CRIPTOGRAFÍA Y SEGURIDAD

PRIMER CUATRIMESTRE 2014

ITBA

SECRETO COMPARTIDO EN IMÁGENES CON ESTEGANOGRAFÍA

TRABAJO PRÁCTICO 2

Grupo "GrupoHuno":

Domingues, Matias Gabriel

Legajo 50.278

Fontanella De Santis, Teresa Natalia

Legajo 52.455

Martinez Correa, Facundo Nahuel

Legajo 49.139

Responsables Académicos:

ABAD, Pablo

ARIAS ROIG, Ana

RAMELE, Rodrigo

ÍNDICE

OBJETIVOS

El presente Trabajo tiene como objetivo: implementar un algoritmo sobre secreto compartido aplicado a la esteganografía; y poder ocultar una imagen en otras, sin que se perciba siquiera su existencia.

1. CUESTIONES ANALIZADAS

1. *Discusión sobre aspectos relativos al documento de Ulutas y sus colegas:*

a. *Organización formal del documento*

El documento tiene la siguiente organización formal: una introducción, una breve explicación sobre el esquema de secreto compartido propuesto por Blakley, el método propuesto (con los respectivos algoritmos de distribución y reconstrucción), los resultados de los experimentos realizados (donde evalúa la correctitud del modelo, el tamaño de las sombras usadas, y los compara con otros modelos) y, finalmente, las conclusiones.

b. *Descripción del paso 7 del algoritmo de reconstrucción*

El paso 7 del algoritmo de reconstrucción consiste en resolver un sistema de k ecuaciones lineales (con módulo 251), usando para ello la inversa de la matriz en cuestión.

c. *La notación utilizada, ¿es clara? ¿Cambia a lo largo del documento?*

La notación, si bien no es del todo clara resulta consistente, ya que no cambia a lo largo del documento.

2. *En el método original de secreto compartido de Blakley se descartan las sombras que tengan ceros. ¿Por qué? ¿Por qué Ulutas y sus colegas no tuvieron en cuenta eso?*

El método original propuesto por Blakley tiene en cuenta como hipótesis (que no prueba, pero que considera plausible), que la probabilidad de que un número random en módulo p (siendo p un número primo) tenga su determinante con el mismo valor, es mayor a 1/2p y menor a 2/p. En el caso del documento de Ulutas, p= 251, y la probabilidad W (considerando a x=0) sería $0.0019<W<0.0079$, es decir está en el orden de milésimas de error, por lo que podría considerarse como muy poco probable, y por eso Ulutas y sus colegas no tienen en cuenta esa restricción.

3. *Una vez recuperada la imagen secreta, ¿es esta imagen exactamente igual a la imagen ocultada? ¿Por qué?*

La imagen recuperada no es exactamente igual a la ocultada, ya que el rango de bits de cada pixel en esta última, no es de 0 a 255 (es de 0 a 251 como máximo).

4. *Discusión sobre aspectos relativos al algoritmo implementado:*

a. *Facilidad de implementación*

Implementar el algoritmo no fue fácil. Por ejemplo, a la hora de obtener la imagen oculta a partir de las sombras, el manejo de bits resultó engorroso (fue preciso pasar los valores al tipo "unsigned int"). Inclusive, como se necesitaba operar con matrices, hubo que implementar la multiplicación y la inversa de matrices (entre otros), lo cual implicó un cierto grado de complejidad.

b. *Posibilidad de extender el algoritmo para que se usen imágenes en color.*

Es posible extender el algoritmo a imágenes de color (usando RGB), al considerar a 16769023 como p (número primo inmediatamente anterior a 2^24), pero las sombras podrían no tener el mismo tamaño que la imagen a ocultar.

c. *Ventajas respecto del algoritmo original de Shamir (mencionar por lo menos 2)*

Una de las ventajas con respecto al algoritmo original de Shamir, es que se pueden obtener sombras "con significado" (es decir, son imágenes que no aparentan ocultar información), cosa que con Shamir no se puede. Además, el algoritmo posibilita que las sombras sean imágenes del mismo tamaño que la imagen oculta (lo que no ocurre con lo propuesto por Shamir).

5. *¿Qué dificultades hubo en la lectura del documento y/o en la implementación?*

Parte de las dificultades superadas son las mencionadas en el **punto 1. 4. a.**

Empero, hubo problemas con la lectura del paper, ya que al describir mal los pasos para incorporar el hash en los subpíxeles (después del cálculo de las "a"), en el cálculo del b están incluyendo el bit que tendría que estar reservado para el bit de paridad. También hubo problemas con las imágenes BMP, al haber inconsistencia en sus headers.

6. *¿Qué extensiones o modificaciones podrían hacerse a la implementación o al algoritmo?*

A la implementación se le podría hacer extensiones tales como:

- Soportar otros tipos de formato de imágenes para los portadores (como jpg, png, entre otros).
- Aceptar como portadores archivos de diferentes formatos (verbigracia, de audio y video).
- Implementar esteganografía de texto (es decir, ocultar información en archivos de texto).
- Entre otros.

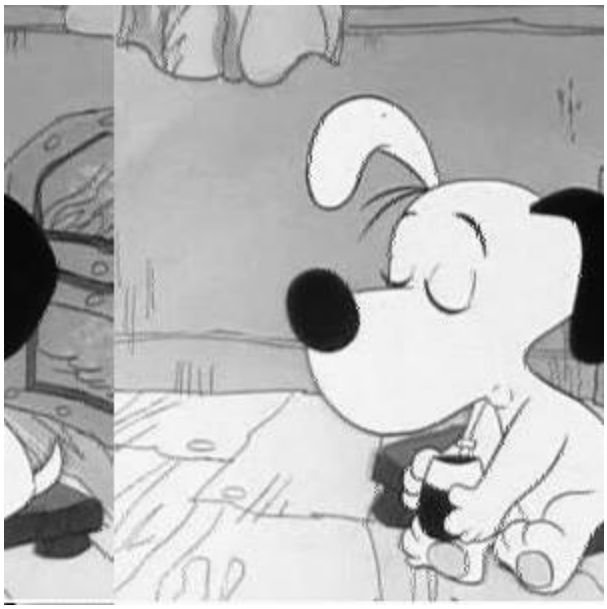
7. ¿En qué situaciones podrían aplicarse este tipo de algoritmos?

Este tipo de algoritmos, podría aplicarse en situaciones en donde se usan imágenes del mismo tamaño que la imagen a ocultar; y es muy útil para transmisión de imágenes militares o comerciales, como cuando para visualizar ciertos datos se requiere que estén todos los involucrados, por ejemplo, que sólo los responsables de una organización puedan ver conjuntamente cierta información confidencial de la misma.

2. SOLUCIÓN A LA RECUPERACIÓN DEL SECRETO COMPARTIDO

Considerando k= 2, la imagen recuperada es la siguiente:

Y para k=3, la imagen obtenida es:



3. FUENTES CONSULTADAS

- Capítulo 15 de Computer Security – Art and Science, Matt Bishop, Addison-Wesley, 2004
- Capítulo 10 y 12 de Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, CRC Press, 1997
- "Improvements in Geometry-Based Secret Image Sharing Approach with Steganography", de Mustafá Ulutas, Vasif V. Nabiyev, y Guzin Ulutas.
- "Secreto Compartido", de Ana María Arias Roig.

Sobre Criptografía Visual

- Página de Criptografía visual de Doug Stinson: http://cacr.uwaterloo.ca/~dstinson/visual.html
- "Visual Cryptography", Moni Naor y Adi Shamir. http://www.fe.infn.it/u/filimanto/scienza/webkrypto/visualdecryption.pdf

Sobre Formato BMP

- http://www.fileformat.info/format/bmp/corion.htm