Instituto Politécnico Nacional

Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas

Multimedia

Estenografía avanzada: Distribución aleatoria y cifrado

Soto Gutiérrez Ian Alexis

3TM2

Esta práctica busca complementar lo realizado en trabajos anteriores siguiendo la línea de la estenografía solo que ahora se busca un cifrado avanzado, no solo para que sea imperceptible a simple vista, sino que también al momento de extraer la información de la imagen. Esto se garantiza con el cifrado de datos XOR con clave derivada donde si se extraen los datos de la imagen (bits) se obtenga contenido basura o ilegible si no se posee la clave de acceso correcta.

Otra manera en la que se garantiza la seguridad de los datos es mediante la generación de coordenadas aleatorias ya que en proceso anteriores la información se guardaba de manera secuencial y ahora, se generan valores aleatorios donde se ocultará la información, con esto se evita que el mensaje se concentre en un solo lugar.

Al realizar la modificación en los bits menos significativos, el algoritmo que implementa Chi-cuadrado (x^2) se encargó de comparar las frecuencias de unos y ceros para las imágenes cargadas, imagen original (BMP), imagen estenografiada y la imagen generada por este código (valores aleatorios).

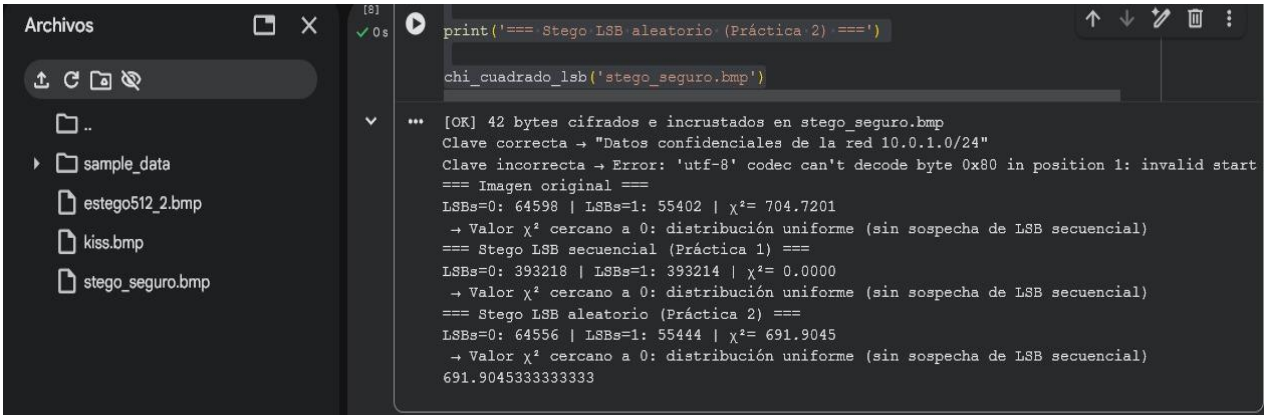

Figura 1. Resultado del algoritmo x^2

Método	PSNR (dB)	X^2 LSB	Detectable	Decodificable sin clave
Imagen limpia	∞	704.7201	No	N/A

LSB secuencial	704.7201	0	No	Si
LSB aleatoria + XOR	706.2536	691.6045	No	No

Preguntas de análisis

1. ¿En qué medida mejora la distribución aleatoria a la resistencia de análisis x^2 respecto al LSB secuencial?

   Mejora de manera significativa dado a la uniformidad estadística, esto dado que los bits se distribuyen a lo largo de la imagen se crea un valor de x^2 manteniendo un rango normal como se muestra en la figura 1. De igual manera, con la distribución aleatoria provoca que la alteración en los bits sea esparcida por toda la imagen lo cuál minimiza la alteración de algún bit es específico.

2. El cifrado XOR con clave derivada de SHA-256 no es criptográficamente seguro por sí solo para todos los caos de uso. ¿Cuál es principal vulnerabilidad? ¿Qué algoritmo recomendaría en su lugar?

   Las vulnerabilidades que se pueden presentar son:

   - Falta de integridad: Al receptor no se le garantiza que el mensaje no fue alterado antes de la entrega.
   - Claves reusadas: Se puede presentar el caso de que se reutilice una contraseña en archivos distintos, el problema radica en que la secuencia de bits implementada por el algoritmo será la misma.
   - Vulnerabilidad: Si algún atacante descifra parte del texto original donde con una operación de tipo XOR se puede obtener la clave derivada.

3. ¿Qué cambios haría en el protocolo no solo para guardar texto sino también un archivo binario?

   Ahora se debería de realizar una lectura de tipo binario (“rb”), esto es con el fin de pasar de analizar cadenas de caracteres a bytes completos, el algoritmo de x^2 se implementará de igual forma, solo que ahora se manejaran bytes completos