Criptografía y Seguridad

Secreto compartido con esteganografía

Integrantes del grupo:

57240 Terenziani, Santiago

57700 Picasso, Sofía

58367 Sampedro, Ignacio

Preguntas para Analizar:

1. **Discutir los siguientes aspectos relativos al documento** (“Sistema de Imagen Secreta Compartida con Optimización de la Carga Útil”).
    a. **Organización formal del documento**

        El documento se encuentra correctamente organizado en sectores de forma ordenada (Resumen, Introducción, Esquema Propuesto, Resultados Experimentales, Conclusiones).

        Algún par de imágenes, como las figuras 5 y 6 respectivamente, podrían obviarse, ya que no aportan a la explicación. Aunque sean ejemplos del uso del algoritmo, a plena vista simplemente son imágenes sin cambio alguno (ya que ese es el punto del sistema).

    b. **La descripción del algoritmo de distribución y la del algoritmo de recuperación.**

        Se encontraron problemas especialmente en la parte donde se describe el algoritmo de recuperación. Esto se debe a la notación confusa que describe a la hora de implementar la interpolación de Lagrange. Las fórmulas presentadas eran difíciles de entender e incluso parecían faltarles partes o símbolos. Sin embargo, esta situación fue superada fácilmente ya que se encuentran varios recursos por fuera del paper que explican la interpolación de Lagrange de forma más sencilla y clara.

    c. **La notación utilizada**

        Como se dijo en la pregunta anterior, la notación de las fórmulas para realizar el algoritmo de recuperación se consideró confusa y posiblemente errónea.

2. **El título del documento hace referencia a que optimiza la carga útil**
    a. **¿A qué se refiere?**

        Se refiere a que el sistema propuesto presenta una mayor carga útil comparado con los resultados de otros métodos propuestos previamente (La calidad de las imágenes camuflaje es mayor que en los algoritmos convencionales cuando la misma cantidad de datos secretos es compartida).
    b. **¿Qué relación existe entre k y el tamaño de la portadora?**

        El valor k controla la carga útil de datos secretos (es decir, es la mínima cantidad de sombras requeridas para poder recuperar el secreto). El que afecta al tamaño de las imágenes portadoras ya que mientras más grande es k, menos bytes necesito de cover. Con k=4 específicamente nos da que el tamaño de la imagen secreta debe ser igual al de las portadoras.

        Por esta razón necesitamos tomar imágenes de igual tamaño en pixeles que el secreto, y así poder recuperar el secreto en los encabezados de las mismas.

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

    Ventajas:
    - La operación GF(2^8) garantiza una recuperación sin pérdida de los datos secretos y una alta calidad de las imágenes camuflaje.
    - Está mejor dividido en bytes.
    - Se toma el valor $2^8 = 256$ debido a los valores posibles que un píxel puede tomar (de 0 a 255), lo cual es ideal al trabajar con imágenes.

    Desventajas:
    - Menos intuitivo que el sistema de aritmética infinita al que acostumbramos.
    - Se deben programar todas las operaciones para que se mantengan dentro del campo de Galois.

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

    Sí. El polinomio generador del campo de Galois 2^n debe ser un polinomio irreducible de grado n, con número impar de términos y por lo menos una constante. Para este caso, podríamos tomar $x^8 + x^4 + x^3 + x^2 + 1$.

    Se lo puede considerar una clave ya que define el funcionamiento del algoritmo y el resultado de las operaciones que realiza.

5. **¿Por qué se pueden guardar secretos de todo tipo?**

Porque las operaciones en GF(2^8), contribuyen a una recuperación sin pérdida de los datos secretos, garantizando que no se pierdan bits de información en el proceso de encripción, y esta se verá de forma correcta.

Si bien el programa desarrollado está enfocado en imágenes de un formato específico, podría generalizarse para emplear el algoritmo en la encripción de cualquier tipo de archivo, ya que trabaja sobre valores byte a byte, que en este caso, representaba un píxel cada uno y facilitaba el seguimiento del proceso.

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

Ya que es posible calcular el tamaño del encabezado, podríamos extraer los datos relevantes y proceder haciendo de cuenta que el binario de todo el archivo es el contenido de la imagen. De esta forma, necesitaríamos sombras de mayor tamaño que el secreto, capaces de almacenar todos los bytes a encriptar y permitir calcular la cantidad de bytes escondidos.

Para recuperar el secreto, simplemente pasaríamos los bytes extraídos a un nuevo archivo, y esta vez no deberíamos agregar anteriormente ningún header, ya que estarán incluídos en los bytes recuperados.

7. **Analizar cómo resultaría el algoritmo si se usaran imágenes en color.**

El algoritmo se usaría de una forma similar, considerando en este caso que se cuenta con tres canales de color distintivos (RGB) y que por lo tanto se necesitarán el triple de bits por pixel (es decir, 24 bits por píxel) para lograr representar la imagen.

Esto puede presentar ciertas dificultades, especialmente en cuanto al tiempo de ejecución del algoritmo, al tener que trabajar con más datos.

Sin embargo, también presenta una mejora a la calidad del sistema, ya que al tener una variedad más grande de colores e intensidades, tenemos también una mayor capacidad de ocultamiento.

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

Mientras se respete la distribución de los bloques en el proceso de encripción y desencripción, los bloques podrían tomarse de cualquier manera, siempre y cuando abarquen toda la información a ocultar.

En el desarrollo del trabajo práctico se optó por rechazar imágenes con una cantidad impar de filas de píxeles, ya que no permitirían seguir el diseño 2x2. Sin embargo, los bloques podrían ser de 1x4, permitiendo así obtener 4 bytes que formen el bloque XWVU sin importar la paridad de las filas. Como beneficio adicional, en este caso no habría conflicto sobre el ancho de la imagen, pues en el binario el ancho es redondeado al próximo múltiplo de 4 y rellenado con información nula.

9. **Discutir los siguientes aspectos relativos al algoritmo implementado**:

   a. **Facilidad de implementación**

      La mayor dificultad a la hora de implementar el algoritmo es comprender la lógica detrás del mismo, ya que puede resultar compleja a primera vista. Sin embargo, una vez que se logra entender cómo funciona el mismo, no es difícil de implementar.

      También facilita su implementación el hecho de que pueda ser dividido en distintos subproblemas (las operaciones en el campo de Galois, el interpolador de Lagrange, etc) para testearlo con mayor facilidad y luego acoplar las partes.

   b. **Posibilidad de extender el algoritmo o modificarlo**

      Gracias a dicha modularización del programa, el algoritmo presenta una gran variedad de posibles modificaciones que podrían permitir extender el mismo. Entre ellos se encuentran la posibilidad de utilizar el algoritmo en imágenes en color (lo cual se detalló previamente).

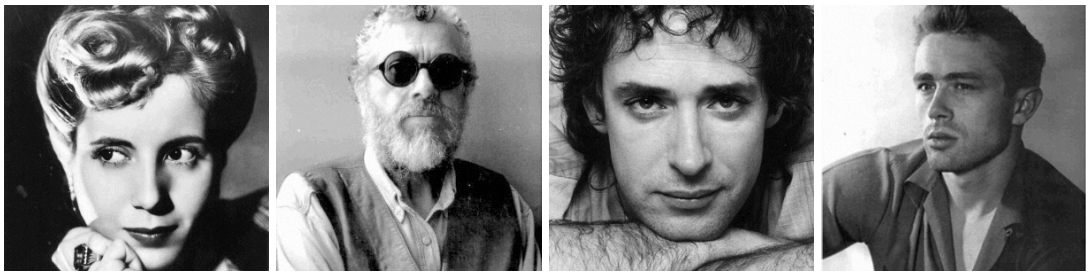
10. ¿En qué situaciones aplicarían este tipo de algoritmos?

Para una aplicación de mensajería, por ejemplo, donde se envían y reciben mensajes 2 o más personas, serviría para encriptar y autenticar mensajes entre las partes.

El beneficio principal del sistema es que no se requieren recuperar todos las sombras para poder desencriptar la imagen, mientras se tenga acceso a k de ellas el sistema continúa funcionando sin problemas.

Existen proyectos como Vanish (un proyecto que utiliza tecnología P2P para darle al usuario la decisión de cuánto tiempo quiere que el contenido que pone en la red perdure), que se aprovecha de la idea detrás de este algoritmo para romper la llave de desencriptación en componentes más pequeños y distribuirlos en tablas hash. Mientras k tablas sean accesibles, es posible desencriptar el mensaje. Sin embargo, las tablas van eliminando la información hasta que menos de la cantidad de sombras necesarias para recuperar el secreto se encuentran disponibles, en cuyo punto se considera perdido para siempre.

Imágenes Camuflaje:



Secreto Recuperado: