# Práctica 2
# Esteganografía Avanzada con Distribución Aleatoria y Cifrado

Daniela Stefany Sánchez Ayala
Ingeniería en Telemática
UPIITA - IPN

## 1. Introducción

La técnica LSB secuencial es vulnerable ante métodos de detección estadística. Para mejorar la seguridad, se implementó una versión robusta que combina distribución pseudoaleatoria de posiciones y cifrado XOR con clave derivada de SHA-256.

## 2. Marco Teórico

El protocolo implementado incluye:

1. Derivación de clave mediante SHA-256.
2. Cifrado XOR del mensaje.
3. Selección pseudoaleatoria de posiciones usando una semilla.
4. Incrustación de bits en posiciones dispersas.

El análisis estadístico se realizó mediante la prueba chi-cuadrado:

$$\chi^2 = \frac{(O_0 - E)^2 + (O_1 - E)^2}{E}$$

Un valor cercano a cero indica distribución uniforme.

# 3. Resultados

| Método | PSNR (dB) | $\chi^2$ | Detectable | Sin clave |
|---|---|---|---|---|
| Imagen original | $\infty$ | 1520 | No | N/A |
| LSB secuencial | 46.8 | 12.4 | Sí | Sí |
| LSB aleatorio + XOR | 46.6 | 1487 | Difícil | No |

Cuadro 1: Comparativa de métodos

Se observa que el método aleatorio mantiene valores de $\chi^2$ similares a la imagen original, reduciendo la sospecha estadística.

# 4. Análisis

La distribución pseudoaleatoria dispersa las modificaciones en toda la imagen, evitando patrones detectables.

El cifrado XOR no es completamente seguro si se reutiliza la clave, ya que puede ser vulnerable a ataques de texto conocido. Se recomienda AES-CTR o AES-GCM para mayor seguridad.

Para ocultar archivos binarios, se debe almacenar directamente la secuencia de bytes junto con el encabezado de longitud.

El análisis RS sería efectivo contra LSB secuencial, pero pierde eficacia cuando se utiliza distribución aleatoria.

# 5. Conclusiones

La combinación de distribución pseudoaleatoria y cifrado mejora significativamente la seguridad del sistema sin afectar notablemente el PSNR. Este enfoque ofrece mayor resistencia ante análisis estadístico y extracción no autorizada.