Secreto compartido en Imágenes con Esteganografía

Nicolas Bombau
Lucas Pizzagalli
Nicolas Purita

1- La imagen recuperada, es prácticamente igual a la imagen original, con exepción de algunos bytes en la extrema derecha que no son codificados cuando el ancho de la foto no es divisible por k. Por otro lado, los pixels que tienen un valor mayor al de 250, son codificados como el modulo de dicho numero y 251, por lo que visualmente se pueden observar pixels que deberían ser blancos, de color negro. Esto se debe a que la ecuación usada durante el proceso de distribución es:

$$(x_1 a_1 + \cdots + x_k a_k) \bmod 251 \equiv b$$

Durante el proceso de recupero la solución del sistema lineal de congruencias podría no ser única. Sin embargo la utilización de 251, que es el numero primo mas grande y menor que 256, como módulo asegura que la solución al sistema no sea ambigua (hay una única solución).

2- En el método original de secreto compartido de Blakley se descartan aquellas sombras que tengan ceros pues la inclusión de las misma puede provocar que el sistema resulte incompatible, dando lugar a la existencia de infinitas soluciones. De producirse esto último se obtendrían infinitos puntos y sería imposible recuperar el secreto.
El método propuesto por Ulutas et al. las n ecuaciones pueden ser levemente modificadas para que dado cualquier subconjuntos de k ecuaciones, estas resulten linealmente independientes. Es decir que el sistema quedará compatible determinado para cualquier conjunto de k ecuaciones. Se habla de una leve modificación, ya que idealmente la modificación deberá modificar lo menos posible las sombras.
Es por lo expuesto en el párrafo anterior que Ulutas y sus colegas no se ven obligados a descartar las sombras que tengan ceros.

3-

a. El documento “Improvements in Geometry-Based Secret Image Sharing Approach with Steganography” presenta el algoritmo propuesto de forma clara y ordenada.
   Empieza haciendo una breve introducción de los distintos esquemas de secreto compartido y de algunas implementaciones, basadas en estos métodos, enfocadas en compartir secretos donde el secreto es una imagen. Esta introducción es importante, no sólo para contextualizar el trabajo, si no para luego realizar comparaciones, entre los distintos métodos ya existentes y el propuesto, en la sección de resultados.
   En el segundo apartado, se hace una breve descripción del método de Shamir que resulta importante pues el algoritmo propuesto se basa en este último.
   La tercer sección, explica detalladamente el algoritmo, distinguiendo claramente el proceso de distribución y el reconstruccion.
   En el penúltimo apartado, se presentan los resultados experimentales de utilizar distintos métodos y se realiza el contraste de los mismos.
   Finalmente, la sección de conclusiones, explica las ventajas de usar el método propuesto basándose en los resultados obtenidos en la sección anterior.
b. El paso 7 del algoritmo de reconstrucción propone resolver el sistema lineal de congruencias computando la matriz inversa del sistema y resolviendo X=A^-1B. En nuestra implementación usamos el método de Gauss no para buscar la matriz inversa, si no para obtener el transformar el sistema en un sistema triangular superior y así obtener los valores las incógnitas del vector **X**.
c. La notación es clara y consistente a lo largo de todo el documento. Aunque las ecuaciones (3.2), (3.3) y (3.4) requieren especial atención para su correcta comprensión.

4-

a. En líneas generales el algoritmo a primera vista no presenta mayores dificultades para

ser entendido. Pero como se explica en el punto 5 varias cuestiones han dificultado considerablemente su implementación y prueba.

b. El paper de Ulutas et al. especifica claramente que el algoritmo puede ser fácilmente extendido para ser utilizado con imágenes en color, solo hace falta modificar el módulo de las operaciones.
c. El algoritmo de Shamir presenta ciertas desventajas frente al propuesto por Ulutas et al.
   El algoritmo de Shamir requiere la utilización de imágenes de 2Nx2N para ocultar una imagen de NxN. Ulutas et al. proponen un algoritmo que requiere imágenes del mismo tamaño que la imagen que se desea ocultar, logrando reducir el espacio necesario para almacenamiento como la cantidad de ancho de banda consumido al transferir las sombras.
   Otra ventaja muy importante es que el algoritmo de Ulutas et al. permite la generación de sombras con significado a diferencia de Shamir en cuyas sombras es preponderante el ruido. Es importante la generación de sombras con poco ruido ya que pueden atraer la atención de un atacante.

5- El documento no presenta mayores dificultades a la hora de ser leído. Sin embargo la implementación puede resultar problemática. El uso de operaciones de manejo de bits es propenso a errores. La mantenibilidad y testeo resultan dificultosos.
La generación del conjunto de ecuaciones linealmente independientes ha presentado un reto importante. Consumiendo varias horas de programación.
Otra dificultad importante, fue la falta de especificación sobre cómo debe manejarse las imágenes.Por ejemplo, mientras la cátedra decidió tomar las líneas separadamente, y codificar las imágenes hasta que la cantidad de pixels de dichas filas sean menores a k. Por otro lado, nuestro primer enfoque codificaba la imagen utilizando las filas como una gran fila, osea, que si al codificar una fila, se llegaba al final y sobraban bytes, los mismos eran codificados con los primeros bytes de la fila siguiente.Esto lograba una codificación de prácticamente el 100% de la imagen, sin embargo, no era compatible con los archivos de testeo por lo que se decidió cambiar al mismo método utilizado en dichas imágenes. Esta incompatibilidad de metodologías, se deben a que en los papers no se detalla que decisión se debe tomar, dejando la decisión libre al programador.

6- La primera modificación, sería tener en cuenta cuando los pixels de las imágenes son mayores al primo que se utilizará para realizar el módulo. De esta forma, normalizar las imágenes para que dichos valores no ocurran y no tener los problemas presentes en el actual algoritmo que transforma valores que deben ser blancos (cercanos al 0xFF) a negro (0x00 o muy cercanos al mismo).
Sería interesante introducir una modificación al algoritmo que permita trabajar con imágenes en color.
Una posible extensión de la presente aplicación es la posibilidad de utilizar valores para n y k que excedan los límites impuestos por el enunciado. Aumentando así la cantidad de sombras que se pueden generar como también aumentando el valor de umbral necesario para recuperar el secreto.

7- Este tipo de algoritmos resulta especialmente útil para proteger un secreto y no tener que preocuparse por la seguridad de la clave. Almacenar una clave en un solo lugar resulta altamente riesgoso y realizar múltiples copias de la misma solo aumenta la brecha de seguridad.
Estos algoritmos tienen la particularidad que el secreto es dividido en n partes (capacidades o sombras) y sólo podrá ser recuperado si se presentan k partes cualesquiera (k<=n). Si se presentan l partes tal que l < k el secreto no podrá ser recuperado.

Sin un atacante tiene acceso a alguna de las sombras, no podrá recuperar el secreto. Deberá obtener las k sobras necesarias.
Como conclusión podemos decir que el uso de criptografía de umbral resulta muy útil si se desea que varias personas actúen como custodios de un secreto y no darle a una sola persona toda la responsabilidad sobre el mismo. Además se puede ver como la pérdida o daño de alguna de las sombras o la traición por parte de una de las personas no da lugar a la pérdida de confidencialidad del secreto.

Secretos escondidos en las imágenes:

Imagen escondida en 2 imagenes (v2).

Secreto ocultado en 3 imagenes (v2).

imagen escondida en 4 imagenes (v2)