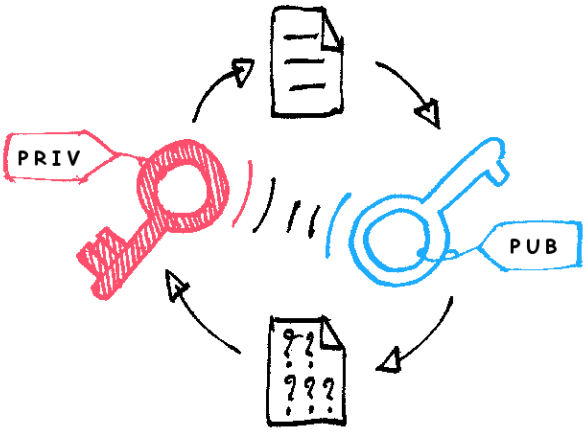
Trabajo Práctico Especial

Criptografía y Seguridad

ITBA

Instituto Tecnológico de Buenos Aires



Gastón Lifschitz - 58225

Bautista Blacker - 57129

Juan Bensadon - 57193

Cuestiones a analizar

1. **Discutir los siguientes aspectos relativos al documento**.
    a. **Organización formal del documento (¿es adecuada? ¿es confusa?)**

    En nuestra opinión, la organización formal del documento es bastante adecuada, pero se nos ocurren ciertos puntos donde podría mejorarse:

        i. Si bien las secciones se encuentran delimitadas por títulos adecuados ("Introducción", "Esquema propuesto de imagen secreta compartida", "Resultados experimentales", "Conclusiones", "Agradecimientos" y "Referencias"), creemos que el documento se vería beneficiado por una división interna de cada sección utilizando subtítulos. La introducción, por ejemplo, podría separarse en "Problema", "Soluciones existentes" (Pudiendo esta parte ser subdividida para distinguir la descripción de las distintas soluciones), "Soluciones EISC" (Con subtítulo para EISC basados en AC y EISC basados en C-ESCV), y "Propuesta de solución EISC". Creemos que el uso de subtítulos a lo largo del documento facilita la lectura y la búsqueda de información en el mismo.

        ii. Además, el documento tiene varios errores de tipeo, como por ejemplo "de las cuales conllevana la divulgación dela misma.Sin embargo", o "en la etapa de decodificación al menos k piezas de lasn son requeridas". Si bien no es un problema mayor, corregirlos facilitaría la lectura y le daría más profesionalidad al documento.

    b. **La descripción del algoritmo de distribución y la del algoritmo de recuperación. (¿es clara? ¿es confusa? ¿es detallada? ¿es completa?)**

        i. La descripción del algoritmo de distribución y recuperación es clara. La descripción inicial de alto nivel de ambas partes del proceso es muy útil, ya que al entrar en detalle de etapas de codificación y decodificación, el documento es muy técnico y detallado en la notación y definición matemática de los procesos, lo cual hace fácil perder de vista el proceso integrado. El detalle de ambos procesos en conjunto con la descripción inicial nos dio una visión completa del sistema.

        ii. En cuanto a los diagramas, algunos fueron útiles (ej. Fig. 2), pero otros no ayudaron demasiado a entender el sistema (ej, Fig 1), sino que son simplemente una repetición de lo escrito en el texto sin aprovechar el medio visual para aclarar ideas.

        iii. En la sección de recuperación del secreto, la relación entre la Interpolación de Lagrange y el algoritmo planteado para aplicarla y obtener el secreto no está clarificada, lo cual es bastante confuso sin

un análisis previo de dicho algoritmo y su relación a las fórmulas de Lagrange.

c. **La notación utilizada, ¿es clara? ¿cambia a lo largo del documento? ¿hay algún error?**

No encontramos ningún error en la notación, y de hecho la minuciosidad del documento nos ayudó a entender el proceso con confianza. Tampoco encontramos ninguna inconsistencia en la notación en el documento. Al referenciar a datos extraídos de una imagen durante el proceso de descodificación, por ejemplo, se utilizó notación distiguiéndolos de los datos manipulados durante la codificación (por ejemplo Tij vs T'ij)

2. **El título del documento hace referencia a que optimiza la carga útil ¿a qué se refiere? ¿Qué relación existe entre k y el tamaño de la portadora?**

La optimización de la carga útil hace referencia a que en este modelo el maximo de carga util que va a tener una portadora viene determinada por la imagen secreta. De está manera el nivel de distorsión de las portadoras en relación a la cantidad de datos que se ocultarán en ellas va a ser más bajo. Si k es mayor o igual que 4, la máxima carga útil de los datos secretos puede ser tan grande como el tamaño de la imagen camuflaje, lo cual permite una eficiente y secreta transmisión de los datos.

Cabe aclarar, la carga util viene dado por las caracteristicas de la imagen portadora y el k, de manera tal que su relacion se determina de la siguiente manera

$$Payload(byte) = \frac{NPixeles\ x\ Ncolor\ x\ 4}{4}$$

3. **¿Qué ventajas y qué desventajas ofrece trabajar en $GF(2^8)$ respecto de trabajar con congruencias módulo?**

La principal ventaja de trabajar con $GF(2^8)$respecto de trabajar con congruencias módulo, es que la imagen revelada se puede obtener sin pérdidas ya que, trabajando sobre bytes, podemos asegurarnos de que los valores se mantendrán entre 0 y 255. Está ventaja es la que hace posible que la comunicacion sea más fiable que la convencional basadas en tecnicas esteganograficas combinadas con algoritmos criptograficos, ya que el esquema propuesto es un esquma de secreto compartido, donde un minimo de k imagenes camuflaje son requeridas para revelar el secreto.

Por otro lado, la principal desventaja está en la performance del algoritmo, ya que la congruencia módulo numérica es mucho más performante que la congruencia módulo en un campo de Galois.

4. **¿Se puede trabajar con otro polinomio generador? ¿podría guardarse como "clave"?**

   Sí, se puede siempre que dicho polinomio sea un polinomio irreducible en el campo de Galois en que se esté trabajando. Ahora bien, este polinomio no podría usarse como "clave", ya que sus coeficientes no necesariamente se requieren para la etapa de recuperación (por lo que no protegerían los datos).

5. **Según el documento se pueden guardar secretos de todo tipo (imágenes, pdf, ejecutables). ¿por qué? (relacionarlo con la pregunta 3)**

   Al no haber pérdida de datos, se pueden ocultar datos en formatos que requieran integridad total. Si hay pérdida de información en una imagen, la imagen puede seguir siendo visible y útil, mientras que la pérdida de información en un ejecutable probablemente rompa toda la lógica del programa que ejecuta**.**

6. **¿Cómo podría adaptarse la implementación realizada para poder guardar un archivo de imagen completo?**

   Al ser el encabezado un conjunto de bytes al igual que los píxeles, se podría tomar toda la imagen completa junto con el encabezado, y hacer la misma división en bloques de L/k bytes, donde L es la longitud del encabezado sumada a la longitud de los píxeles.

7. **Analizar cómo resultaría el algoritmo si se usaran imágenes en color (24 bits por píxel)**

   Si se usaran imágenes a color, se dividirán las imágenes camuflaje de la misma manera (en grupos de 4 bytes), y el algoritmo funciona igual. La distorsión sobre las imágenes camuflaje sería menor, ya que la información de cada píxel se encuentra distribuida entre 3 bytes en lugar de uno solo, y por lo tanto, la información se vería modificada en menor medida.

8. **¿Se podrían tomar los bloques de otra manera, en lugar de como matrices 2x2? Explicar.**

   No es absolutamente necesario que se trate de bloques cuadrados 2x2. Mientras que los píxeles se agrupen de a 4, la disposición/distribución de los píxeles del grupo puede ser cualquiera, siempre que el algoritmo de encripción y desencripción coincidan. En cuanto a la cantidad de píxeles por bloque, sabemos que con 4 píxeles y la forma de distribuir la información entre ellos detallada en el paper, la distorsión sobre la imagen es mínima. Matemáticamente, se podría distribuir el resultado de F(X) sobre hasta 8 píxeles distintos (teniendo así grupos de 9 píxeles), pero esto permitiría ocultar menos cantidad de pares (x, F(x)) en una imagen.

9. **Discutir los siguientes aspectos relativos al algoritmo implementado:**
    a. **Facilidad de implementación**: la mayor dificultad encontrada a la hora de implementar el algoritmo fue en la realización de operaciones algebraicas mediante código. Una vez logrado esto, el resto de la implementación fue relativamente simple y rápida.

    b. **Posibilidad de extender el algoritmo o modificarlo**: En nuestro caso, el código está bastante orientado al ocultamiento de imágenes, y más específicamente de imágenes en formato BMP, pero no sería un problema mayor modificar el código para trabajar con secuencias de bytes arbitrarias.

10. **¿En qué situaciones aplicarían este tipo de algoritmos?**

    Este algoritmo es muy útil en cualquier situación donde se requiera que ninguna parte tenga la información completa, pero que al haber un cierto quórum, se pueda obtener la información. Por ejemplo, si se quisiera requerir el aval de múltiples dirigentes de un grupo financiero para poder realizar transferencias, pero no necesariamente de todos (porque la coordinación constante entre los miembros sería mucho trabajo).

Recuperación de imágenes

Imágenes entregadas por la cátedra:

Imagen recuperada: