Esquemas de Seguridad para Imágenes Digitales

Dra. Kelsey Alejandra Ramírez Gutiérrez
Cátedra CONACyT - INAOE

CONACYT

INAOE

Contenido

- Introducción
- Manipulación de Imágenes Digitales
- Métodos Activos
  - Criptografía
  - Marcas de Agua
  - Esteganografía
  - Diferencias
- Métodos Pasivos
-

Introducción

- La fotografía surge a principios del siglo XIX y desde entonces ha formado parte en la narrativa de la historia.
- La primera fotografía creada por una cámara oscura y una placa cubierta de betún en 1826 por el francés Nicéphore Niepce

Point de vue du Gras

- Actualmente, la cantidad de información transmitida y compartida a través de Internet crece exponencialmente.
- Este intercambio de información no siempre es seguro.

"Las imágenes digitales se pueden modificar muy fácilmente utilizando diferentes programas muy robustos de edición de imágenes y gráficos".

Manipulación de imágenes digitales

En la década de 1860, una composición del cuerpo de un político llamado John Calhoun y la cabeza de Lincoln





- En general, la falsificación de imágenes se puede clasificar en dos tipos:
  - alteraciones que cambian el contenido
    - splicing y copy-move
  - las que preservan el contenido
    - las manipulaciones comunes de imágenes digitales como remuestreo, compresión, mejora de contraste, desenfoque y nitidez no causan alteración de información y generalmente no tienen una intención maliciosa

- Métodos activos, extraen cierta información de la imagen; o incrustan información útil sobre la imagen bajo análisis. En ambos casos, la información extraída o incrustada se usa durante la verificación.
  - -esquemas basados criptografía, en marca de agua y en esteganografía.

- Métodos pasivos, también llamados métodos forenses, no requieren información previa sobre la imagen que está siendo analizada.

Objetivos de la seguridad de la información

Los tres objetivos de la seguridad de la información son: confidencialidad, integridad y disponibilidad (CIA).

Confidencialidad significa que la información es segura y no está disponible para la persona no autorizada.

La integridad se refiere a la exactitud de la información y la disponibilidad significa que la información está en tiempo de acceso a la persona autorizada.

La seguridad de la red no es suficiente para el intercambio confiable de información (texto, audio, vídeo, imágenes digitales, etc.)

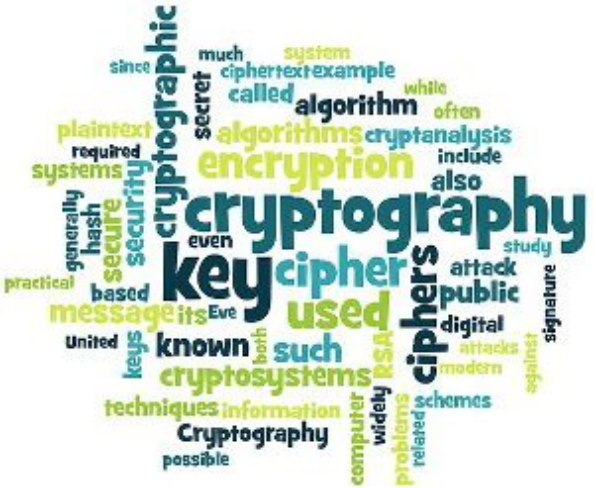
Métodos Activos: Criptografía

- La palabra criptografía proviene del griego *krypto* que significa escondido y de la palabra *graphein* que significa escritura.
- El primer sistema criptográfico (siglo V a.C,) fue la Escítala, un cilindro en el que se enrollaba una cinta con el mensaje escrito longitudinalmente(cifrar), la cinta se desenrollaba para ser enviada al receptor, quien la envolvía en un cilindro gemelo y podía leer el mensaje (descifrar).

Escítala*

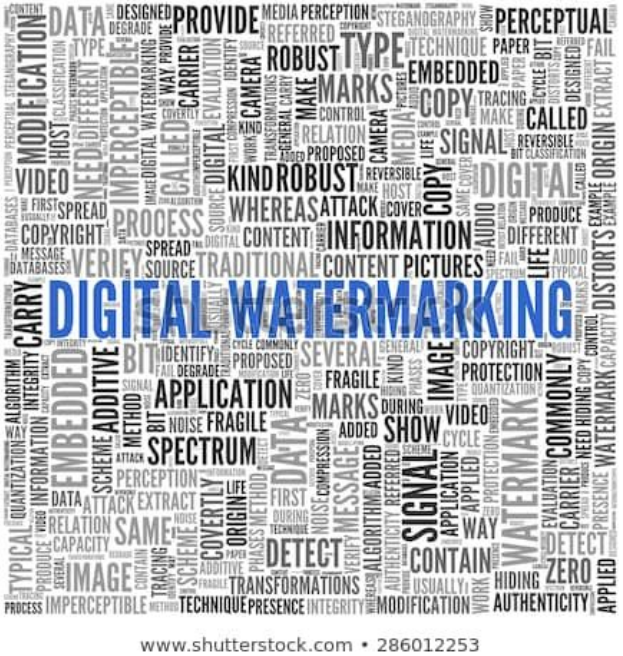
*https://es.wikipedia.org/wiki/Esc%C3%ADtala

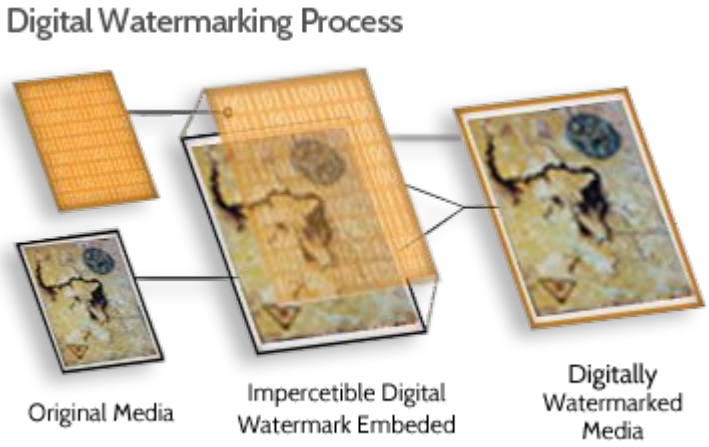
- La criptografía codifica un mensaje para que no se pueda entender. Su propósito es proteger el contenido de archivos (documentos, fotos, videos, etc.) durante su transmisión, modificando los datos originales para que sólo puedan ser recuperados por personas autorizadas.



Métodos Activos: Marcas de Agua

- Las marcas de agua se pueden clasificar como visibles e invisibles.
  - Las primeras son visibles para el ojo humano, como facturas, logotipos de compañías y logotipos de canales de televisión, etc; estas se pueden destruir fácilmente; por ser visibles y la forma de ser creadas, muchas páginas en internet en la actualidad ofrecen este servicio.
  - Las marcas de agua invisibles incrustan una señal aleatoria o una señal relacionada con la imagen, su ubicación es secreta, solo las personas autorizadas extraen la marca de agua durante el proceso de autenticación, y son invisibles al ojo humano.



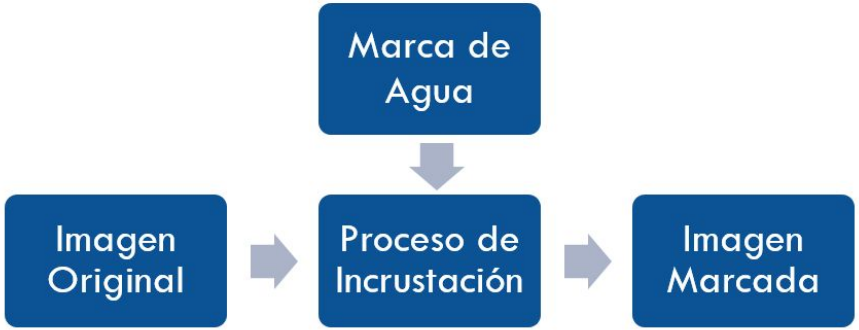


- Existen diversas aplicaciones de marcas de agua, como la detección de alteraciones, la protección de derechos de autor, la inserción de metadatos y protección de imágenes médicas.
- Se requieren algunos cálculos matemáticos para recuperar la marca de agua. Las marcas de agua invisibles son más seguras y robustas que las marcas de agua visibles.

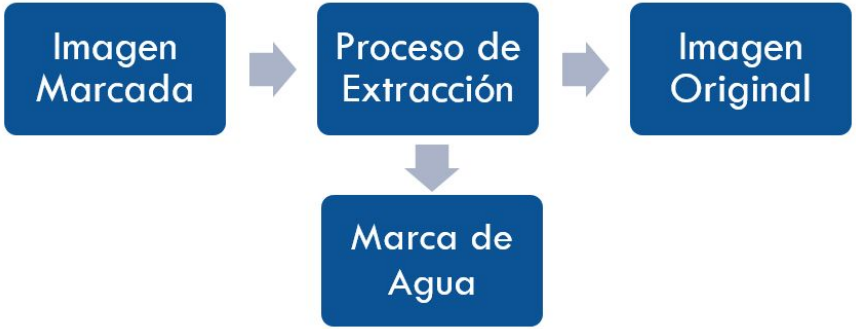
http://www.mtechprojects.org/digital-watermarking-projects.html

Proceso de Marcado de Imágenes

Incrustación de marca de agua en la imagen host.



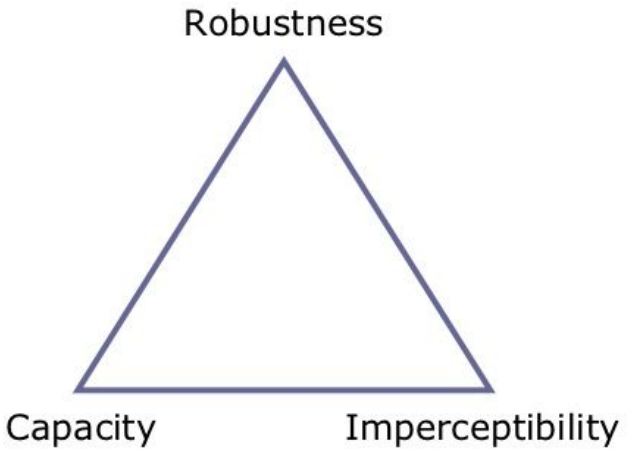
Extracción de marca de agua de la imagen.



Propiedades de las marcas de agua

- **Robustez**: La robustez es la capacidad de detección de la marca de agua después de alguna modificación a la imagen, como filtrado espacial, escaneo e impresión, compresión con pérdida, escalado y rotación, corte, mejora de imagen.
  - Robusta: está diseñada para poder sobrevivir contra ataques accidentales e intencionales. Este tipo de marca de agua se puede utilizar en monitoreo de transmisión, protección de derechos de autor, huellas digitales y control de copia.
  - Frágil: está diseñada para ser destruida en cualquier tipo de modificación, con el objetivo de detectar cualquier manipulación ilegal, incluso pequeños cambios, ataques accidentales e intencionales. Las marcas de agua frágiles se utilizan principalmente en la autenticación de contenido y la verificación de integridad. Utilizan el tipo de detección a ciegas. Además, la implementación de técnicas frágiles es más fácil que la implementación de técnicas robustas.
  - Semi-frágil: es robusta contra modificaciones incidentales, pero frágil contra ataques maliciosos. Y se utiliza para la autenticación de imágenes.

- **Imperceptibilidad**: es el requisito más importante en el sistema de marca de agua y se refiere a la similitud perceptiva entre la imagen original antes del proceso de marca de agua y la imagen con marca de agua. En otras palabras, la imagen con marca de agua debe ser similar a la imagen original, y la marca de agua debe ser invisible a pesar de la aparición de una pequeña degradación en el contraste o brillo de la imagen.
- Sin embargo, el desafío es que para lograr la imperceptibilidad se reducirá la robustez y la capacidad, y viceversa, se puede sacrificar la imperceptibilidad al aumentar la robustez y la capacidad. Además, la marca de agua no siempre desea ser invisible, a veces Se prefiere tener una marca de agua visible en la imagen.

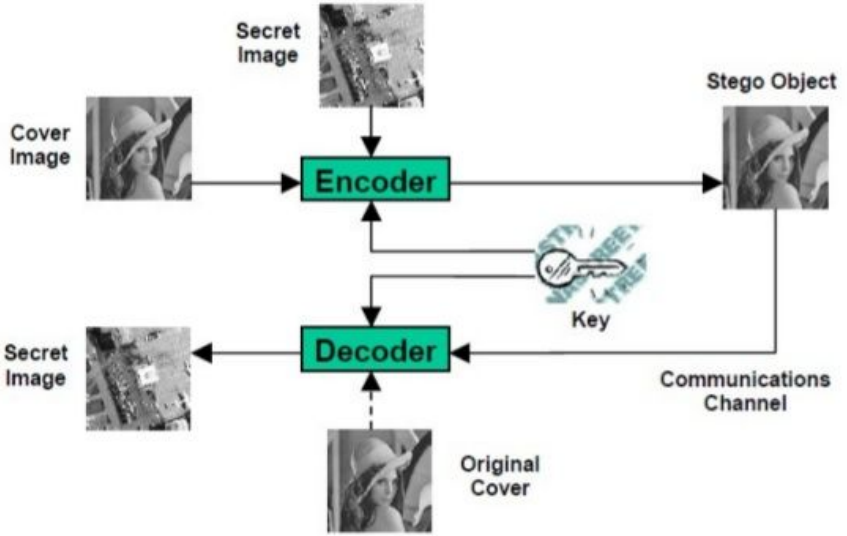


- **Capacidad**: se refiere al número de bits incrustados en la imagen. La capacidad de una imagen podría ser diferente según la aplicación para la que está diseñada la marca de agua. Además, estudiar la capacidad de la imagen puede mostrarnos el límite de la información de marcas de agua que se incrustaría y, al mismo tiempo, satisfacer la imperceptibilidad y la robustez.

- La **seguridad** es la capacidad de resistir contra ataques intencionales. Estos ataques pretenden cambiar el propósito de incrustar la marca de agua. Los tipos de ataques se pueden dividir en tres categorías principales:
  - eliminación no autorizada,
  - incrustación no autorizada y
  - detección no autorizada.
- De acuerdo con el uso específico de la marca de agua, la característica específica debe estar disponible en la marca de agua para resistir los ataques.
  - Para la *eliminación no autorizada*, la marca de agua debe ser robusta y no debe quitarse,
  - y para la *incorporación no autorizada* (también conocida como falsificación), la marca de agua debe ser frágil o semi-frágil para detectar cualquier modificación.
  - Por último, para la detección no autorizada, debe ser una marca de agua imperceptible.

Métodos Activos: Esteganografía

- Es la práctica de ocultar un archivo, mensaje, imagen o video dentro de otro archivo, mensaje, imagen o video.
- La palabra esteganografía proviene del griego *steganos (στεγανός)*, que significa "cubierto, oculto o protegido", y *graphein* (γράφειν) que significa "escritura".



- En general, un sistema esteganográfico consta de tres elementos:
  - 1) objeto de cubierta, que oculta el objeto secreto,
  - 2) el objeto secreto y
  - 3) el objeto de stego, que es el objeto de portada con el objeto secreto incrustado en su interior.
- Algunas aplicaciones de la esteganografía son: comunicación confidencial y almacenamiento de datos secretos, protección de alteración de datos, sistema de control de acceso para distribución de contenido digital, sistemas de base de datos multimedia, entre otros.

Técnicas de esteganografía digital

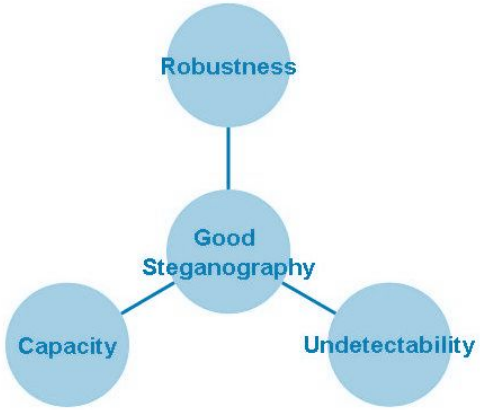
- Métodos de sustitución
  - Sustituye partes redundantes de una portadora con un mensaje secreto
  - Métodos del bit menos significativos (LSB)
- Técnicas de métodos de transformación.
  - Incrustar información secreta en un espacio de transformación de una señal (por ejemplo, dominio de frecuencia)
- Técnicas de distorsión
  - Almacena información por distorsión de señal y mide la desviación de la portadora original en el paso de decodificación
- Métodos de generación de portadoras
  - Codifica la información creando un objeto de portada (por ejemplo, generación fractal)

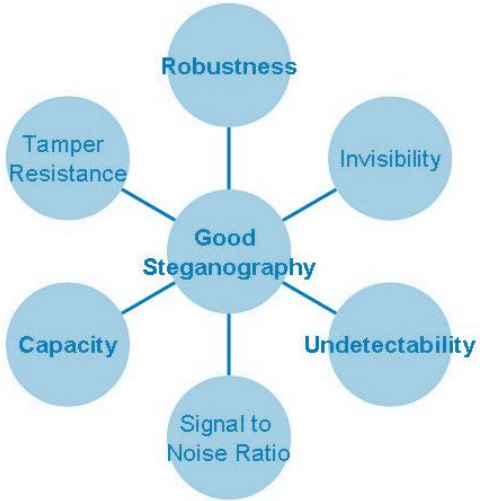
Características de la esteganografía fuerte

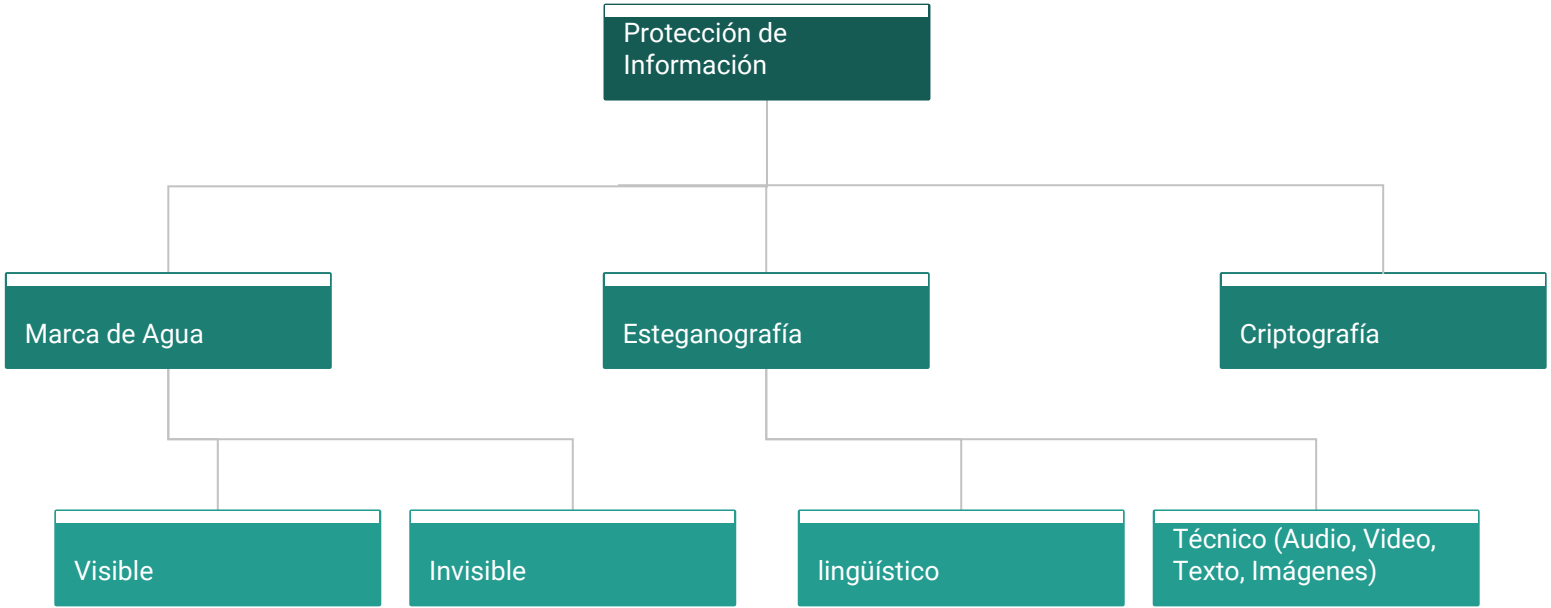
- **Capacidad**: cuántos datos pueden ocultarse
- **Invisibilidad**: incapacidad para que los humanos detecten una distorsión en el objeto stego
- **Indetectabilidad:** Incapacidad para que una computadora use estadísticas u otros métodos computacionales para diferenciar entre portadas y objetos stego
- **Robustez** :la capacidad del mensaje para persistir a pesar de la compresión u otras modificaciones comunes
- **Resistencia a la manipulación**:la capacidad del mensaje para persistir a pesar de las medidas activas para destruirlo
- **Relación señal / ruido**: la cantidad de datos codificados frente a la cantidad de datos no relacionados

Los tres componentes principales, que trabajan en oposición unos con otros, son la *capacidad*, la *indetectabilidad* y la robustez. El aumento de uno de estos hace que los otros disminuyan; por lo tanto, ninguna técnica esteganográfica puede ser perfectamente indetectable y robusta y tener una capacidad máxima.

En la mayoría de los casos, la capacidad no es tan importante como las otras dos, y mientras que la marca de agua favorece la *robustez* más fuertemente, la esteganografía en general considera la *indetectabilidad* lo más importante.






Protección de Información
Marca de Agua
Esteganografía
Criptografía
Visible
Invisible
lingüístico
Técnico (Audio, Video, Texto, Imágenes)

Diferencias

Criptografía

- Se trata de proteger el contenido de los mensajes (su significado).
- La criptografía oculta el contenido del mensaje de un atacante, pero no la existencia del mensaje.

Esteganografia

- Se trata de ocultar la existencia de mensajes.
- La esteganografía / marca de agua incluso oculta la existencia misma del mensaje en los datos de comunicación

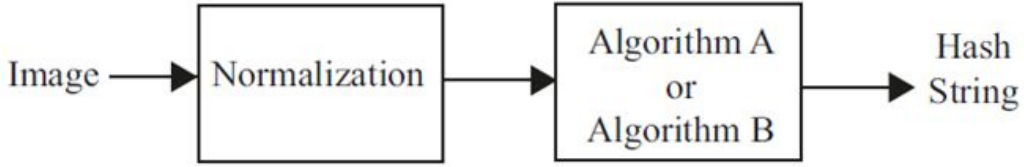
El objetivo principal de la *esteganografía* es ocultar un mensaje *m* en algunos datos de audio o video (portadora) *d*, para obtener nuevos datos *d '*, prácticamente indistinguibles de *d,* por parte de personas, de tal manera que un intruso no pueda detectar la presencia de *m* en *d '*.

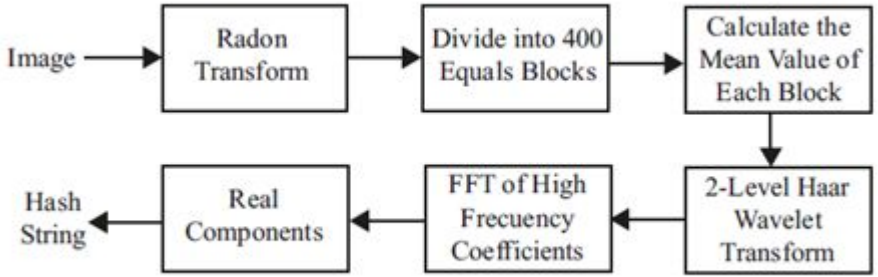
El objetivo principal de las *marcas de agua* es ocultar un mensaje *m* en algunos datos de audio o video (portadora) *d*, para obtener nuevos datos *d '*, prácticamente indistinguibles de *d*, por parte de personas, de tal manera que un intruso no pueda eliminar o reemplazar *m* en *d'.*

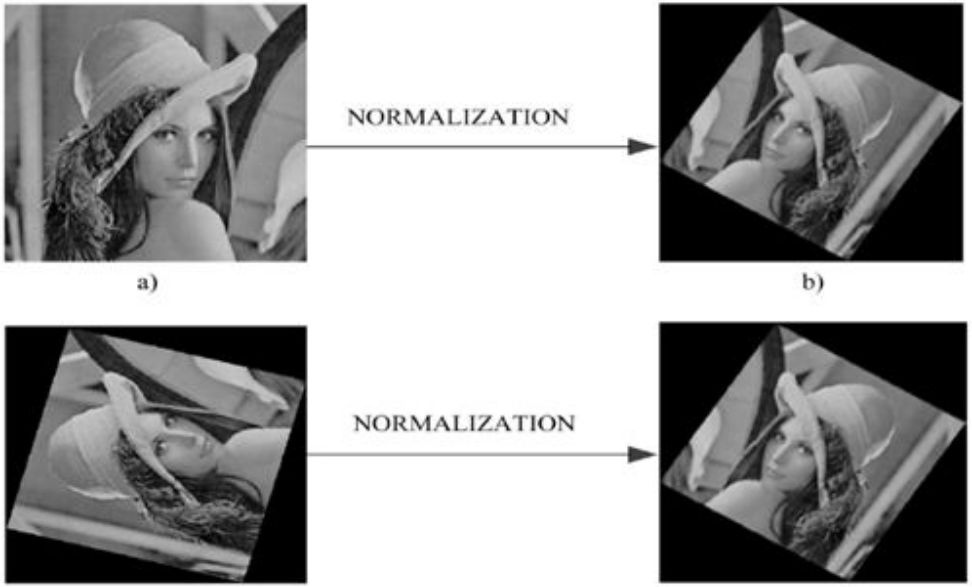
Métodos Pasivos

- Basados en detección de bordes
- Irregularidades de ruido
- Características iluminantes
- Características de textura

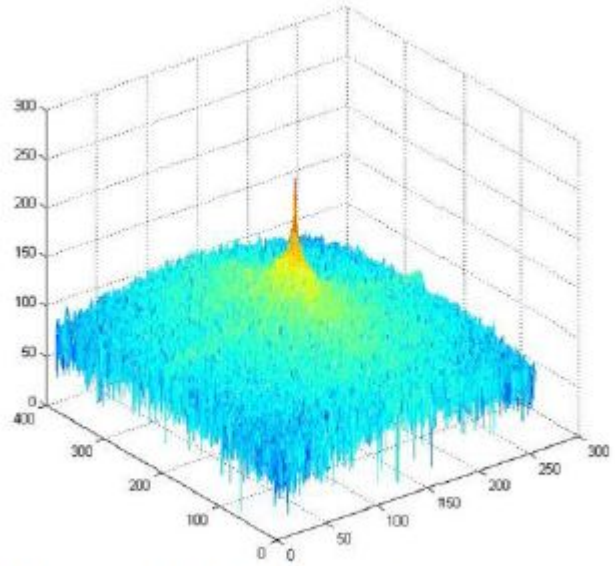
Radon-based Image Hashing using Image Normalization



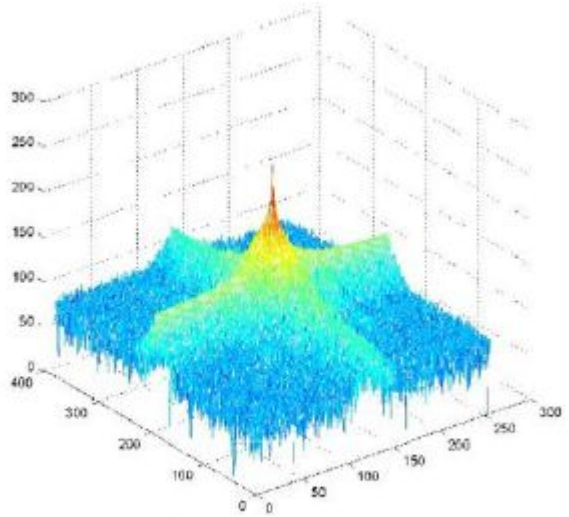




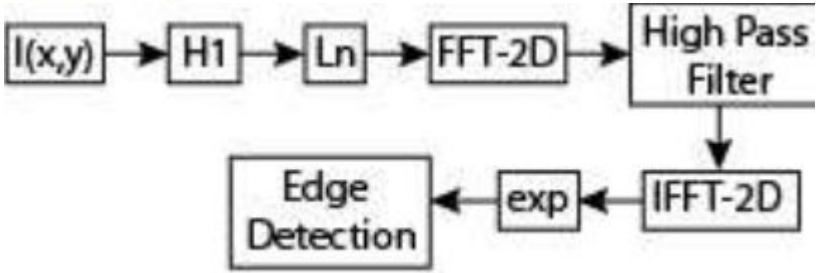
BLIND DETECTION OF IMAGE FORGERY USING BLUR EDGE DETECTION

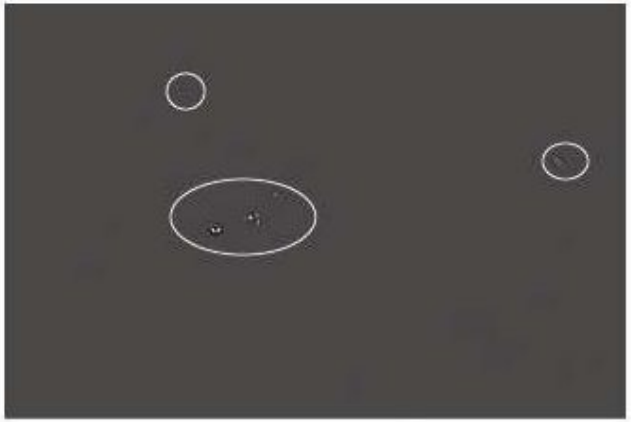


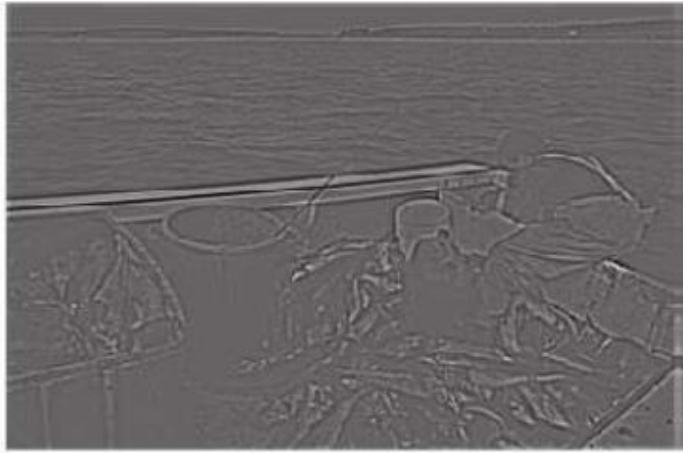
Normal image spectrum without blurring.



. Image spectrum with blurring.

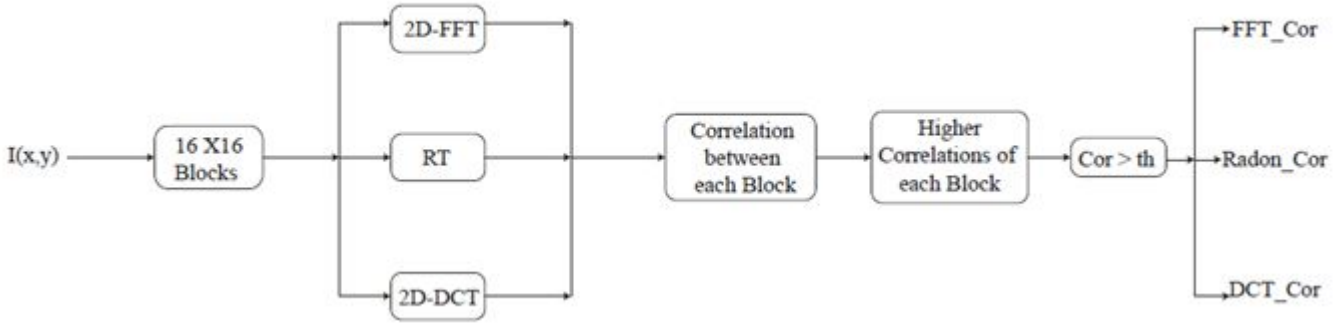




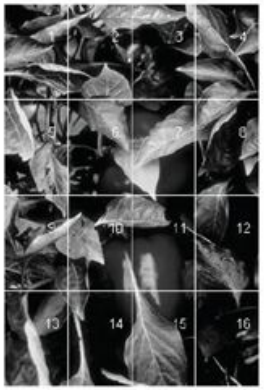


(a) (b)

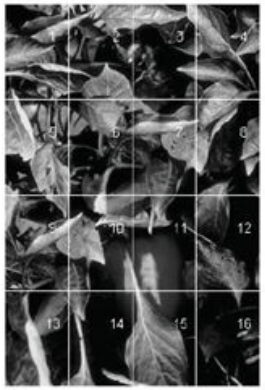
Blind Tamper Detection to Copy Move Image Forgery using SURF and MSER



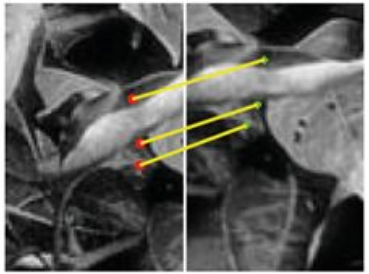
	Posibles Bloques Alterados															
Bloque No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2D-FFT	7	0	12	13	0	0	1	0	0	0	7	3	4	0	0	0
Radon	5	6	0	15	10	2	9	0	7	5	15	0	5	0	4	0
2D-DCT	5	6	0	15	15	2	4	0	7	5	15	15	5	0	4	0



(a)



(b)



(a) Imagen Original, (b) Imagen Alterada, (

(a)

(b)

(c)

Conclusiones

- La esteganografía digital es una técnica cada vez más utilizada para ocultar las comunicaciones dentro de actividades delictivas y es difícil de mitigar por los investigadores.
- Por otro lado, la marca de agua digital ayuda a los investigadores a rastrear la identidad real de los medios digitales.
- Ambos campos son relativamente jóvenes y se están realizando investigaciones para aumentar la seguridad y la solidez de estas técnicas.

1. Image Security With Different Techniques Of Cryptography And Coding: A Survey. Mona F. M. Mursi, Hossam Eldin H. Ahmed, Fathi E. Abd El-samie, Ayman H. Abd El-aziem
2. A Survey of Digital Watermarking Techniques and its Applications. Lalit Kumar Saini1, Vishal Shrivastava.
3. CHAPTER 13: Steganography and Watermarking.
4. Properties of Digital Image Watermarking. Mohammad Abdullatif, Akram M. Zeki, Jalel Chebil, Teddy Surya Gunawan
5. An Overview of Image Security Techiques. Madhu B.
6.

Gracias!

Preguntas?

kramirez@inaoep.mx