Departamento de Lenguajes y Sistemas Informáticos
E.T.S. Ingeniería Informática. Universidad de Sevilla

Avda Reina Mercedes s/n. 41012 Sevilla
Tlf/Fax 954 557 139 **E-mail** lsi@lsi.us.es **Web** www.lsi.us.es

E.T.S. ingeniería informática

SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

CAI 2. CONSULTA SOBRE LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN UNA ENTIDAD HOSPITALARIA (Parte 2)

Debido a que se han detectado incidencias en determinadas radiografías, el Hospital desea añadir una firma oculta en cada una de las radiografías que se realicen. En está consultoría se pide valorar la **esteganografía** como técnica para dar una solución a este problema, ya que consiste en la ocultación de la información sobre un objeto (imagen, sonido, video, …). El Hospital nos comunica que se puede usar cualquier herramienta que considere oportuna el equipo Consultor para el estudio que a continuación nos propone. De acuerdo con ello, se pide:

Apartado a). Estudio del método LSB. La entidad hospitalaria nos pide un estudio sobre la idoneidad del método LSB para ocultar la firma en las imágenes (preferiblemente bmp). Nos entregan **los criterios de decisión** a tener en cuenta en la consultoría. **El tamaño de las firmas a ocultar está entre 128 y 512 caracteres**:

1. **Tamaño:** Tamaño que debe tener la imagen original para que la firma quede oculta (sin tener que aumentar el tamaño de la imagen original).
2. **Confidencialidad:** Imposibilidad de detectar y/o decodificar las firmas añadidas. ¿Qué medidas se pueden tomar para mejorar la confidencialidad?.
3. **Robustez:** Representa la cantidad de distorsiones que el estego objeto (imagen) puede soportar antes que se pierda la información oculta y no se perciba que existe texto embebido en el estego objeto. Se podrían probar dos tipos de distorsiones, como por ejemplo introducir 4 órdenes de distorsión para Salt-Pepper encadenadas, o distorsión Crop para anchos y altos (W/H) diferentes. ¿Qué se puede hacer para mejorar los resultados ante cada una de las distorsiones aplicadas?

Esta **tarea exige experimentación,** se deben presentar los resultados obtenidos en las pruebas de distorsión (Robustez).

Apartado b). La dirección del Hospital tiene sospechas de que un Jefe de Servicio está enviando información confidencial de la misma a terceras personas ajenas a la entidad hospitalaria, de forma codificada utilizando quizás algún método relacionado con la esteganografía. Hemos recibido una de las imágenes enviadas sobre la que se cree existe información confidencial oculta. Se quiere determinar si existe un mensaje oculto detrás de esta imagen, y extraerlo si es posible. Primero debe realizarse el estegoanálisis (detectar si hay información oculta) pudiendo utilizar cualquier herramienta que estime oportuna (se valorará con mayor satisfacción si se utiliza alguna herramienta diferente a VSL para hacer el estegoanálisis). Se debe presentar en el informe dicho análisis y el resultado obtenido del mismo. En segundo lugar, se debe presentar el proceso seguido para extraer dicho mensaje si es que existe (puede usar cualquier herramienta).

Apartado c). También nos consultan sobre la posible pérdida de información en uno de los ordenadores que ha sido sustraído del Hospital. Para la firma automatizada de documentos

internos, se tenían almacenadas en dicho ordenador imágenes de tipo BMP, que contienen las firmas escaneadas de los médicos, su nombre y NIF. Dichas imágenes están cifradas con el algoritmo AES mediante una aplicación que utiliza una clave de 32 dígitos/letras/símbolos totalmente aleatorios (256 bits), y las claves no estaban almacenadas en el ordenador. En el momento de la sustracción sólo dos ficheros estaban descifrados y el resto estaban cifrados. Se adjunta los dos ficheros descifrados y uno cifrado. Nos consultan si podemos estar tranquilos que la información almacenada en las imágenes cifradas no será accesible por nadie dadas las medidas de seguridad tomadas. ¿Se pueden tomar más medidas para proteger mejor la información guardada en las imágenes cifradas? La empresa valorará la justificación de la respuesta.

Normas del entregable

- Cada ***Security Team X*** debe entregar el informe ST-X-CAI2-ParteB.pdf que contenga todos los detalles que responden a los puntos de la consultoría (se debe indicar expresamente los alumnos del equipo que han participado en el trabajo) a través de la actividad creada al efecto en el curso de Enseñanza Virtual. El informe debe recoger evidencias del proceso, pruebas realizadas, así como de las respuestas a las consultas planteadas.
- La consulta se desarrollará en la sesión dispuesta al efecto, y en el tiempo indicado por el profesor.