

# Watermarking

M. Graña

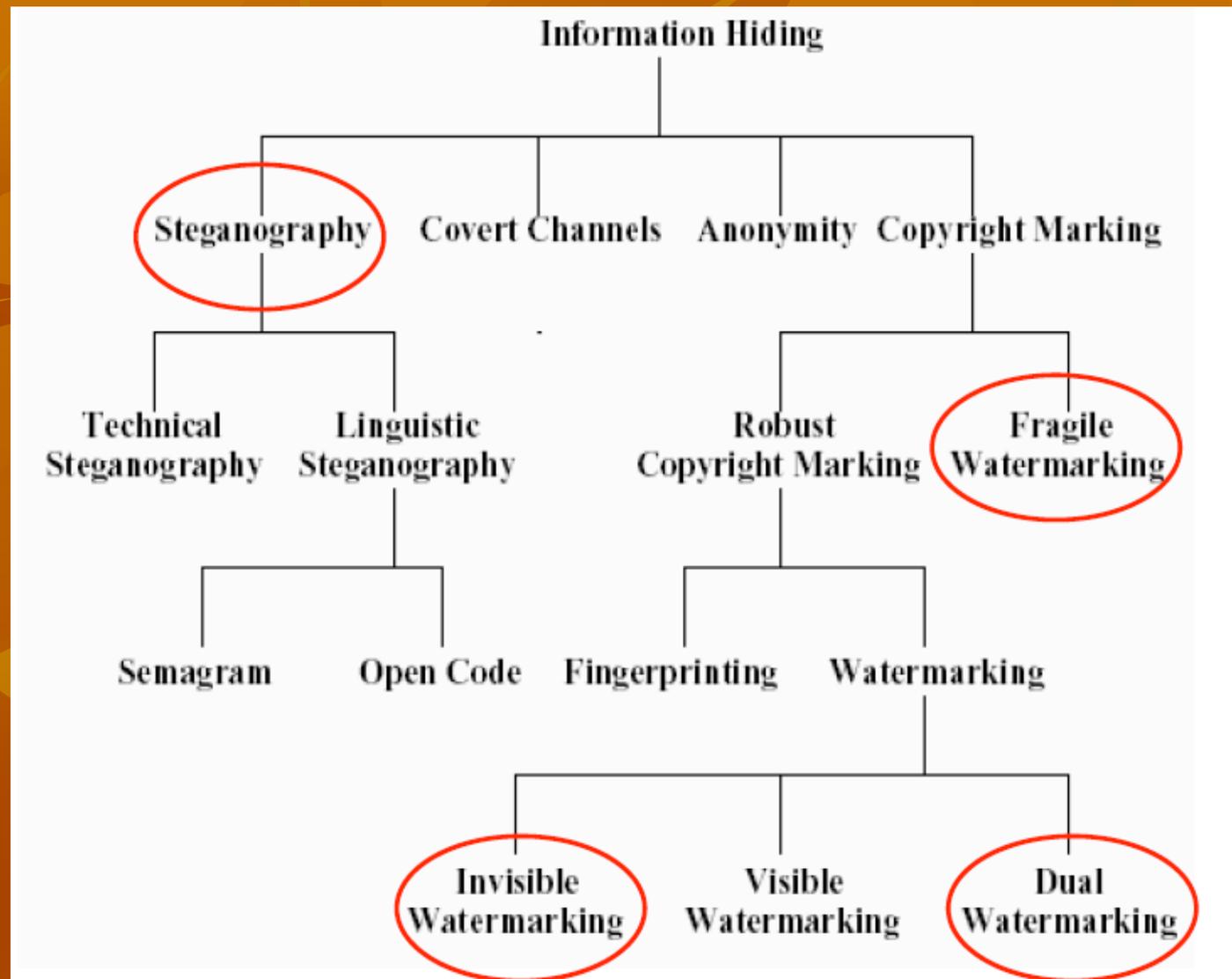
Grupo de Inteligencia Computacional

UPV/EHU



# Indice de la presentación

- Definiciones
- Esquemas de los algoritmos
- Aplicaciones





# Definiciones

- **Criptografía:** codificación de un mensaje para que sólo pueda ser descifrado por el poseedor de la clave apropiada.
- **Estenografía:** ocultación de la existencia de una codificación en un mensaje aparente.
- **Marca de agua (watermark):** encastrado de la información en el objeto



# Definiciones

- Marca de agua
  - Prensado del papel en pasta para obtener una impresión de una imagen cuando se realiza el secado de las fibras:
    - Papel moneda
    - Certificación de origen del papel
  - En objetos digitales se encastra la información que constituye la marca en el objeto introduciendo distorsión



# Definiciones

- Tipos de objetos digitales
  - Audio
  - Imagen
    - Fotografía digital
    - Médica
    - Reconocimiento remoto
  - Video
  - Otros:
    - señales de sensores diversos
    - Objetos 3D sintéticos



# Definiciones

- Utilidad de la marca de agua digital
  - Certificación de
    - autoría y
    - propiedad intelectual
  - Detección de alteraciones



# Definiciones

- Tipos de marcas de agua
  - Perceptible o visible
  - Imperceptible
    - Frágil
    - Robusta
  - Doble perceptible/imperceptible



# Definiciones

- Visible watermark
  - Tipos de objetos: imágenes, señales de video
  - Superposición de una imagen traslúcida sobre la imagen original
  - Utilidad: indicación de propiedad
  - Inconveniente: altera visiblemente la imagen/video
  - Propiedades deseables
    - Difícil de remover
    - Automatización



# Definiciones

- Watermark invisible y robusto
  - Información encastrada de forma que
    - la señal marcada no se altera perceptualmente
    - puede ser recuperada tras manipulaciones de la señal
  - Utilidad: demostración de propiedad
  - Tipos de señales: audio, imagen, video
  - Propiedades deseables:
    - Baja distorsión de la señal marcada
    - Automatización,
    - Recuperación sólo con el algoritmo apropiado



# Definiciones

- Watermark invisible y frágil
  - La información se encastra de forma que
    - No es perceptible el cambio en la señal marcada
    - Las zonas manipuladas de la señal se muestran en la marca recuperada
  - Utilidades: detección de manipulaciones
  - Tipos de señal: audio, imagen, video
  - Propiedad deseable:
    - Segura: debe ser imposible rehacer el marcado tras la manipulación de la señal



# Definiciones

- Dual watermark
  - Se añade una marca visible
  - Se encastra una marca invisible
  - Utilidad: reforzar la marca visible



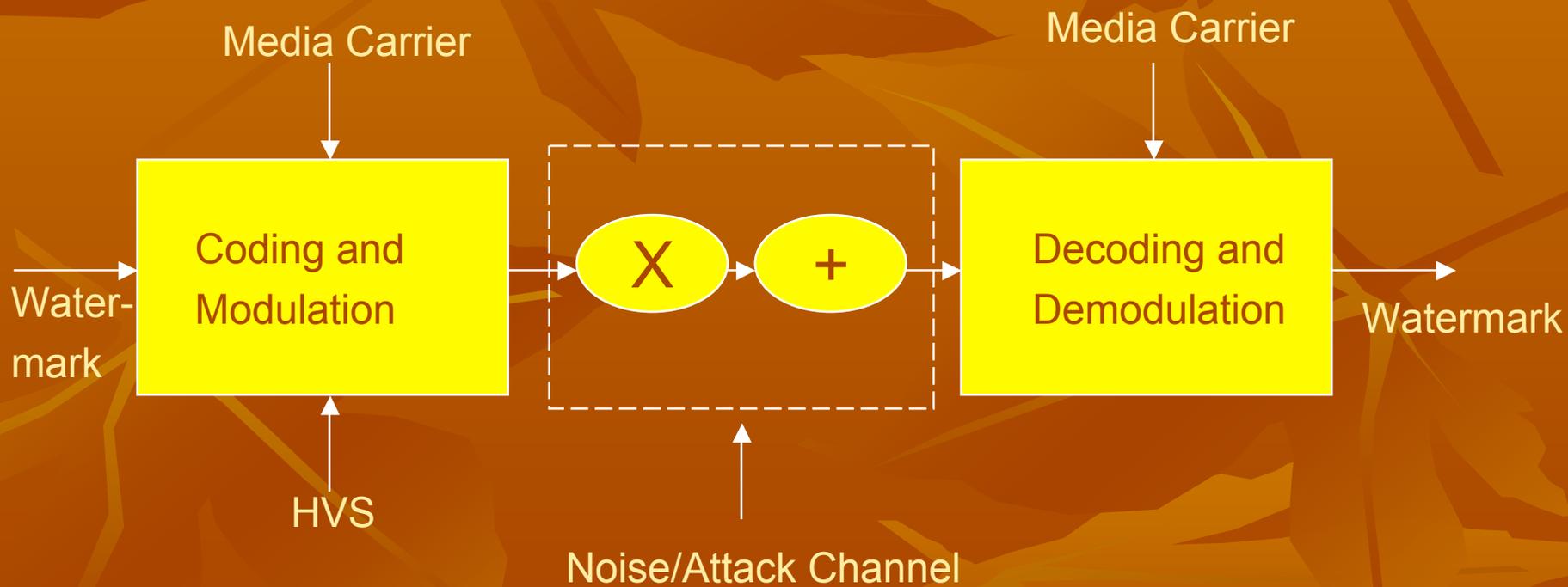
# Definiciones

- Elementos del proceso de marcado
  - Watermark, marca de agua
  - Algoritmo de encastrado (embedding, encoder)
  - Algoritmo de extracción de la marca (decoder, extraction)
    - Algoritmo de extracción
    - Algoritmo de comparación de marcas (i.e.: correlación)



# Definiciones

- Tipos de ataques a las imágenes marcadas
  - Compresión con pérdida: JPEG, MPEG
  - Distorsión geométrica: escalado, rotación, traslación, recorte
  - Operaciones de procesado: filtrado, conversiones analógico/digital, remuestreo, cambios de espacio de color, dithering, intercambio de píxeles,...
  - Intencionales: impresión y reescaneado, rewatermarking, ...



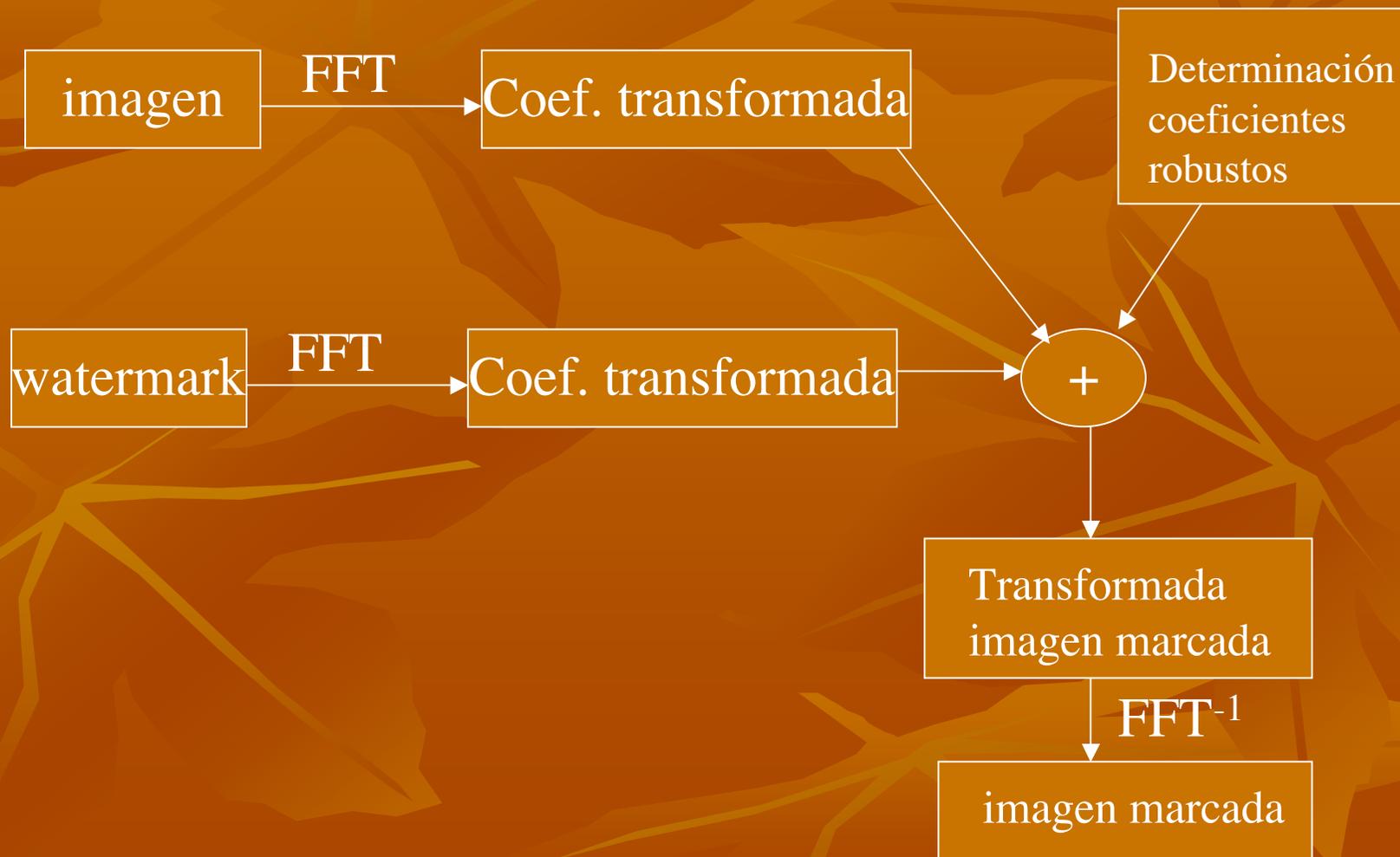


# Algoritmos de encastrado

- Tipos básicos:
  - Operación sobre el espacio transformado
    - FFT
    - DWT
    - DCT
  - Operación sobre la intensidad de la imagen
    - Determinación de las posiciones de pixeles a alterar

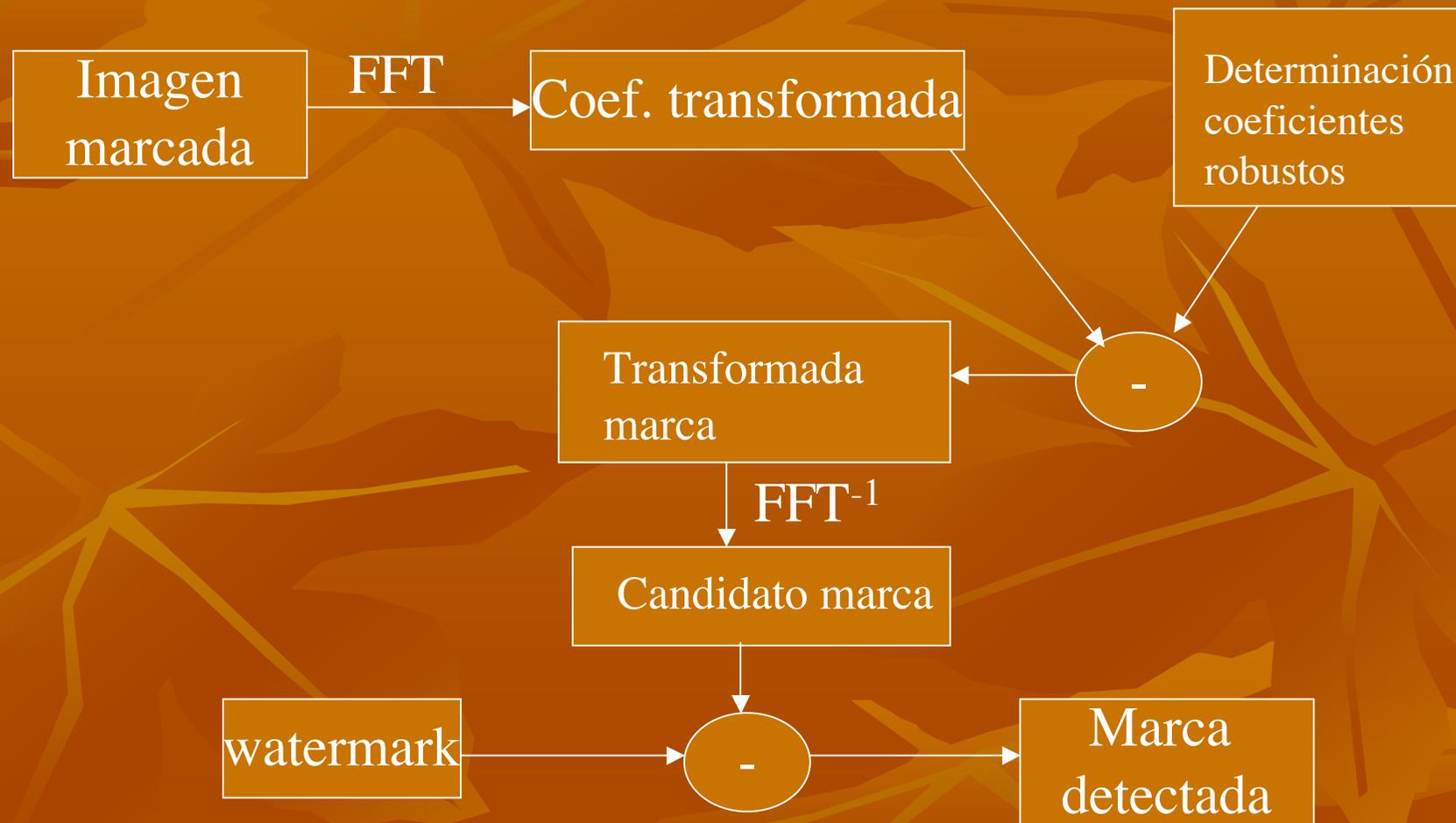


# Encastrado





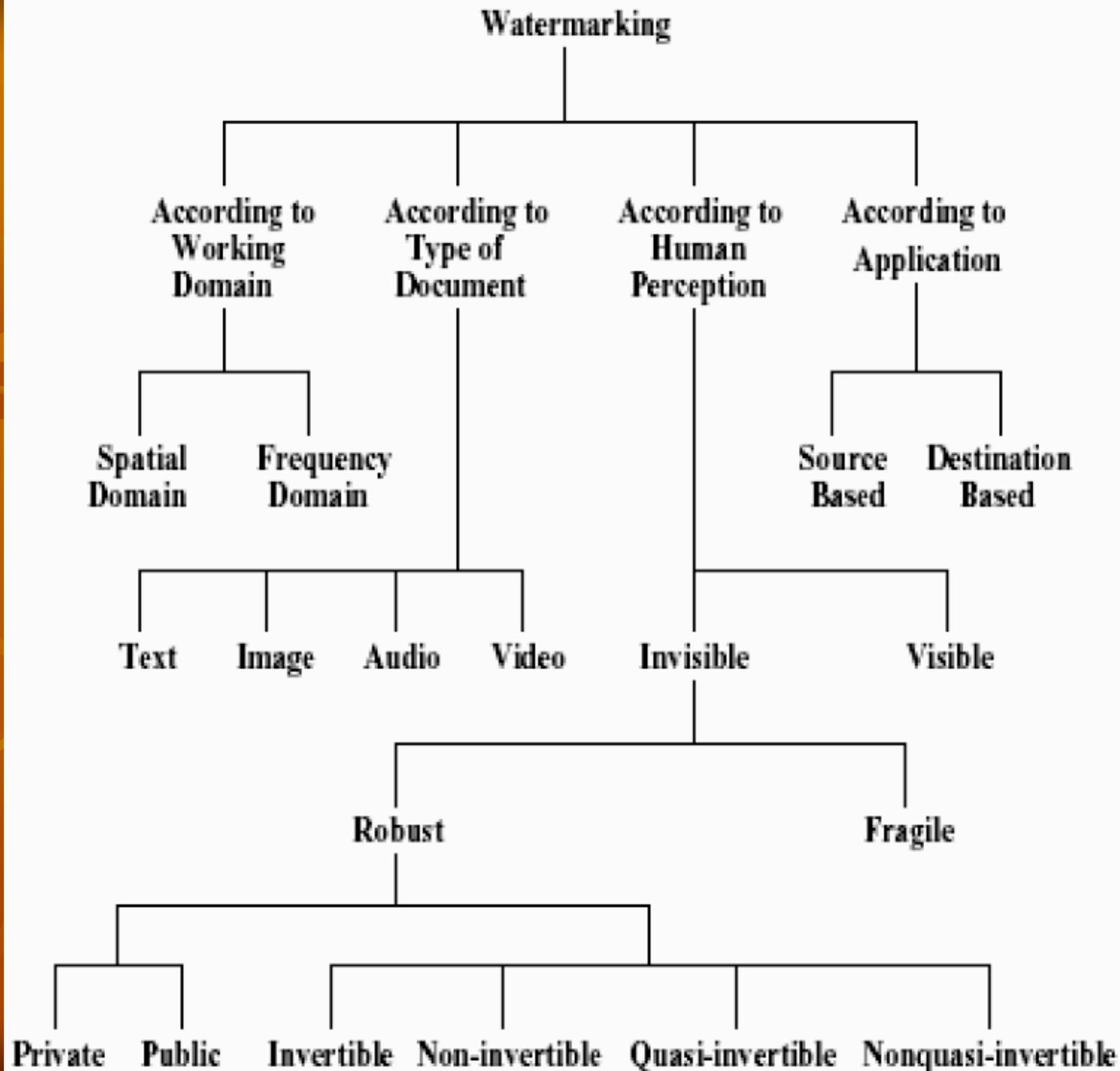
# Extracción





# Variaciones

- La marca se encripta con llave pública
  - Dar la impresión de que no existe marca (estenografía)
- Transformada utilizada
  - Transformaciones específicas del objeto
- Test de detección de la marca





# Aplicaciones

- Búsqueda de imágenes/ señales publicadas con watermarks no reconocidos: property mining
- Fingerprinting:
  - encastrar información sobre el receptor legal de transacciones electrónicas
- Monitorización de emisiones
- Protección de copia (DVD)
- Copyright protección
- Autenticación de contenidos



# Requerimientos

- Imperceptibilidad
- Robusted
- Seguridad:
  - Conocimiento del algoritmo de marcado no permite detectar o eliminar la marca
- Payload: cantidad de información en la marca
- Informado vs no informado:
  - Se requiere o no la imagen (señal) original para extraer la marca