UNIVERSIDAD DE GUADALAJARA

Centro Universitario de Ciencias Exactas e Ingenierías

División de Tecnologías para la Integración Ciber-Humana

Análisis de algoritmos

Jennifer Patricia Valencia Ignacio, Código: 223991721

Elizabeth Arroyo Moreno, Código: 221453749

Karla Rebeca Hernández Elizarrarás, Código: 223991977

Ingeniería en computación

Avance - presentación Divide y Vencerás

15 de Octubre de 2025

Detección y extracción LSB implementando Divide y Vencerás

La esteganografía por Least Significant Bit altera los bits menos significativos de los canales de una imagen para ocultar información. Este algoritmo inserta información en los bits menos importantes de las píxeles de una imagen y luego revisa si hay mensajes escondidos usando pruebas estadísticas en el canal rojo. Permite esconder mensajes en imágenes sin que se note y también detectar cambios o datos ocultos de manera rápida. Se puede usar en seguridad digital y en análisis forense de imágenes.

Usando divide y vencerás te permite localizar rápidamente las regiones sospechosas para evitar hacer trabajo sobre áreas limpias, lo que reduce significativamente el costo mediante la división de subregiones.
Técnicamente permite localizar hotspots estadísticos con pruebas baratas y podar regiones que se comportan como limpias, concentrando el esfuerzo donde hay mayor probabilidad de que exista algo oculto. Esto reduce el costo práctico y facilita la localización y extracción dirigida.

Estructura general del algoritmo

1. División
La imagen se va dividiendo en partes más pequeñas, si alguna parte todavía es muy grande se sigue dividiendo hasta llegar a un tamaño mínimo.

2. Resolución de subproblemas
A cada una de esas subregiones se le aplica una prueba rápida para ver si hay señales de manipulación en el canal rojo. Si se detecta algo raro, esa zona se vuelve a dividir para encontrar con más precisión el área sospechosa.

3. Combinación de resultado
Se juntan los resultados de todas las subregiones para crear un mapa general que muestra dónde es más probable que haya algo oculto. Las zonas donde no hay nada raro se descartan y las sospechosas se marcan para analizarlas más a fondo.

Aplicación en la vida real

En contextos de seguridad informática y forense digital, la esteganografía digital representa una amenaza crítica. A diferencia de la criptografía que hace datos ilegibles, la esteganografía oculta la existencia misma de la comunicación. Agentes de seguridad, analistas forenses y profesionales de ciberseguridad necesitan detectar y extraer información oculta que puede revelar actividades delictivas, comunicaciones no autorizadas o transferencia no controlada de información clasificada.

Aplicación práctica

En seguridad de redes, detectores automáticos interceptan imágenes compartidas en redes sociales así como plataformas de mensajería para identificar posibles canales ocultos de comunicación delictiva. En forense digital e investigación criminal, analistas procesan gran variedad de imágenes confiscadas de dispositivos sospechosos, necesitando localizar rápidamente cuáles contienen información oculta y donde se encuentra. En protección de derechos de autor, sistemas automatizados verifican si marcas de agua o metadatos han sido alterados o complementados con información no autorizada.

Complejidad computacional

Con la Fuerza Bruta siendo un método lineal se recorren todos los píxeles de la imagen, aplicando tests estadísticos sobre la totalidad de datos. Una imagen típica de 4000×3000 píxeles contiene 12 millones de píxeles. Aplicar Chi-cuadrado, Entropía y RS Analysis sobre cada píxel y región requiere tiempo de ejecución que escala linealmente: O(n) por cada test, resultando en tiempo acumulado O(m·n) donde n es el número de tests aplicados. Para imágenes de muy alta resolución, esto se vuelve ineficiente . Adicionalmente, el método tradicional no proporciona información sobre dónde está concentrada la anomalía, lo cual es crítico para análisis forense dirigido. El desafío es reducir el tiempo de análisis mediante identificación y exclusión temprana de regiones limpias, concentrando recursos computacionales sólo donde exista evidencia de ocultamiento.

Peor caso (todo es sospechoso): el algoritmo recorre todas las hojas : O(n), similar a Fuerza Bruta.
Caso esperado con poda: si gran parte de la imagen es “limpia”, el costo baja a $O(n \cdot \alpha)$con $\alpha < 1$, debido a que muchas ramas se podan tras un test ligero.

Ventaja:

- Permite paralelizar por subregión (hilos o procesos), acelerando el tiempo real de ejecución.
- Evitar trabajo innecesario y no analizar cada píxel si no hace falta.
- Más rápido en imágenes grandes o con ocultamiento localizado.
- Localiza zonas exactas donde hay datos ocultos.
- Paralelizable: puede usar varios núcleos del procesador.
- Escalable y adaptable: se ajustan los umbrales según el tipo de imagen.

División de tareas.

Jennifer: Investigación y Diseño.

- Investigación de Divide y Vencerás aplicado a esteganografía LSB.
- Diseño de estrategia de división de imagen en subregiones.
- Definición de criterios de poda y umbrales.
- Análisis de complejidad computacional O(n) vs O(n·α).
- Pseudocódigo del algoritmo.

Rebeca: Implementación

- Implementación de función recursiva dividir_y_analizar().
- Implementación de sistema de poda de regiones limpias.
- Integración de pruebas estadísticas en cada nivel de recursión.
- Implementación de detección de "hotspots" (zonas sospechosas).
- Optimización del código para evitar cálculos redundantes.

Elizabeth: Visualización y Pruebas.

- Representación visual de áreas con alteraciones.
- Creación de casos de prueba (imágenes limpias/modificadas).
- Comparación de rendimiento: Fuerza Bruta vs Divide y Vencerás.
- Medición de tiempos y benchmarking.
- Gráficas comparativas de resultados.