Criptografía y Seguridad *(72.44)*

TRABAJO PRÁCTICO: ESTEGANOGRAFÍA

Cuestiones a analizar

1. Discutir los siguientes aspectos relativos al documento.
    a. Organización formal del documento.
    b. La descripción del algoritmo.
    c. La notación utilizada, ¿es clara? ¿hay algún error o contradicción?
2. Esteganografiar un mismo archivo en un .bmp con cada uno de los tres algoritmos, y comparar los resultados obtenidos. Hacer un cuadro comparativo de los tres algoritmos estableciendo ventajas y desventajas.
3. Explicar detalladamente el procedimiento realizado para descubrir qué se había ocultado en cada archivo y de qué modo. Indicar qué se encontró en cada archivo.
4. Algunos mensajes ocultos tenían, a su vez, otros mensajes ocultos. Indica cuál era ese mensaje y cómo se había ocultado.
5. Uno de los archivos ocultos era una porción de un video, donde se ve ejemplificado una manera de ocultar información ¿cuál fue el portador?
6. ¿De qué se trató el método de estenografiado que no era LSB1 ni LSB4 ni LSBI? ¿Es un método eficaz? ¿Por qué?
7. Para la implementación del algoritmo del documento de Juneja y Sandhu, se tomó como clave RC4 los primeros pixeles de la imagen portadora. ¿de qué otra manera podría considerarse o generarse o guardarse la clave RC4?
8. Según el libro de Katz, hay una forma más segura de usar RC4. ¿se podría implementar en este algoritmo LSBI?
9. ¿por qué la propuesta del documento de Juneja y Sandhu es realmente una mejora respecto de LSB común?
10. En el documento, Juneja y Sandhu indican que la inserción de los bits en la imagen es aleatoria. ¿es realmente así? ¿de qué otra manera podría hacerse los “saltos” de inserción de bits?
11. ¿Qué dificultades encontraron en la implementación del algoritmo del paper?
12. ¿Qué mejoras o futuras extensiones harías al programa stegobmp?