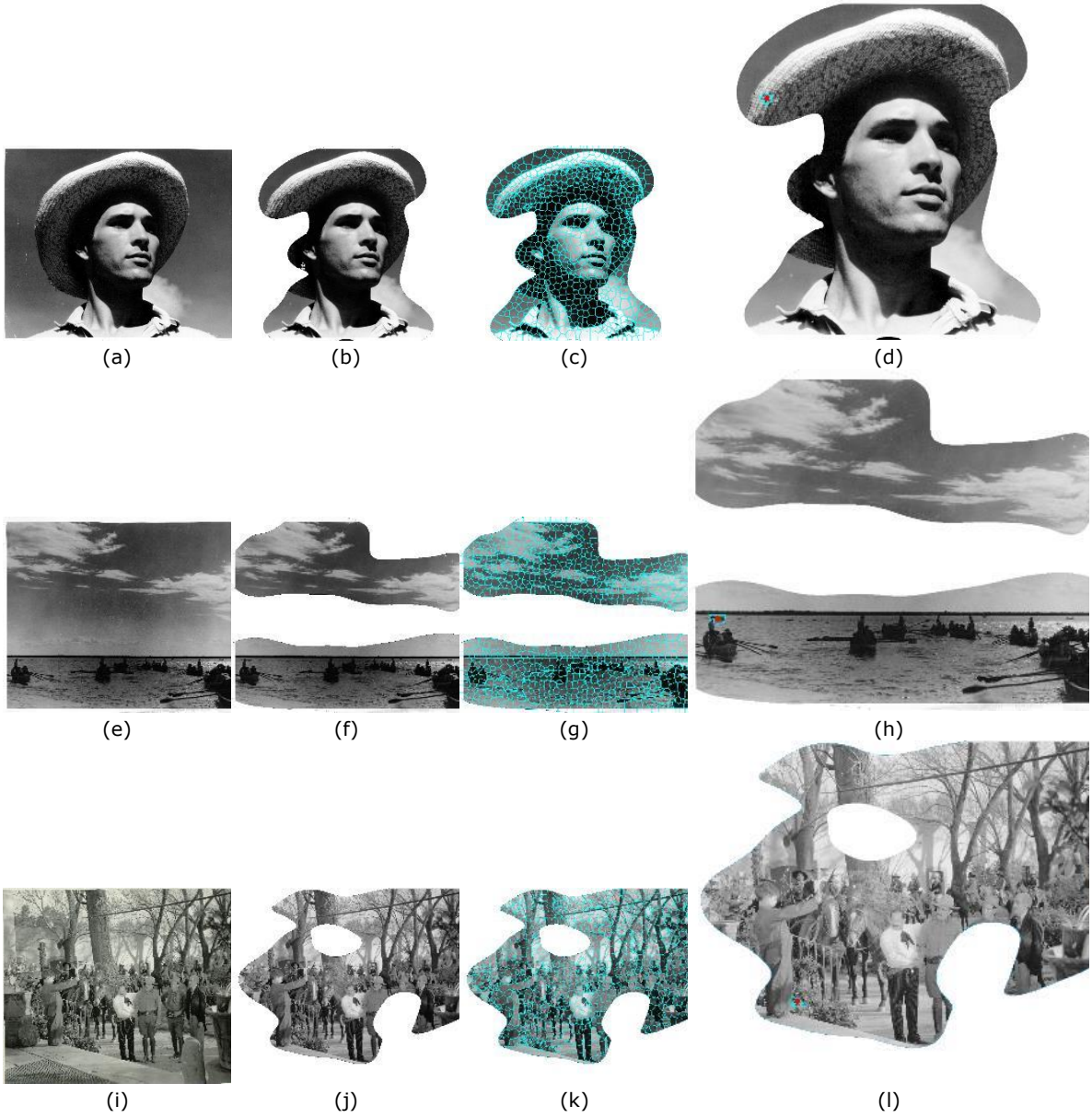



*Figura 4.1 Imágenes originales (1ra columna), Área de atención visual $I_{e_{AV}}$ correspondiente al segundo paso (2da columna), Segmentación aplicando $SP_m$ correspondiente al tercer paso (3ra columna) y región de incrustación seleccionada correspondiente al cuarto paso (4ta columna). Fotografías de primera y segunda fila de la película "Redes", y fotografía de la fila inferior de "El compadre Mendoza" (los títulos de las películas están entre comillas y en español). Las fotografías usadas son cortesía de Filmoteca y propiedad de Filmoteca UNAM.*

En la Figura 4.2 se muestra el comportamiento de los diferentes logos incrustados en una imagen, en la misma región. Se puede apreciar entre más sencillo y conciso sea el logo, más se distinguirá una vez incrustado, sobre todo contrastando estos logos con la "F" incrustada en la imagen Inuit.

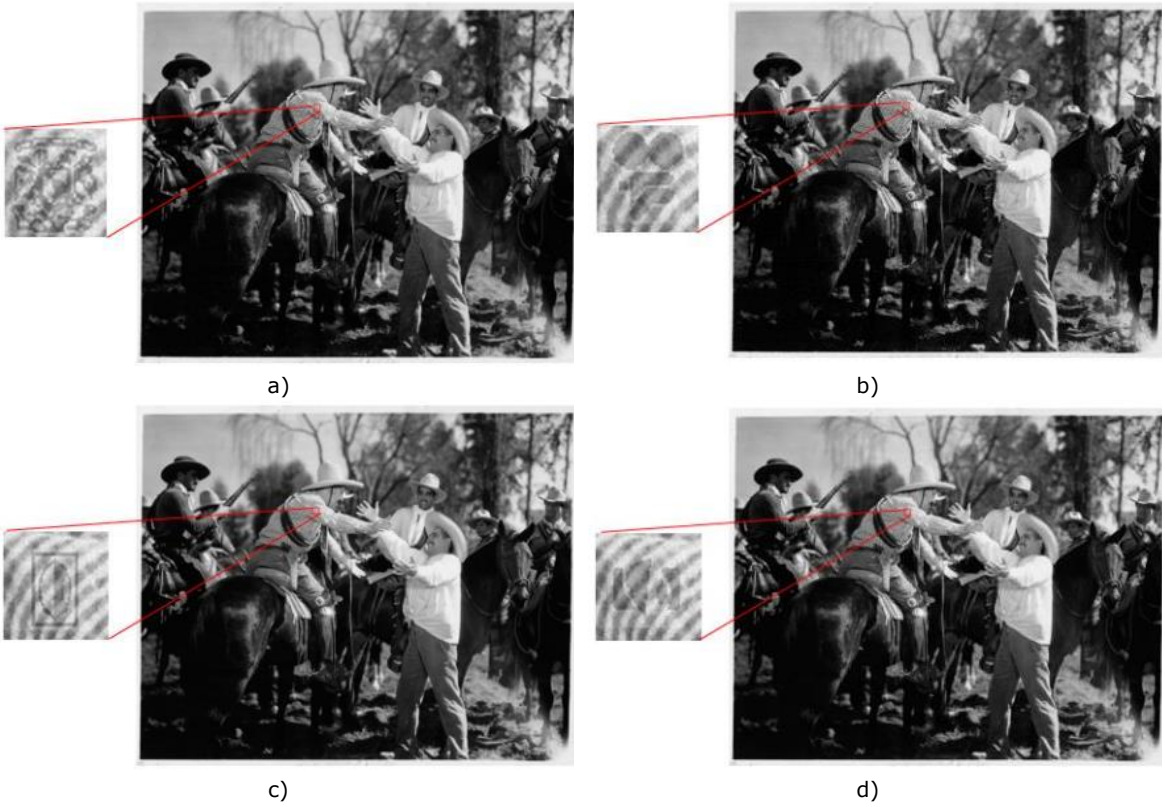



*Figura 4.2 Imágenes con marca de agua, utilizando una fotografía de la película "Vámonos con Pancho Villa", cortesía de Filmoteca, propiedad de Filmoteca UNAM.*

El marcado visible admite variaciones que podrían aumentar la robustez de la marca, como elegir el segundo, o tercer, súper pixel listado en lugar del primero, o insertar marcas múltiples. Este último caso se ilustra en la Figura 4.6.

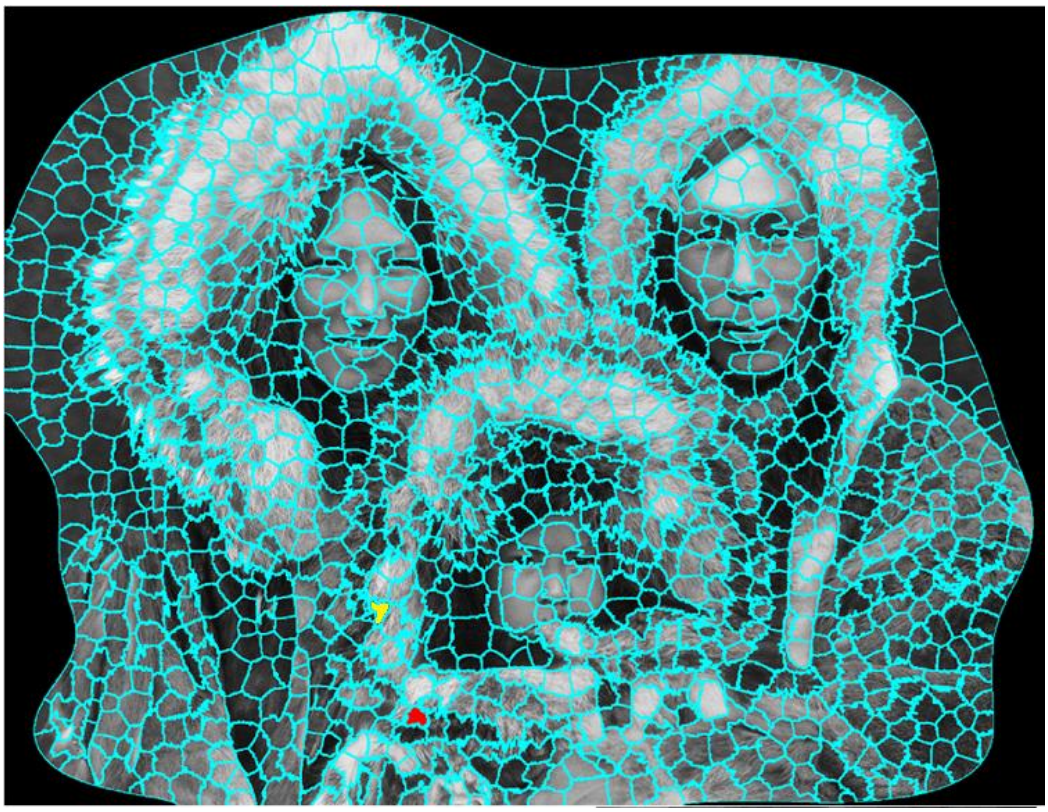


*Figura 4.3 Selección del segundo (amarillo) y tercer (rojo) SP.*

En la Figura 4.4 se muestran las marcas incrustadas en las posiciones señaladas en la Figura 4.3. Se puede apreciar que la marca incrustada es el complemento (con fondo blanco) de la imagen original (con fondo negro). En este caso las métricas de imperceptibilidad también muestran buenos resultados SSIM= 0.99994 y PSNR= 56.47715.

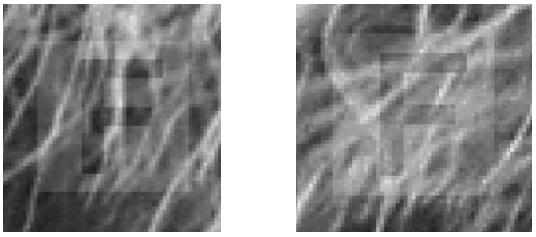


*Figura 4.4 Marcas incrustadas, segundo SP a la izquierda y tercer SP a la derecha.*

En la Figura 4.5 se muestra la imagen marcada, con las marcas mostradas en la Figura 4.4, para exhibir la imperceptibilidad de dichas marcas.

*Figura 4.5 Imagen con dos marcas visibles camufladas.*

*Figura 4.6 Imagen con múltiples marcas camufladas, utilizando una fotografía de la película "Vámonos con Pancho Villa", cortesía de Filmoteca, propiedad de Filmoteca UNAM.*

En general, el equilibrio entre la imperceptibilidad y la robustez de la marca de agua camuflada y la marca de agua invisible es un problema difícil de superar para los investigadores. En esta sección, se muestran los resultados experimentales del método propuesto en términos de estos requisitos. Para ello, se consideraron imágenes del patrimonio cultural mexicano bajo el resguardo de la Dirección General de Actividades Cinematográficas (Filmoteca) de la Universidad Nacional Autónoma de México (UNAM), en formato TIFF con una resolución espacial promedio de 3800 x 3000 píxeles y profundidad en una escala de 8 bit/píxel de gris. Los algoritmos de camuflaje y marca de agua invisible, diseñados en este trabajo, se implementaron utilizando Matlab © R2021b en una computadora con sistema operativo Microsoft Windows © 11, procesador Intel © Core i7 1.8Ghz y 16 GB de RAM.

## *4.1. Imperceptibilidad*

La imperceptibilidad requiere que la calidad visual de las imágenes marcadas se conserve lo mejor posible, con el objetivo que la marca de agua pase inadvertida.

**Marca de agua visible camuflada**

La imperceptibilidad de la marca de agua se evaluó cuantitativamente calculando el valor medio de la base de datos marcados digitalmente, lo que resultó en PSNR = 58 dB y SSIM = 0.99. Para la marca de agua visible camuflada se aplicaron métodos cualitativos. Para medir cualitativamente la imperceptibilidad de las marcas de agua integradas, se aplicó un cuestionario a 22 personas que evalúan 20 imágenes. Los resultados de esta encuesta se muestran en la Tabla 4.1. Además, observamos que cuanta menos textura la imagen tiene, es más fácil identificar la marca de agua.

*Tabla 4.1 Encuesta de imperceptibilidad de marca de agua visible.*

| Pregunta | Yes | No |
|---|---|---|
| Identificar la imagen con marca de agua sin saber que tiene marca de agua | 0% | 100 % |
| Reconocer marca de agua sabiendo que la imagen tiene marca de agua sin conocer la marca de agua | 40% | 60% |
| Reconocer marca de agua sabiendo que la imagen tiene marca de agua y conocer la marca de agua | 50% | 50% |
| Reconocer marca de agua conociendo la marca de agua y su localización | 73% | 27% |

**Marca de agua invisible**

La imperceptibilidad de la marca de agua se evaluó en términos de la fidelidad de la información visual (VIF) [14], la relación señal pico / ruido máxima (PSNR) y el índice de similitud estructural (SSIM) [13]. Estas métricas de calidad de imagen se definieron por (2.8),(2.9) y (2.21), respectivamente.

Como se sabe en la literatura [14], el valor VIF (2.21) refleja distorsiones perceptivas con mayor precisión que la métrica PSNR. El rango de valores de VIF es [0, 1], y un valor más cercano a 1 representa una mejor fidelidad con respecto a la imagen original. Los lectores interesados pueden consultar [14] para obtener más detalles sobre la métrica VIF. La Tabla 4.2 muestra los resultados de imperceptibilidad en términos de valores promedio de PSNR, SSIM y VIF, respectivamente. En general, un valor de PSNR superior a 37dB [61], o un valor de SSIM superior a 0.93 [32] significa que las dos imágenes comparadas no son visiblemente diferentes. En términos de SSIM, los valores promedio son aproximados a 0.99, los cuales son bastante satisfactorios.

*Tabla 4.2. Valores medios de PSNR, SSIM Y VIF*

| Metric | Average Value |
|---|---|
| PSNR | 46.91 dB |
| SSIM | 0.9952 |
| VIF | 0.9564 |

## 4.2. Robustez

La robustez requiere que la marca de agua pueda sobrevivir a varios ataques. Se realizaron diferentes ataques sobre imágenes con marcas de agua para probar su robustez, como ataques geométricos, procesamiento de imágenes, proceso de impresión y escaneo.

**Marca de agua visible camuflada**

En la Figura 4.7 se muestra la marca atacada de la imagen "Inuit", donde: (a) es la marca incrustada en la imagen sin ningún ataque; (b) es un aumento de nitidez; (c) aumento de contraste; (d) aumento de brillo; (e) difuminación mediante un filtro mediana; (f) compresión jpg 90%; (g) compresión jpg 70%; (h) compresión jpg 50%; (i) compresión jpg 30%; (j) compresión jpg 10%; (k) reducción de tamaño al 30%; (l) reducción de tamaño al 50%; las marcas (m-ar) corresponden al ataque de impresión-escaneo cuyos detalles se listan en la Tabla 4.3.

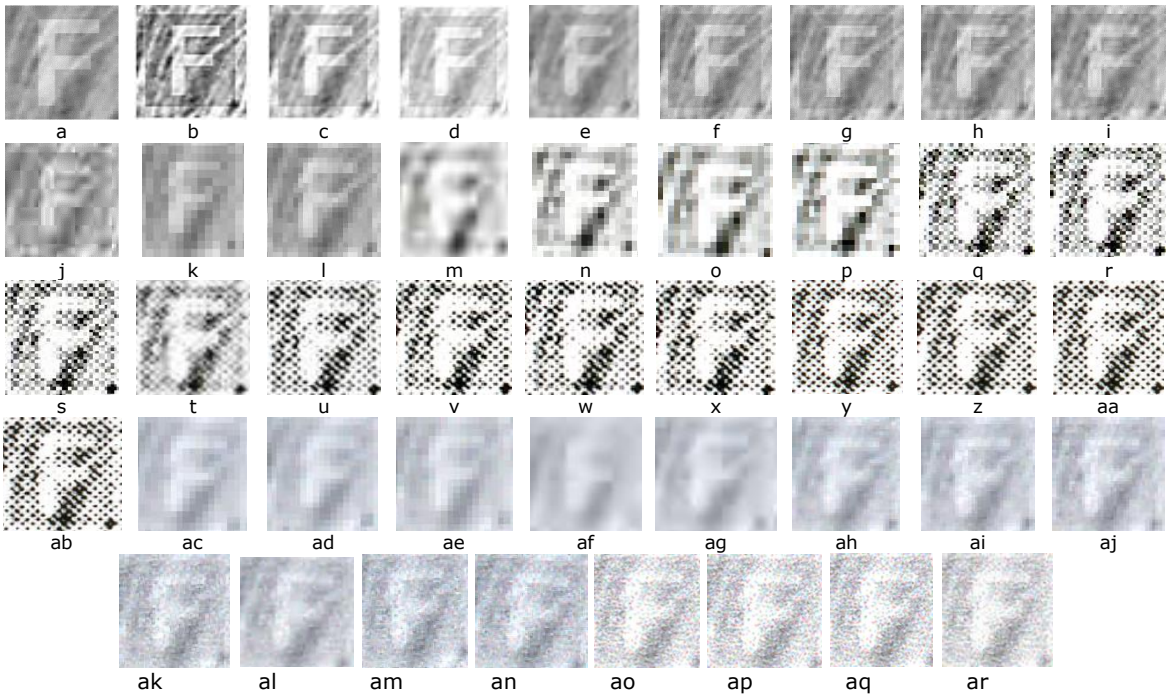



*Figura 4.7. Marca original (a) y atacadas (b-ar), imagen inuit.*

*Tabla 4.3 Ataques de impresión-escaneo Figura 4.7.*

| Impresora | Escáner Epson Perfection V600 Photo | Formato | Inciso |
|---|---|---|---|
| Laser jet 600 configurada con una resolución Pro Res 1200 | 150 ppi | PDF | m |
| | | JPEG | n |
| | | TIFF | o |
| | | BMP | p |
| | 300 ppi | BMP | q |
| | | TIFF | r |
| | | JPEG | s |
| | | PDF | t |
| | 600 ppi | PDF | u |
| | | JPEG | v |
| | | TIFF | w |
| | | BMP | x |
| | 1200 ppi | BMP | y |
| | | TIFF | z |
| | | JPEG | aa |
| | | PDF | ab |
| Inkjet Canon PIXMA G1100 configurada en calidad alta | 150 ppi | JPEG | ac |
| | | BMP | ad |
| | | TIFF | ae |
| | | PDF | af |
| | 300 ppi | PDF | ag |
| | | BMP | ah |
| | | JPEG | ai |
| | | TIFF | aj |
| | 600 ppi | TIFF | ak |
| | | PDF | al |
| | | JPEG | am |
| | | BMP | an |
| | 1200 ppi | BMP | ao |
| | | JPEG | ap |
| | | TIFF | aq |
| | | PDF | ar |

Adicionalmente en la Figura 4.8 se muestran las marcas recuperadas de las fotografías digitales las imágenes impresas con Laser jet 600 configurada con una resolución Pro Res 1200 (a); y Inkjet Canon PIXMA G1100 configurada en calidad alta (b); tomadas con un celular Motorola e5 plus cuya cámara es de 5 megapíxeles y posteriormente enviadas por whatsapp para procesarlas en el computador.

*Figura 4.8. Marca original (a) y fotografiadas (b-c), imagen inuit.*

Una muestra representativa de la marca de agua visible atacada se muestra en la Figura 4.9, la imagen superior derecha de la Figura 4.2 es la que recibe los ataques, los resultados se muestran en la Figura 4.9 donde: (a) es la marca de agua sin ningún ataque; (b-q) corresponden al ataque de impresión-escaneo cuyos detalles se enumeran en la Tabla 4.4. ; (r) aumento de la nitidez; (s) realce de contraste; (t) aumento del brillo; (u) desenfoque por filtro mediano; Compresión JPEG con pérdida en (v) 90%; (w) 70%; (x) 50%; (y) 30%; (z) 10%; (aa) complemento; (ab) 30% de reducción de tamaño; y (ac) 50% de reducción de tamaño. Los resultados experimentales muestran que la marca de agua visible puede resistir varios ataques ya que es aún reconocible en imágenes atacadas con marca de agua.

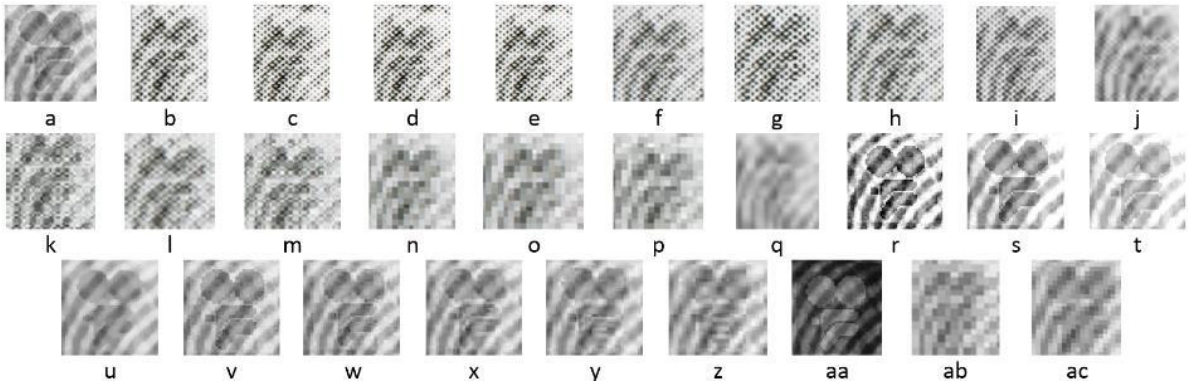



*Figura 4.9 Marcas de agua extraídas de la imagen que se muestra en la Figura 4.2 (a) Marca de agua sin ataques y (b-ac) marcas de agua atacadas.*

*Tabla 4.4 Ataques de impresión-escaneo Figura 4.2.*

| Printer | Scanner Epson Perfection V600 Photo | Format | Letter |
|---|---|---|---|
| HP TopShot LaserJet Pro M275 | 150 ppi | PDF | b |
| | | JPEG | c |
| | | TIFF | d |
| | | BMP | e |
| | 300 ppi | BMP | f |
| | | TIFF | g |
| | | JPEG | h |
| | | PDF | i |
| | 600 ppi | PDF | j |
| | | JPEG | k |
| | | TIFF | l |
| | | BMP | m |
| | 1200 ppi | BMP | n |
| | | TIFF | o |
| | | JPEG | p |
| | | PDF | q |

**Marca invisible**

Debe definirse un valor de umbral de decisión $T_d$ para determinar si $W2$ está presente, o no, en la imagen $I_w$. Considerando una distribución binomial con una probabilidad de éxito igual a 0.5, una probabilidad de falsa alarma $P_{fa}$ para $L$ bits de datos de marca de agua viene dada por (4.1), donde se debe controlar un valor de umbral T para obtener un valor menor de $P_{fa}$ que se define de la manera mostrado en la ecuación (4.1):

$$P_{fa} = \sum_{\lambda=T}^{L} (0.5)^L \cdot \left(\frac{L!}{\lambda!\,(L-\lambda)!}\right) \tag{4.1}$$

donde $L = 80$ es la longitud de $W2$. Basado en el supuesto de los ensayos de Bernoulli, λ es una variable aleatoria independiente con distribución binomial [62].

La probabilidad de falsa alarma debe ser inferior a $10^{-6}$, que se establece para satisfacer los requisitos de la mayoría de las aplicaciones de marcas de agua para una detección confiable [62], y luego un valor de umbral de decisión adecuado $T_d$, se define mediante la ecuación (4.2):

$$T_d = 1 - \left(\frac{T}{L}\right) \tag{4.2}$$

De (4.2), considerando $L = 80$ y $T = 60$, entonces $T_d = 0.75$, de acuerdo con el hecho de que cuando BER + la tasa de bits correctos (BCR) debe ser igual a 1. Si el valor de BCR entre $W2$ y $W2'$ es menor al 75%, el proceso de detección considera la ausencia de

$W2$, en caso contrario, se detecta $W2$ de manera exitosa, en consecuencia, detectando al usuario infractor. Las pruebas de robustez se clasifican en los tipos: procesamiento de señal y distorsiones geométricas, así como ataques combinados compuestos por compresión JPEG con factor de calidad 70 +, ya sea procesamiento de señal, o distorsiones geométricas. Las pruebas de robustez se muestran en las Tablas 4.5, 4.6 y 4.7, respectivamente.

*Tabla 4.5 Valores promedio de BCT a las distorsiones geométricas.*

| **Distorsión geométrica** | **Valor Promedio BCR** |
|---|---|
| Rotación 45° | 0.99 |
| Rotación 135° | 0.99 |
| Escalamiento 0.6 | 0.99 |
| Escalamiento 2 | 1 |
| Recorte central 256x256 | 1 |
| Traslación $x$= 200, $y$=200 | 1 |

*Tabla 4.6 Valores promedio de BCR al procesamiento de señal.*

| **Procesamiento de Señal** | **Valor Promedio BCR** |
|---|---|
| Sin ataque | 1 |
| JPEG QF = 20 | 0.90 |
| JPEG QF = 30 | 0.98 |
| JPEG QF = 50 | 0.99 |
| Ruido Gaussiano $\mu$=0, $\sigma^2$=0.01 | 0.94 |
| Ruido Gaussiano $\mu$=0, $\sigma^2$=0.05 | 0.86 |
| Ruido impulsivo densidad=0.09 | 0.79 |
| Ruido Speckle $\mu$=0, $\sigma^2$=0.15 | 0.78 |
| Ruido Speckle $\mu$=0, $\sigma^2$=0.09 | 0.80 |
| Filtrado promedio 3x3 | 0.99 |
| Filtrado promedio 5x5 | 0.99 |
| Ecualización del Histograma | 1 |
| Filtrado Gaussiano 7x7 | 1 |
| Aumento de la nitidez | 1 |
| Reducción del brillo | 0.99 |
| Aumento del brillo | 0.99 |
| Filtrado Mediana 3x3 | 0.99 |
| Filtrado de movimiento 5x5 | 0.99 |
| Corrección Gamma $\gamma$=2 | 1 |
| Corrección Gamma $\gamma$=0.5 | 0.99 |

*Tabla 4.7 Valores promedio de BCR para distorsiones combinadas.*

| Distorsiones combinadas con JPEG 70 + | Valor Promedio BCR |
|---|---|
| Ruido Gaussiano $\mu$=0, $\sigma^2$=0.01 | 0.93 |
| Ruido Gaussiano $\mu$=0, $\sigma^2$=0.05 | 0.76 |
| Ruido impulsivo densidad =0.09 | 0.77 |
| Ruido Speckle $\mu$=0, $\sigma^2$=0.09 | 0.76 |
| Filtrado promedio 3x3 | 0.99 |
| Filtrado promedio 5x5 | 0.96 |
| Ecualización del Histograma | 1 |
| Filtrado Gaussiano 7x7 | 0.99 |
| Sharpening | 1 |
| Aumento de la nitidez | 0.98 |
| Reducción del brillo | 0.98 |
| Aumento del brillo | 0.98 |
| Filtrado Mediana 3x3 | 0.99 |
| Filtrado de movimiento 5x5 | 0.99 |
| Corrección Gamma $\gamma$=2 | 0.99 |
| Rotación 45° | 0.98 |
| Rotación 135° | 0.98 |
| Escalamiento 0.6 | 0.99 |
| Escalamiento 2 | 0.99 |
| Recorte central 256x256 | 0.98 |
| Traslación $x$= 200, $y$=200 | 0.98 |

## 4.3. Trabajos relacionados

La mayoría de las marcas visibles que pretenden proteger el derecho de propiedad de imágenes obstruyen gran parte de la imagen [63]–[65], algunos otros métodos suavizan la marca visible para que sean apenas perceptible [66]. La gran ventaja de este tipo de marcas es que no requieren ningún tipo de proceso de extracción o revelado, una desventaja de una marca que es evidente es que es más susceptible de ser atacada y/o removida [16], [67].

Las marcas visibles-invisibles (*unseen-visible*) [68], [69], generalmente se aprovechan para dos funciones principales proporcionar información adicional [70], o para la protección de la propiedad [17], [71]. Una ventaja de este tipo de algoritmos es que el proceso de revelado de la marca suele ser muy sencillo. Sin embargo, una vez impreso el trabajo es muy probable que la marca no pueda ser recupera porque van dirigidos principalmente al despliegue digital de las imágenes.

En [54] se presenta una marca visible similar, pero se centra únicamente en retratos y se vale del color para la selección del área de incrustación, ambas

características que no podemos aplicar a la base de imágenes de la presente investigación. Debido a que nuestra base de imágenes no posee la característica del color, no se puede emplear el tono de piel como un medio de selección de la región para la incrustación de la marca de agua como en [54]. Adicionalmente, nuestra base de imágenes es heterogénea, incluyendo paisajes, edificios, animales, etc.; a diferencia de la usada en [54], donde se emplean solamente retratos.

Se estudiaron diferentes técnicas de marca de agua dual, los datos comparados se muestran en la Tabla 4.8. Es notable que ninguno haya sido probado para ataques de escaneo de impresión, y nuestra propuesta tiene el mejor PSNR.

*Tabla 4.8 Comparación con otros algoritmos de marca de agua dual.*

| Métodos | Imágenes | Robustez | Dominio Incrustación | Visibilidad | Extracción | Protección Copyright | Autenticación de imagen | PSNR |
|---|---|---|---|---|---|---|---|---|
| Esquema propuesto | Grises | Robusta<br>Robusta | Espacial<br>DFT | Visible<br>Invisible | Ciega<br>No Ciega | Sí | No | ~47 dB |
| Liu et al. [72] | Color | Frágil<br>Robusta | Espacial<br>DWT | Invisible<br>Invisible | Ciega<br>Ciega | Sí | Sí | ~40 dB |
| Lusson et al. [73] | Color | Robusta<br>Robusta | Espacial<br>Espacial | Invisible<br>Invisible | Ciega<br>No Ciega | Sí | No | ~39 dB |
| Lin et al. [74] | Grises | Robusta<br>Robusta | Espacial<br>DCT | Visible<br>Invisible | Ciega<br>Ciega | Sí | No | ~30 dB |
| Lu and Liao [75] | Color | Frágil<br>Robusta | DWT<br>DWT | Invisible<br>Invisible | Ciega<br>No Ciega | Sí | Sí | ~40 dB |

En [72] se presenta un mecanismo de marca de agua dual invisible ciega para imágenes en color, que consiste en una marca de agua robusta en el espacio de color YCbCr que aplica DWT, y una marca de agua frágil en el espacio RGB. En [73] se propone un esquema de marca de agua robusta dual para la protección de los derechos de autor, mediante la incorporación de una marca de agua incrustando una imagen en el espacio de color RGB, y otra marca de agua binaria en el espacio de color YCbCr de una imagen portadora en color *host*. En [74] se presenta un esquema de marca de agua dual para la protección intensiva de los derechos de autor, este esquema consiste en una imagen de marca de agua visible directamente incrustada en el dominio espacial de la imagen portadora, y una marca de agua invisible donde se incrusta una imagen oculta en el dominio de frecuencia utilizando la técnica de la distorsión apenas notable. En[75] se propone un esquema de marca de agua ciega mediante la incorporación de marcas de agua robusta y frágil en una imagen portadora para la protección simultánea de los derechos de autor y la autenticación de la imagen.

# 5. Conclusiones

Uno de los objetivos principales de los dos tipos de marcas de agua (visible e invisible) es que una imagen con marca de agua debe soportar varias manipulaciones que intentan eliminar la marca de agua digital del contenido de la imagen. Por ejemplo, la compresión con pérdida, la transmisión en un canal ruidoso, las distorsiones geométricas, así como los procesos de impresión-escaneo. Dadas todas estas posibilidades de ataque, el problema no tiene una solución única y universal; por lo tanto, la investigación en este campo siempre será un desafío para nuevas propuestas y avances, dependiendo de la evolución de las aplicaciones y tecnologías a lo largo del tiempo.

Considerando lo anterior, el presente trabajo de investigación cumplió con la hipótesis propuesta al desarrollar un algoritmo que involucra la administración y detección de infracciones de uso de imágenes cinematográficas digitalizadas del patrimonio cultural mexicano. La propuesta consta de dos modalidades de marca de agua digital: la primera consiste en una marca de agua visible camuflada basada en el dominio espacial, y la segunda, perteneciente a una marca de agua invisible basada en el dominio de la frecuencia, junto con la optimización del enjambre de partículas. Los resultados experimentales muestran la versatilidad del algoritmo propuesto después de los procesos de impresión y escaneo, considerando una evaluación desde el punto de vista de los requisitos de imperceptibilidad y robustez, evitando dependencias en el uso de *hardware* específico.

Esta investigación propuso una incrustación y extracción para un esquema de marca de agua dual para imágenes de cine, digitalizadas y antiguas, descritas en el punto 3.1. Se implementaron datos de usuarios autorizados embebidos utilizando la Transformada Discreta de Fourier, la optimización del enjambre de partículas (permitiendo ajustar de forma automática sus parámetros clave de operación) y el Espectro ensanchado de Secuencia Directa para la marca de agua invisible; así como, descomposición de texturas de dibujos animados, mapa de prominencia y SLIC de superpíxeles. Los resultados experimentales se han mostrado el capítulo 4, y estos resultados se comparan con los de algunas técnicas de marcado de agua en imágenes existentes de última generación que demuestran un buen rendimiento.

El principal aporte corresponde al desarrollo de una marca de agua visible, camuflada y resistente al ataque de impresión-escaneo, que tiene alta robustez y se combina con una marca de agua invisible que contiene datos importantes para rastrear

las copias, brindando mayor seguridad. La protección de los derechos de autor de las imágenes no se ha explorado ampliamente para los ataques de escaneo de una impresión. Sin embargo, se identificó un verdadero problema de seguridad sobre las imágenes cinematográficas digitalizadas del patrimonio cultural mexicano, que pueden ser impresas, escaneadas, y distribuidas sin autorización.

La presente propuesta utiliza una marca de agua camuflada junto con una marca de agua invisible. Ambas marcas de agua funcionan juntas para decidir si se autoriza el uso de una imagen, para su distribución. Los resultados mostraron que la información incrustada tiene una gran solidez y se puede utilizar para rastrear copias de imágenes de manera efectiva. Además, la información de seguridad adicional no afecta a la calidad de la imagen, obteniendo valores de PSNR superiores a otras propuestas también con doble marca de agua. Esta investigación es importante porque implementa una solución de marca de agua para un conjunto específico de imágenes con características que dan solución a la necesidad de la Filmoteca de la UNAM y, hasta donde sabemos, no existe ningún algoritmo como el que presentamos, contribuyendo así al campo de la marca de agua.

Adicionalmente, como resultado de la presente investigación se publicaron dos artículos en revistas indexadas, cuyas primeras páginas se encuentran en el ANEXO, y una ponencia, cuya constancia también se incluye en el ANEXO.

# *ANEXO: Publicaciones y participaciones*

*electronics*

MDPI

*Article*

## Additional Information Delivery to Image Content via Improved Unseen–Visible Watermarking

**Oswaldo Ulises Juarez-Sandoval [1,*], Laura Josefina Reyes-Ruiz [1], Francisco Garcia-Ugalde [1,*], Manuel Cedillo-Hernandez [2], Jazmin Ramirez-Hernandez [2] and Robert Morelos-Zaragoza [3]**

[1] Facultad de Ingenieria, Universidad Nacional Autónoma de Mexico (UNAM), Av. Universidad No. 3000, Ciudad Universitaria, Coyoacán, Mexico City 04510, Mexico; laura.reyes@ingenieria.unam.edu
[2] Instituto Politecnico Nacional (IPN), Escuela Superior de Ingenieria Mecanica y Electrica, Unidad Culhuacan, Av. Santa Ana No. 1000, San Francisco Culhuacan, Coyoacán, Mexico City 04430, Mexico; mcedilloh@ipn.mx (M.C.-H.); jramirezhe@ipn.mx (J.R.-H.)
[3] College of Engineering, San Jose State University, San Jose, CA 95192, USA; robert.morelos-zaragoza@sjsu.edu
* Correspondence: ojuarezs@ipn.mx (O.U.J.-S.); fgarciau@unam.mx (F.G.-U.)

**Abstract:** In a practical watermark scenario, watermarks are used to provide auxiliary information; in this way, an analogous digital approach called unseen–visible watermark has been introduced to deliver auxiliary information. In this algorithm, the embedding stage takes advantage of the visible and invisible watermarking to embed an owner logotype or barcodes as watermarks; in the exhibition stage, the equipped functions of the display devices are used to reveal the watermark to the naked eyes, eliminating any watermark exhibition algorithm. In this paper, a watermark complement strategy for unseen–visible watermarking is proposed to improve the embedding stage, reducing the histogram distortion and the visual degradation of the watermarked image. The presented algorithm exhibits the following contributions: first, the algorithm can be applied to any class of images with large smooth regions of low or high intensity; second, a watermark complement strategy is introduced to reduce the visual degradation and histogram distortion of the watermarked image; and third, an embedding error measurement is proposed. Evaluation results show that the proposed strategy has high performance in comparison with other algorithms, providing a high visual quality of the exhibited watermark and preserving its robustness in terms of readability and imperceptibility against geometric and processing attacks.

**Keywords:** invisible–visible watermarking; unseen–visible watermarking; imperceptible–visible watermarking; watermark complement strategy; visual degradation; histogram distortion; QR code

check for updates

Citation: Juarez-Sandoval, O.U.; Reyes-Ruiz, L.J.; Garcia-Ugalde, F.; Cedillo-Hernandez, M.; Ramirez-Hernandez, J.; Morelos-Zaragoza, R. Additional Information Delivery to Image Content via Improved Unseen–Visible Watermarking. *Electronics* 2021, *10*, 2186. https://doi.org/10.3390/electronics10182186

Academic Editor: Cheonshik Kim

Received: 13 August 2021
Accepted: 1 September 2021
Published: 7 September 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

### 1. Introduction

In the future, the current growth of technological development will be compared only with the period called the industrial revolution. This development allows people easy access to electronic devices that are capable of capturing and displaying different multimedia files, especially images and videos, which could be easily copied, edited, and distributed without any protection, turning these practices into a problem of copyright protection and intellectual property. To solve this problem, in the last decade, several digital watermarking algorithms have been proposed [1–5]. However, in a real-life scenario, the watermarks are used to deliver auxiliary information, such as banknotes, official documents, etc., where the watermarked document delivers information about its authenticity when its visualization is enhanced, seeing it against light. In this context, several watermarking algorithms have been proposed to deliver auxiliary information about the visual content of images [6–11]; opening with this target a new research field that is denoted as invisible–visible watermarking, which can be divided according to the exhibition stage in unseen–visible watermarking (UVW) [6–8], and imperceptible–visible watermarking (IVW) [9,11]. The main idea of invisible–visible watermarking algorithms applied to digital color images is based on the

# Robust Dual Digital Watermark Applied to Antique Digitized Cinema Images: Resistant to Print-Scan Attack

Laura Reyes-Ruiz [1], Eduardo Fragoso-Navarro [1], Francisco Garcia-Ugalde [1], Oswaldo Juarez-Sandoval [2], Manuel Cedillo-Hernandez [2,*], and Mariko Nakano-Miyatake [2]

[1] Universidad Nacional Autónoma de México, Facultad de Ingeniería, Ciudad de México, Mexico
[2] Instituto Politécnico Nacional, SEPI ESIME Culhuacán, Ciudad de México, Mexico
*Correspondence: mcedilloh@ipn.mx (M.C.H.)

***Abstract*—Nowadays, advances in information and communication technologies along with easy access to electronic devices such as smartphones have achieved an agile and efficient storing, edition, and distribution of digital multimedia files. However, lack of regulation has led to several problems associated with intellectual property authentication and copyright protection. Furthermore, the problem becomes complex in a scenario of illegal printed exploitation, which involves printing and scanning processes. To solve these problems, several digital watermarking in combination with cryptographic algorithms has been proposed. In this paper, a strategy of robust watermarking is defined consisting of the administration and detection of unauthorized use of digitized cinematographic images from Mexican cultural heritage. The proposed strategy is based on the combination of two types of digital watermarking, one of visible-camouflaged type based on spatial domain and another of invisible type based on frequency domain, together with a particle swarm optimization. The experimental results show the high performance of the proposed algorithm faced to printing-scanning processes or digital-analogue attack, and common image geometric and image processing attacks such as JPEG compression. Additionally, the imperceptibility of the watermark is evaluated by PSNR and compared with other previously proposed algorithms.**

***Keywords*—digital watermarking, image processing, information security, authentication, copyright protection, cultural heritage**

## I. Introduction

Currently, more and more information are transferred electronically. Multimedia data such as image, video, and audio can be transmitted by different means, for instance, via the internet, to be visualized in different devices. One of the issues associated with intellectual property occurs when someone has access to all the data, and then copy and retransmit it to unauthorized users without restriction. This will always be possible because digital data can be reproduced identically and unlimitedly. A promising solution to protect information, intellectual property and copyright against unauthorized users is the use of digital watermarking, which in general terms hides certain information associated with the owner and/or distributor, in such a way that only authorized users can make legal use of the data in question [1–8]. Thus, digital watermark in an image can contain information about the author, or the distributor, or even information of the image itself.

Watermarks can be visible or invisible, depending on the application. In the visible case, the embedding location could be chosen based on properties of human vision [9] in such a way that the watermark is unperceived by the naked eye and can be found just with the location information. This feature, in conjunction with visible watermark robustness, are especially useful for certain intentional attacks with optical disturbance equipment, e.g. scanning and printing processes on paper [10]. On the one hand, an invisible mode watermarking algorithm is composed by three elements: the watermark, the encoder (embedding algorithm), and the decoder (detection algorithm). On the other hand, a visible watermarking algorithm consists of only two parts, the watermark, and the embedding algorithm since detection can be performed by bare eye. In a digital imaging context, invisible watermarks can be embedded both in spatial domain as well as in frequency domain. Meanwhile, visible watermarks are usually embedded in the spatial domain.

One of the main objectives of both modalities is that a watermarked image must withstand several manipulations that attempt to remove the digital watermark from the image content. For instance, lossy compression, transmission in a noisy channel, geometric distortions, as well as print-scan processes. Given all these attack possibilities, the problem does not have a single and universal solution; therefore, the research in this field will always be a challenged for new proposals and advances, depending on the evolution of applications and technologies over time.

Considering the foregoing, this article proposes an algorithm that involves the administration and detection of

Manuscript received July 11, 2022; revised August 30, 2022; accepted November 20, 2022.

doi: 10.18178/joig.11.1.61-71

# INSTITUTO POLITÉCNICO NACIONAL

**ESCUELA SUPERIOR DE INGENIERÍA MÉCANICA Y ELÉCTRICA**

UNIDAD CULHUACAN

*SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN*
*CAPÍTULO DE CIRCUITOS Y SISTEMAS DE LA IEEE SECCIÓN MÉXICO*
*IEEE RAMA ESTUDIANTIL-ESIME CULHUACAN*

OTORGA LA PRESENTE **CONSTANCIA** POR SU PARTICIPACIÓN EN LA **14ª SEMANA BEIFI Y PROYECTOS DE INVESTIGACIÓN** QUE SE REALIZÓ LOS DÍAS 28, 29 Y 30 DE NOVIEMBRE DE 2022 EN MODALIDAD PRESENCIAL A:

**LAURA JOSEFINA REYES RUÍZ,**
**FRANCISCO JAVIER GARCÍA UGALDE,**
**MANUEL CEDILLO HERNÁNDEZ,**
**OSWALDO ULISES JUÁREZ SANDOVAL**

CON LA **PONENCIA** TITULADA:

## MARCA DE AGUA DIGITAL ROBUSTA DUAL APLICADA A IMÁGENES ANTIGUAS DE CINE DIGITALIZADAS: RESISTENTE AL ATAQUE DE IMPRESIÓN Y ESCANEO

*"La Técnica al Servicio de la Patria"*

M. en I. Lidia Prudente Tikteco
Jefa del Departamento de Investigación

Dr. Juan Carlos Sánchez García
Presidente CAS IEEE Sección México

M. en C. Osvaldo López Garma
Jefe Interino de la Sección de Estudios de Posgrado e Investigación

M. en E. Dalia Ruiz Domínguez
Directora

S. E. P.
SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION
ESIME CULHUACAN

S.E.P. I.P.N.
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN
DIRECCIÓN

# *Referencias*


[1] G. Morrison, "No Title," *cnet en español*, 2016. https://www.cnet.com/es/noticias/1080p-2k-uhd-4k-8k-que-significan-resolucion-televisores/ (accessed Jan. 31, 2017).

[2] J. Pérez Porto and M. Merino, "Definición DE," 2018. https://definicion.de/hdr/ (accessed Jul. 04, 2022).

[3] J. C. Lopez, "La biblia del HDR: qué es, cuáles son los estándares actuales y cómo no todo lo que dicen que es HDR lo es en realidad," 2019. https://www.xataka.com/televisores/biblia-hdr-que-cuales-estandares-actuales-como-no-todo-que-dicen-que-hdr-efectivamente (accessed Sep. 17, 2020).

[4] F. Shih, *Digital Watermarking and Steganography*. Boca Raton: CRC Press, 2008. doi: https://doi.org/10.1201/9781315219783.

[5] F.-H. Wang, *Innovations in Digital Watermarking Techniques*, 1st ed. Springer-Verlag Berlin Heidelberg, 2009. doi: 10.1007/978-3-642-03187-8.

[6] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *J. Appl. Res. Technol.*, vol. 12, no. 1, pp. 122–138, 2014, doi: 10.1016/S1665-6423(14)71612-8.

[7] M. L. Miller, I. J. Cox, J.-P. M. G. Linnartz, and T. Kalker, "A review of watermarking principles and practices," *Digit. signal Process. Multimed. Syst.*, pp. 461–485, 1999.

[8] O. U. Juarez-Sandoval, F. J. Garcia-Ugalde, M. Cedillo-Hernandez, J. Ramirez-Hernandez, and L. Hernandez-Gonzalez, "Imperceptible–visible watermarking to information security tasks in color imaging," *Mathematics*, vol. 9, no. 19, 2021, doi: 10.3390/math9192374.

[9] W. De Ploey, "Digitization, digitalization and digital transformation: the differences." https://www.i-scoop.eu/digitization-digitalization-digital-transformation-disruption/ (accessed Jan. 06, 2020).

[10] A. Grillo, A. Lentini, M. Querini, and G. F. Italiano, "High capacity colored two dimensional codes," *Comput. Sci. Inf. Technol. (IMCSIT), Proc. 2010 Int. Multiconference*, pp. 709–716, 2010, doi: 10.1109/IMCSIT.2010.5679869.

[11] K. Solanki, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Modeling the print-scan process for resilient data hiding," *Secur. Steganography, Watermarking Multimed. Contents VII*, vol. 5681, no. March, p. 418, 2005, doi: 10.1117/12.588002.

[12] P.-Y. Chen and C.-L. Lin, "Print and scan resistant watermarking scheme for colour images," *Imaging Sci. J.*, vol. 63, no. 5, pp. 273–284, 2015, doi: 10.1179/1743131X15Y.0000000010.

[13] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, 2004, doi: 10.1109/TIP.2003.819861.

[14] H. R. Sheikh and A. C. Bovik, "Image information and visual quality," *ICASSP,*

*IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, vol. 15, no. 2, pp. 430–444, 2006, doi: 10.1109/icassp.2004.1326643.

[15] W. Yin, D. Goldfarb, and S. Osher, "Image Cartoon-Texture Decomposition and Feature Selection using the Total Variation Regularized L 1 Functional," in *International Workshop on Variational, Geometric, and Level Set Methods in Computer Vision*, 2005, pp. 73–84. doi: https://doi.org/10.1007/11567646_7.

[16] H. Santoyo-garcia, E. Fragoso-navarro, R. Reyes-reyes, G. Sanchez-perez, M. Nakano-miyatake, and H. Perez-meana, "An Automatic Visible Watermark Detection Method using Total Variation".

[17] O. Juarez-Sandoval, E. Fragoso-Navarro, M. Cedillo-Hernandez, M. Nakano, H. Perez-Meana, and A. Cedillo-Hernandez, "Improved unseen-visible watermarking for copyrigth protection of digital image," *Proc. - 2017 5th Int. Work. Biometrics Forensics, IWBF 2017*, 2017, doi: 10.1109/IWBF.2017.7935084.

[18] C. A. Micchelli, L. Shen, Y. Xu, and X. Zeng, "Proximity algorithms for the L1/TV image denoising model," *Adv. Comput. Math.*, vol. 38, no. 2, pp. 401–426, 2013, doi: 10.1007/s10444-011-9243-y.

[19] W. Yin, D. Goldfarb, and S. Osher, "Total Variation Based Image Cartoon-Texture Decomposition ‡," 2005.

[20] V. Le Guen, "Cartoon + Texture Image Decomposition by the TV-L1 Model," *Image Process. Line*, vol. 4, pp. 204–219, 2014, doi: 10.5201/ipol.2014.103.

[21] M. Yakno, J. Mohamad-Saleh, and B. A. Rosdi, "New technique for larger ROI extraction of hand vein images," *2015 Int. Conf. BioSignal Anal. Process. Syst. ICBAPS 2015*, pp. 82–87, 2015, doi: 10.1109/ICBAPS.2015.7292223.

[22] D. Koundal, R. Vishraj, S. Gupta, and S. Singh, "An automatic ROI extraction technique for Thyroid Ultrasound image," *2015 2nd Int. Conf. Recent Adv. Eng. Comput. Sci. RAECS 2015*, no. December, pp. 1–5, 2016, doi: 10.1109/RAECS.2015.7453309.

[23] L. Itti, C. Koch, and E. Niebur, "A Model of Saliency-Based Visual Attention for Rapid Scene Analysis," vol. 20, no. 11, pp. 1254–1259, 1998.

[24] Q. Lin, X. Xu, Y. Zhan, and D. Liao, "Extracting regions of interest based on visual attention model," *2011 Int. Conf. Multimed. Technol. ICMT 2011*, pp. 313–316, 2011, doi: 10.1109/ICMT.2011.6003038.

[25] V. A. Models, "Validation and Evaluation for Visual Attention Models," 2013.

[26] X. Hou, J. Harel, and C. Koch, "Image Signature: Highlighting Sparse Salient Regions," *IEEE Trans Pattern Anal Mach Intell*, vol. 34, no. 1, pp. 194–201, 2011, doi: 10.1109/TPAMI.2011.146.

[27] B. Peng, L. Zhang, and D. Zhang, "Automatic image segmentation by dynamic region merging," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3592–3605, 2011, doi: 10.1109/TIP.2011.2157512.

[28] J. Shen, Y. Du, and X. Li, "Interactive segmentation using constrained laplacian optimization," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 7, pp. 1088–1100, 2014, doi: 10.1109/TCSVT.2014.2302545.

[29] G. Mori, X. Ren, A. A. Efros, J. Malik, U. C. Berkeley, and O. Ox, "Recovering

Human Body Configurations : Combining Segmentation and Recognition 2 . Related Work," *Iccv*, no. c, p. volume 1, pages 10-17, 2003, doi: 10.4161/hv.26890.

[30] Z. Li, X. M. Wu, and S. F. Chang, "Segmentation using superpixels: A bipartite graph partitioning approach," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, no. Section 4, pp. 789–796, 2012, doi: 10.1109/CVPR.2012.6247750.

[31] J. Cheng *et al.*, "Superpixel classification based optic disc and optic cup segmentation for glaucoma screening," *IEEE Trans. Med. Imaging*, vol. 32, no. 6, pp. 1019–1032, 2013, doi: 10.1109/TMI.2013.2247770.

[32] B. Liu, H. Hu, H. Wang, K. Wang, X. Liu, and W. Yu, "Superpixel-based classification with an adaptive number of classes for polarimetric SAR images," *IEEE Trans. Geosci. Remote Sens.*, vol. 51, no. 2, pp. 907–924, 2013, doi: 10.1109/TGRS.2012.2203358.

[33] F. Yang, H. Lu, and M. H. Yang, "Robust superpixel tracking," *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1639–1651, 2014, doi: 10.1109/TIP.2014.2300823.

[34] D. Comaniciu and P. Meer, "Mean shift: A robust approach toward feature space analysis," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 5, pp. 603–619, 2002, doi: 10.1109/34.1000236.

[35] A. Vedaldi and S. Soatto, "Quick Shift and Kernel Methods for Mode Seeking," in *10th European Conference on Computer Vision*, 2008, pp. 705–718. doi: 10.1016/0020-7101(78)90038-7.

[36] L. Vincent and P. Soille, "Watersheds in Digital Spaces: An Efficient Algorithm based on Immersion Simulations," *Trans. Pattern Anal. Mach. Intell.*, vol. 13, no. 6, pp. 583–598, 1991, doi: 10.1109/34.87344.

[37] Jianbo Shi and Jitendra Malik, "Normalized Cuts and Image Segmentation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 8, pp. 888–905, 2000, doi: 10.1109/34.868688.

[38] P. F. Felzenszwalb and D. P. Huttenlocher, "Efficient graph-based image segmentation," *Int. J. Comput. Vis.*, vol. 59, no. 2, pp. 167–181, 2004, doi: 10.1023/B:VISI.0000022288.19776.77.

[39] A. P. Moore, S. J. D. Prince, J. Warrell, U. Mohammed, and G. Jones, "Superpixel lattices," *26th IEEE Conf. Comput. Vis. Pattern Recognition, CVPR*, 2008, doi: 10.1109/CVPR.2008.4587471.

[40] O. Veksler, Y. Boykov, and P. Mehrani, "Superpixels and supervoxels in an energy optimization framework," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6315 LNCS, no. PART 5, pp. 211–224, 2010, doi: 10.1007/978-3-642-15555-0_16.

[41] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Süsstrunk, "SLIC Superpixels Compared to State-of-the-Art Superpixel Methods," *EEE Trans. PATTERN Anal. Mach. Intell.*, vol. 68, no. 2, pp. 214–225, 2003, doi: 10.14890/minkennewseries.68.2_214.

[42] Y. Zhang, X. Li, X. Gao, and C. Zhang, "A Simple Algorithm of Superpixel Segmentation with Boundary Constraint," *IEEE Trans. Circuits Syst. Video*

*Technol.*, vol. 27, no. 7, pp. 1502–1514, 2017, doi: 10.1109/TCSVT.2016.2539839.

[43] H. Dobbertin, A. Bosselaers, and B. Preneel, "RIPEMD-160: A strengthened version of RIPEMD," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1039, pp. 71–82, 1996, doi: 10.1007/3-540-60865-6_44.

[44] J. Amat Rodrigo, "Optimización con enjambre de partículas (Particle Swarm Optimization)," 2019. https://www.cienciadedatos.net/documentos/py02_optimizacion_pso (accessed Sep. 18, 2022).

[45] J. Kennedy and R. Eberhart, "Particle Swarm Optimization," in *Proceedings of ICNN'95 - International Conference on Neural Networks*, 1995, pp. 1942–1948. doi: 10.1002/9780470612163.

[46] "Instituto Nacional del Derecho de Autor." https://indautor.gob.mx/accesibilidad/accesibilidad_autor.html (accessed Dec. 04, 2018).

[47] "Derecho de autor," *Fundación Wikimedia Inc*, 2018. https://es.wikipedia.org/wiki/Derecho_de_autor (accessed Jul. 23, 2018).

[48] "Diferencias entre Derechos de autor y Copyright | Creación reutilización y distribución de contenidos digitales." http://formacion.intef.es/pluginfile.php/37147/mod_imscp/content/7/diferencias_entre_derechos_de_autor_y_copyright.html (accessed Dec. 04, 2018).

[49] "Propiedad intelectual," 2023.

[50] "What Is a Copyright? - FindLaw." https://smallbusiness.findlaw.com/intellectual-property/what-is-copyright.html (accessed Dec. 04, 2018).

[51] M. Vecco, "A definition of cultural heritage: From the tangible to the intangible," *J. Cult. Herit.*, vol. 11, no. 3, pp. 321–324, 2010, doi: 10.1016/j.culher.2010.01.006.

[52] B. Borg, M. Dunn, A. Ang, and C. Villis, "The application of state-of-the-art technologies to support artwork conservation: Literature review," *J. Cult. Herit.*, 2020, doi: 10.1016/j.culher.2020.02.010.

[53] R. I. De Conservación, C. Sáizar, and I. Medina-gonzález, "Intervención. Revista Internacional de Conservación, Restauración y Museología," *Escuela Nacional de Conservación, Restauración y Museografía-INAH*, Ciudad de México, p. 92, 2010. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj3r-ay8vfqAhUDbq0KHVKjDyIQFjACegQIBxAB&url=https%3A%2F%2Fmediateca.inah.gob.mx%2Frepositorio%2Fislandora%2Fobject%2Fissue%253A1026&usg=AOvVaw1TDdYlg3HTYhIzHz_GqDlu

[54] A. Cedillo-Hernandez, M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Mariko-Nakano, and P.-M. Hector, "A Visible Watermarking with Automated Location Technique for Copyright Protection of Portrait Images," *IEICE*, vol. E99-D, no. 6, pp. 1541–1552, 2016.

[55] Nobuyuki Otsu, "A Threshold Selection Method from Gray-Level Histograms," *IEEE Trans. Syst. Man Cybern*, vol. 9, no. 1, pp. 62–66, 1979.

[56] H. Dobbertin, A. Bosselaers, and B. Preneel, "RIPEMD-160: Astrengthened version of RIPEMD," *Lect. Notes Comput. Sci.*, vol. 1039, pp. 71–82, 1996, doi: 10.1001/archsurg.1983.01390100008003.

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

[58] M. Cedillo-Hernandez, A. Cedillo-Hernandez, and F. J. Garcia-Ugalde, "Improving dft-based image watermarking using particle swarm optimization algorithm," *Mathematics*, vol. 9, no. 1795, pp. 1–20, 2021, doi: 10.3390/math9151795.

[59] O. E. Okman and G. B. Akar, "Quantization index modulation-based image watermarking using digital holography," *J. Opt. Soc. Am. A*, vol. 24, no. 1, pp. 243–252, 2007, doi: 10.1364/JOSAA.24.000243.

[60] J. G. Proakis and M. Salehi, "An Introduction to Information Theory," in *Digital Communication*, 5th ed., McGraw-Hill, 2008, pp. 336, 351, 361. doi: 10.4018/978-1-7998-6745-6.ch010.

[61] H. A. Chang and H. H. Chen, "Stochastic color interpolation for digital cameras," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 8, pp. 964–973, 2007, doi: 10.1109/TCSVT.2007.897471.

[62] C.-W. Tang and H.-M. Hang, "A Feature-Based Robust Digital Image," *IEEE Trans. signal Process.*, vol. 51, no. 4, pp. 950–959, 2003, doi: https://doi.org/10.1109/TSP.2003.809367.

[63] P. Yu, Y. Shang, and C. Li, "A new visible watermarking technique applied to CMOS image sensor," *MIPPR 2013 Multispectral Image Acquis. Process. Anal.*, vol. 8917, no. October 2013, p. 891719, 2013, doi: 10.1117/12.2031136.

[64] N. Wang, Z. Li, X. Cheng, and Z. Li, "Diffusion weighted image reversible visible watermarking algorithm based on support vector regression," *Int. Conf. Signal Process. Proceedings, ICSP*, vol. 2018-Augus, pp. 1144–1148, 2019, doi: 10.1109/ICSP.2018.8652283.

[65] K. Rangel-Espinoza, E. Fragoso-Navarro, C. Cruz-Ramos, R. Reyes-Reyes, M. Nakano-Miyatake, and H. M. Pérez-Meana, "Adaptive removable visible watermarking technique using dual watermarking for digital color images," *Multimed. Tools Appl.*, vol. 77, no. 11, pp. 13047–13074, 2018, doi: 10.1007/s11042-017-4931-3.

[66] H. Santoyo-Garcia, E. Fragoso-Navarro, R. Reyes-Reyes, C. Cruz-Ramos, and M. Nakano-Miyatake, "Visible watermarking technique based on human visual system for single sensor digital cameras," *Secur. Commun. Networks*, vol. 2017, 2017, doi: 10.1155/2017/7903198.

[67] T. Dekel, M. Rubinstein, C. Liu, and W. T. Freeman, "On the effectiveness of visible watermarks," *Proc. - 30th IEEE Conf. Comput. Vis. Pattern Recognition, CVPR 2017*, vol. 2017-Janua, pp. 6864–6872, 2017, doi: 10.1109/CVPR.2017.726.

[68] S.-C. Chuang, H. Chun-Hsiang, Wu, and Ja-Ling, "Unseen Visible Watermark," *IEE Int. Conf. Image Pro*, pp. 261–264, 2007.

[69] Y. H. Lin and J. L. Wu, "Unseen visible watermarking for color plus depth map 3D images," *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, pp. 1801–1804, 2012, doi: 10.1109/ICASSP.2012.6288250.

[70] C. H. Huang, S. C. Chuang, Y. L. Huang, and J. L. Wu, "Unseen visible watermarking: A novel methodology for auxiliary information delivery via visual contents," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 2, pp. 193–206, 2009, doi: 10.1109/TIFS.2009.2020778.

[71] O. U. Juarez-sandoval, M. Cedillo-hernandez, and M. Nakano-miyatake, "Digital image ownership authentication via camouflaged unseen-visible watermarking," pp. 26601–26634, 2018.

[72] X. L. Liu, C. C. Lin, and S. M. Yuan, "Blind Dual Watermarking for Color Images' Authentication and Copyright Protection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 5, pp. 1047–1055, 2018, doi: 10.1109/TCSVT.2016.2633878.

[73] F. Lusson, K. Bailey, M. Leeney, and K. Curran, "A novel approach to digital watermarking, exploiting colour spaces," *Signal Processing*, vol. 93, no. 5, pp. 1268–1294, 2013, doi: 10.1016/j.sigpro.2012.10.018.

[74] P. Y. Lin, J. S. Lee, and C. C. Chang, "Dual digital watermarking for internet media based on hybrid strategies," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 8, pp. 1169–1177, 2009, doi: 10.1109/TCSVT.2009.2020263.

[75] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579–1592, 2001, doi: 10.1109/83.951542.