TRABAJO PRÁCTICO DE IMPLEMENTACIÓN

Secreto compartido en imágenes con esteganografía

Asignatura: Criptografía y Seguridad

Profesores: Abad, Pablo Eduardo
Ramele, Rodrigo Ezequiel
Arias Roig, Ana Maria

Alumnos: Azarola, Ivana Martina
Dantur, Juan Pablo
Rivas, Leandro Matias

Fecha de entrega: 29 de junio de 2017

Índice

Introducción

La idea básica de secreto compartido es transformar una imagen en n imágenes sombra que puedan transmitirse y almacenarse por separado. La imagen original puede ser reconstruida solo si las imágenes sombra que participan en el proceso para revelarlo forman un conjunto adecuado. Para evitar un simple point of failure, se desarrolló el umbral(r,n) image sharing scheme.

En este esquema, la imagen original solamente puede ser revelada si se obtienen r o más sombras, pero teniendo r -1 o menos no podrá revelarse.

Thien y Lin propusieron un Secret Image Sharing (SIS) Scheme en base al umbral(r,n). El tamaño de las imágenes sombra generadas son de 1/r respecto a la original, lo que facilita al almacenamiento y transmisión de ellas.

Luego, como indica el paper sugerido por la cátedra, Kuang-Shyr Wu y Tsung-Ming mejoraron la idea de Shamir, cambiando el valor del número primo a 257.

The Shamir (r, n) Secret Image Sharing Scheme

Shamir desarrolló tomando los valores r y n como 2 <= r <= n, siendo r el número de imágenes sombra. El secreto puede obtenerse juntando r de n sombras.

$$f(x) = (a_0 + a_1 x + a_2 x^2 + \ldots + a_{r-1} x^{r-1}) \bmod p, \quad (1)$$

donde P es un número primo, a0 es el secreto y los restantes coeficientes son valores random enteros pertenecientes al intervalo [0 P-1].

Para cada secret data, un secret share es un par (xi,yi) donde

$$y_i = f(x_i),\ 1 \le i \le n,\ \text{and}\ 0 < x_1 < x_2 < \ldots < x_n < p. \quad (2)$$

De acuerdo a las Eq.1 y Eq.2, si adquirimos r o más pares del total de n, entonces al menos r ecuaciones yi=f(xi) pueden obtenerse y descubrir el secreto a0.
Por otra parte, el secreto también puede obtenerse utilizando la interpolación de Lagrange.

The Thien-Lin(r, n) Secret Image Sharing Scheme

Thien y Lin extendieron la idea de Shamir y propusieron un esquema SIS basado en un umbral(r, n) que genera la imagen sombra de tamano 1/r respecto a la imagen secreta.

Las operaciones aritméticas son evaluadas con el número primo 251. Dado que las imágenes el rango para una intensidad de color se representa en el intervalo que va de 0 a 255 es necesario truncar valores en esta implementación de secreto compartido. Como consecuencia de esto, Thien y Lin proponen truncar los valores de píxeles mayor de 250, generandose una pérdida de la información original, obteniéndose al recuperar la imagen una de menor calidad en cuanto a la original.

Otro aspecto interesante que presenta el algoritmo de Thien y Lin es que aplica una permutación sobre la imagen original para ocultar la correlación entre píxeles vecinos.

Los pasos necesarios para ocultar una imagen en imágenes portadoras y recuperarla de sus respectivas imágenes sombras según el algoritmo de Thien y Lin se encuentran descritos en por Kuang-Shyr Wu y Tsung-Ming en su paper.

The Kuang-Shyr Wu y Tsung-Ming (r, n) Secret Image Sharing Scheme

Kuang-Shyr Wu y Tsung-Ming introducen las siguientes modificaciones al algoritmo propuesto por Thien y Lin:

Se utiliza el número primo 257 en lugar de 251.

Como consecuencia de este cambio se presenta el inconveniente de que el término independiente en el polinomio de la Ec. 1 puede valer 256, un número fuera del rango de colores representables que va de 0 a 255.

El método propuesto por los autores tiene los siguientes beneficios:

- Utilizando el número primo 257, el truncamiento ya no es necesario.
- El único inconveniente del método de Thien-Lin es que las imágenes con luz podrían no ser aplicables por el truncamiento. Este método propuesto puede superar este inconveniente.

Técnicamente hablando, la principal diferencia entre el método propuesto y Thein-Lins es que utiliza el primo 257 en lugar de 251.

Para ocultar una imagen en imágenes portadoras y recuperarla de sus respectivas imágenes sombras se realizan los pasos descritos por Kuang-Shyr Wu y Tsung-Ming en su paper.

Análisis

La imagen recuperada

Al ejecutar el algoritmo se notó que la imagen recuperada es ligeramente distinta a la imagen original ocultada (sin tomar en cuenta los headers). Esto se debe a que en los casos en donde f(x) = 256, se debe modificar el valor de los coeficientes, y eso modifica ligeramente algunos pixeles en la imagen.

La elección de imágenes portadoras

Como se observa en el paper de Kuang-Shyr Wu y Tsung-Ming el recupero de una imagen secreta se realiza mediante el procesamiento de los pixeles de las sombras. Las sombras no guardan las dimensiones del tamaño de la imagen secreta, solamente la cantidad de pixeles de la misma. De esta forma es imposible definir si se trata de una imagen con 1000 pixeles si se trata de una imagen de 25 x 40 o de 100 x 10.

Debido a esto de necesario establecer una precondición que el ancho de las imágenes portadoras sea igual al ancho de la imagen a ocultar, y que el cociente entre la altura de las mismas y la altura de la imagen a ocultar fuera 8/k. Nótese que para el caso de k igual a 8 la altura de las imágenes portadoras y la imagen secreta deben ser iguales.

Criterio utilizado para ocultar el secreto

Para las imágenes de las sombras se establecieron algunas condiciones:

- las dimensiones deben ser las mismas entre todas las sombras utilizadas,
- todas las sombras deben tener la misma semilla
- los identificadores de las sombras no pueden repetirse, ya que se trataría de una sombra repetida y no de distintas sombras
- todos los identificadores son mayores a cero.

A partir de las dimensiones de las imágenes de las sombras se determina el tamaño de la imagen secreta. A la imagen secreta se le asigna el mismo ancho que el de las imágenes de las sombras y la altura de la misma se calcula como la altura de las imágenes de las sombras multiplicada por k/8.

Nótese que con las imágenes descriptas en este apartado y en el anterior puede tomarse una imagen secreta y un conjunto de imágenes portadoras, generarse un conjunto de sombras y decodificar las mismas obteniendo una imagen muy similar a la imagen “secreta” original.

Facilidad del algoritmo implementado

El algoritmo se destaca por el uso de operaciones y pasos sencillos.

La principal ventaja de este algoritmo en cuanto a su implementación es que posee un único aspecto conflictivo por el uso de módulo 257 que se produce al generar las sombras si la evaluación el término independiente del polinomio es igual a 256.

Dado que los colores solo pueden representarse en el intervalo que va de 0 a 255, los autores proponen como solución a este caso en particular el decremento en una unidad del término independiente. A continuación deben volver a generarse los pixeles correspondientes a las sombras para ese paso.

Extensiones del algoritmo a imágenes color

El algoritmo de de Kuang-Shyr Wu y Tsung-Ming puede extenderse a imágenes color de distintas formas. Si se toman imágenes RGB, puede aplicarse el algoritmo por bandas o bien por tomando k elementos que incluyera colores de las tres bandas a la vez.

Sobre la implementación

Si bien no hubo dificultad para implementar el método que genera el polinomio para distribuir una imagen secreta en las imágenes portadoras, la recuperación del secreto requiere resolver sistemas de ecuaciones con aritmética modular y eso fue más complicado. Para esto se utilizó una implementación del método de eliminación de Gauss-Jordan para la aritmética modular[1].

Otro aspecto que revistió gran complejidad fue el uso de imágenes BMP. La dificultad asociada al uso de estas imágenes se encontró principalmente en la lectura y escritura del encabezado de las mismas.

Por cuestiones de simplicidad para realizar las pruebas del código si no se indica un directorio se requiere de una carpeta “resources” donde se buscan los archivos deseados. Esto permite diferenciar claramente cuáles son los archivos que se genera con una corrida del algoritmo y cuales son los preexistentes.

Uso de este tipo de algoritmos

El uso de algoritmos de secreto compartido permite otorgar a distintos entes una porción del secreto en mayor o en menor medida. Si todos poseen menos partes de las necesarias para obtener el secreto, se garantiza que se requiera la reunión de tantos entes como sea necesarios para obtener el mínimo de sombras requerido para la recuperación del secreto.

Adicionalmente se destaca que si se pierde o un atacante se hace de una sombra o de varias, siempre que no tenga el mínimo de sombras requerido para la recuperación del secreto, el mismo se permanece secreto.

Aplicación de algoritmos de este tipo puede ser la administración de recursos dentro de una organización donde para dar el acceso a documentación de tipo sensible se le requiera a los gerentes acumular un cierto número de sombras para acceder a ciertos recursos. La asignación de una o más sombras por gerente podría llevar a escenarios donde:

- un individuo puede acceder siempre al secreto, y otros para poder acceder al mismo deben asociarse a otros individuos,
- todos los individuos deben asociarse a otros para acceder al secreto,

[1] https://www.nayuki.io/page/gauss-jordan-elimination-over-any-field

- el mínimo de sombras requerido para la recuperación del secreto es el número de sombras totales generadas y si alguna se pierde, el secreto también.

Imagen obtenida de la recuperación del secreto

Conclusión

El uso de esteganografía permite ocultar información de un objeto en otros, en nuestro caso una imagen en otras imágenes alterando el bit menos significativo de cada uno de los píxeles.

Kuang-Shyr Wu y Tsung-Ming en su paper presentan una alternativa a la técnica de Thien y Lin permitiendo ocultar una imagen en otras y recuperar la imagen original con una menor pérdida de la calidad de la imagen original.

La implementación de esteganografía junto con el algoritmo de Kuang-Shyr Wu y Tsung-Ming permitió conocer de cerca una aplicación de la criptografía visual.

Bibliografía

- “An Efficient Secret Image Sharing Scheme” http://192.192.83.167/bitstream/987654321/1099/2/AMM.284-287.3025.pdf

- “Secreto Compartido”, de Ana María Arias Roig.