Ejercicios Finales

Ejercicio 1:

Descarga el siguiente archivo:

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas mauris nunc, gravida ac elementum quis, viverra sit amet nibh. In venenatis nulla ac tellus condimentum rhoncus faucibus eros volutpat. Donec sit amet tempus ante. Aenean a risus dui. Vivamus iaculis, augue at mollis blandit, mi lacus dapibus mauris, sit amet aliquam urna sapien sed nisl.....

`http://www.0xword.com/recursos/esteganografia/ej1.txt`

Usa “stepic” para ocultar el mensaje en ej1.tif con el siguiente comando, tal y como se ha explicado en el apartado 3.1.2:

```
$ stepic -e -i ej1.tif -o ej1_stepic.tif -t ej1.txt
```

Puedes verificar que el mensaje ser recupera correctamente usando el siguiente comando:

```
$ stepic -d -i ej1_stepic.tif -o ej1_stepic.txt
```

a) ¿Existe un mensaje oculto con Stepic en la imagen ej1.tif? ¿Cómo podemos estar seguros?
b) Esconde el archivo ej1.txt en ej1.tif y realiza un ataque visual para detectar que se está escondiendo información.

Ejercicio 2:

Descarga los archivos:

`http://www.0xword.com/recursos/esteganografia/ej2a.png`
`http://www.0xword.com/recursos/esteganografia/ej2b.png`

¿Se trata de imágenes con mensaje oculto?

Ejercicio 3:

¿Cuál es el principal riesgo de obtener una imagen *cover* de Internet y usarla para ocultar datos mediante esteganografía?

Ejercicio 4:

Descarga los archivos:
`http://www.0xword.com/recursos/esteganografia/ej4a.jpg`
`http://www.0xword.com/recursos/esteganografia/ej4b.jpg`

¿Se trata de imágenes con mensaje oculto?**.**

Ejercicio 5:

¿Es posible recuperar la imagen en su estado original después de extraer el mensaje?

Ejercicio 6:

Descarga el archivo: `http://www.0xword.com/recursos/esteganografia/ej6.tif`

Esta imagen tiene un mensaje oculto ¿Sabrías decir con que método se a insertado?

Ejercicio 7:

La inserción mediante el desplazamiento del histograma de predicción de errores proporciona un método reversible que no deja marcas en el histograma de intensidad de los píxeles. Pero si puede existir cierta marca en el histograma de predicción, aunque queda un poco oculta por el hecho de que el atacante no conoce la fórmula usada para realizar la predicción. Por ello, esta fórmula es importante para la seguridad del sistema.

Diseña una fórmula de predicción para este método que varíe en función de una clave.

Ejercicio 8:

El *matrix embedding* nos permite ocultar información en la imagen modificando menos píxeles, pero para ello tenemos que construir bloques de píxeles, que aunque no los modificaremos, deben existir. Por ejemplo, si dividimos la imagen en bloques de 15 píxeles, podemos ocultar 4 bits de información, modificando un único bit.

a) Si usamos bloques de 1023 bits ¿Cuántos bits insertaremos cada vez que modifiquemos un bit?
b) ¿Qué tamaño debería tener una imágen para poder almacenar en ella 32 bits modificando un solo bit?

Ejercicio 9:

Los sistemas modernos de esteganografía ocultan información en zonas de la imágenes difíciles de modelar, como bordes o texturas. ¿Cuál es el motivo de que usen *Wet Paper Codes*?

Ejercicio 10:

En la actualidad el *machine learning* se ha convertido en una herramienta indispensable para el estegoanalista. Con ella, es posible entrenar a un clasificador para que reconozca qué imágenes tienen mensaje oculto y cuáles no.

Consigue una base de datos de imágenes, separa 2000 imágenes y forma dos grupos de 1000 imágenes cada uno.

En cada uno de los grupos, escoge 500 imágenes e inserta en ellas información usando LSB*matching*. Borrando posteriormente las originales.

De esta manera te quedarán dos grupos de 1000 imágenes, 500 cover y 500 stego. Al primer grupo lo llamaremos conjunto de entrenamiento, al segundo, conjunto de prueba.

Entrena una máquina SVM con el conjunto de prueba y verifica con el conjunto de test que los resultados son buenos.

a) ¿Qué ocurre si pruebas el clasificador con imágenes de la misma base de datos, que no estén en los conjuntos de entrenamiento y prueba?
b) ¿Qué ocurre si pruebas el clasificador con imágenes de otra base de datos distinta?

Ejercicio 11:

Descargar el fichero de audio que se encuentra en la siguiente dirección:
`http://www.0xword.com/recursos/esteganografia/ej11.wav`

¿Se puede afirmar que existe un mensaje oculto en este fichero de audio? en caso afirmativo, ¿qué técnica se ha utilizado?
Intenta descubrir el mensaje.

Ejercicio 12:

Descargar el fichero de audio que se encuentra en la siguiente dirección:
`http://www.0xword.com/recursos/esteganografia/ej12.wav`

¿Se puede afirmar que existe un mensaje oculto en este fichero de audio? en caso afirmativo, ¿qué técnica se ha utilizado?
Intenta descubrir el mensaje.

Ejercicio 13:

Descargar el fichero de audio que se encuentra en la siguiente dirección:

`http://www.0xword.com/recursos/esteganografia/ej13.wav`

Inserta el siguiente mensaje dentro del fichero utilizando la técnica del LSB pero aplicando aleatoriedad para que no pueda ser reconocido el contenido y a la vez, utilizando todo el fichero, lo que imposibilitará el ataque visual.

"Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas mauris nunc, gravida ac elementum quis, viverra sit amet nibh. In venenatis nulla ac tellus condimentum rhoncus faucibus eros volutpat. Donec sit amet tempus ante. Aenean a risus dui. Vivamus iaculis, augue at mollis blandit, mi lacus dapibus mauris, sit amet aliquam urna sapien sed nisl. Curabitur gravida semper elit, a pharetra ipsum cursus et. Proin lectus neque, auctor venenatis pharetra sed, dignissim ac urna. Nulla sed erat lorem, eget mollis sapien. In viverra nunc sed risus laoreet id convallis quam dapibus. Nulla gravida, leo ut volutpat porta, lorem lorem commodo sem, id dapibus magna mauris quis magna."

Ejercicio 14:

A partir del mismo fichero del ejercicio 13, implementar la técnica del espectro, obtener el espectro y aplicar los cambios en los coeficientes de la transformada de Fourier para insertar un mensaje repetidas veces.

Hay que decidir en qué frecuencias se ha de aplicar el cambio.

Mensaje: "mensaje que se va a ocultar en el fichero de audio"

Ejercicio 15:

Descargar la imagen que se encuentra en la siguiente dirección: `http://www.0xword.com/recursos/esteganografia/ej15.jpg`

¿Existe algún contenido oculto dentro de este archivo? ¿qué técnica se ha utilizado para ocultar el contenido?

Ejercicio 16:

Descargar la imagen audio que se encuentra en la siguiente dirección: `http://www.0xword.com/recursos/esteganografia/ej16.jpg`

Mediante la herramienta `enscribe` y el fichero descargado, crear un fichero de audio que mediante el cual después se pueda visualizar la imagen con la herramienta `baudline`.

Ejercicio 17:

¿Existe algún mensaje oculto en esta comunicación?
Crea, mediante la misma técnica y dos equipos informáticos conectados en una Intranet, una comunicación oculta entre ellos.
¿Cuánto se tardaría en enviar un documento de una página? ¿sería posible enviar un archivo binario o ejecutable?

```
21:43:54.835975 IP (tos 0x0, ttl 255, id 102, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x734b (correct),
seq 1269990416, win 65535, length 0
21:43:54.866128 IP (tos 0x0, ttl 255, id 101, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x5b3c (correct),
seq 2663129452, win 65535, length 0
21:43:54.882457 IP (tos 0x0, ttl 255, id 100, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x1bf0 (correct),
seq 2372760071, win 65535, length 0
21:43:54.898585 IP (tos 0x0, ttl 255, id 105, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x5e16 (correct),
seq 2114438752, win 65535, length 0
21:43:54.914391 IP (tos 0x0, ttl 255, id 99, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x5db1 (correct),
seq 326159723, win 65535, length 0
21:43:54.929801 IP (tos 0x0, ttl 255, id 105, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xa058 (correct),
seq 787309455, win 65535, length 0
21:43:54.945802 IP (tos 0x0, ttl 255, id 100, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x580e (correct),
seq 3265974906, win 65535, length 0
21:43:54.961691 IP (tos 0x0, ttl 255, id 97, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x26f4 (correct),
seq 2809469271, win 65535, length 0
21:43:54.977092 IP (tos 0x0, ttl 255, id 100, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x4b02 (correct),
seq 401651826, win 65535, length 0
21:43:54.993138 IP (tos 0x0, ttl 255, id 101, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x0590 (correct),
seq 1069218574, win 65535, length 0
21:43:55.009376 IP (tos 0x0, ttl 255, id 115, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xb63f (correct),
seq 2159797353, win 65535, length 0
21:43:55.024723 IP (tos 0x0, ttl 255, id 32, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xf493 (correct),
seq 1065871177, win 65535, length 0
21:43:55.040130 IP (tos 0x0, ttl 255, id 104, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x513b (correct),
seq 39867813, win 65535, length 0
21:43:55.055598 IP (tos 0x0, ttl 255, id 97, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xf197 (correct),
seq 2962367296, win 65535, length 0
21:43:55.071160 IP (tos 0x0, ttl 255, id 98, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x4b0c (correct),
seq 574402076, win 65535, length 0
21:43:55.086298 IP (tos 0x0, ttl 255, id 101, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x8d0b (correct),
seq 1656196401, win 65535, length 0
21:43:55.102767 IP (tos 0x0, ttl 255, id 105, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xb6e2 (correct),
seq 2016275796, win 65535, length 0
21:43:55.118247 IP (tos 0x0, ttl 255, id 115, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x3f41 (correct),
seq 83089200, win 65535, length 0
21:43:55.133672 IP (tos 0x0, ttl 255, id 32, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x160e (correct),
seq 1124944107, win 65535, length 0
21:43:55.149712 IP (tos 0x0, ttl 255, id 97, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x5f7e (correct),
seq 2411695036, win 65535, length 0
21:43:55.165431 IP (tos 0x0, ttl 255, id 99, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x6549 (correct),
seq 2263023579, win 65535, length 0
21:43:55.180712 IP (tos 0x0, ttl 255, id 97, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x1d63 (correct),
seq 2912833695, win 65535, length 0
21:43:55.196142 IP (tos 0x0, ttl 255, id 98, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xe57e (correct),
seq 1074226453, win 65535, length 0
21:43:55.211805 IP (tos 0x0, ttl 255, id 97, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x2799 (correct),
seq 2612028371, win 65535, length 0
21:43:55.227656 IP (tos 0x0, ttl 255, id 100, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x5e4f (correct),
seq 3706939910, win 65535, length 0
21:43:55.243269 IP (tos 0x0, ttl 255, id 111, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x56c5 (correct),
seq 3561812050, win 65535, length 0
21:43:55.264138 IP (tos 0x0, ttl 255, id 32, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xb5fb (correct),
seq 3137058341, win 65535, length 0
21:43:55.280174 IP (tos 0x0, ttl 255, id 101, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xcca33 (correct),
seq 3022232946, win 65535, length 0
21:43:55.296634 IP (tos 0x0, ttl 255, id 108, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xf2dd (correct),
seq 1444794985, win 65535, length 0
21:43:55.311058 IP (tos 0x0, ttl 255, id 32, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xdb2d (correct),
seq 2529470834, win 65535, length 0
21:43:55.326543 IP (tos 0x0, ttl 255, id 108, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x7ea9 (correct),
seq 2846683915, win 65535, length 0
21:43:55.341899 IP (tos 0x0, ttl 255, id 105, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xf0b8 (correct),
seq 3347145514, win 65535, length 0
21:43:55.357266 IP (tos 0x0, ttl 255, id 98, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0xdbe8 (correct),
seq 2603322182, win 65535, length 0
21:43:55.373299 IP (tos 0x0, ttl 255, id 114, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x9800 (correct),
seq 1828553346, win 65535, length 0
21:43:55.390835 IP (tos 0x0, ttl 255, id 111, offset 0, flags [none],
proto TCP (6), length 40)
    localhost.0 > 192.168.84.132.http: Flags [S], cksum 0x7ae5 (correct),
seq 3221345477, win 65535, length 0
```