



## MANUAL DE STEGSECRET. (v0.1)

---

0. **Breves Definiciones. Estegoanálisis y Esteganografía.**
1. **¿ Qué es StegSecret?.**
2. **¿Qué detecta StegSecret beta v0.1?.**
3. **¿Porqué es StegSecret una beta?.**
4. **Manual de uso de XStegSecret.**
5. **Agradecimientos y Colaboración.**
6. **Sobre el Autor.**

### 0. Breves Definiciones. Estegoanálisis y Esteganografía.

**El término Esteganografía se define como la ciencia y/o arte de ocultar una información dentro de otra, que haría la función de “tapadera” (estegomedio o cubierta).** En la criptografía, en cambio, no se oculta la existencia del mensaje sino que se hace ilegible para quien no esté al tanto de un determinado secreto (la clave).

**El término Estegoanálisis se define como la ciencia que estudia la detección (ataques pasivos) y/o anulación (ataques activos) de información oculta en distintas tapaderas,** así como la posibilidad de localizar la información útil dentro de la misma (existencia y tamaño). Dependiendo del proceso empleado para ocultar la información, su recuperación puede ser inviable, correspondiendo su inversión a la ciencia del criptoanálisis. Piense, por ejemplo, en el cifrado de una información utilizando un algoritmo criptográfico “seguro” (¿?) y la utilización de un PRNG para seleccionar las posiciones donde se ocultara la información dentro de un estegomedio dado.

Resumiendo, el estegoanálisis (ataques pasivos) se centran fundamentalmente (hasta donde es posible):

1. Detectar la presencia de información oculta.
2. Estimación del tamaño de la información oculta.
3. Localización exacta de la información oculta dentro de una cubierta.
4. Extracción de la información útil, invirtiendo la codificación aplicada, si es necesario.

## 1. ¿Qué es StegSecret?.

**StegSecret** es el nombre que recibe el proyecto de software libre que tiene la intención de desarrollar y mantener un conjunto de herramientas libres que permitan la detección de información esteganografiada en diferentes medios de información. Su objetivo principal consiste en recopilar, implementar y facilitar el uso de los numerosos estudios estegoanalíticos que faciliten la detección de información ocultada en diferentes medios, especialmente medios digitales, como imágenes, audio y video. Este proyecto pretende alertar sobre la inseguridad que presenta la utilización de multitud de herramientas y algoritmos esteganográficos, así como el uso indebido de ciertas técnicas más seguras.

Actualmente, el proyecto StegSecret está constituido por dos herramientas. StegSecret una herramienta en modo consola que facilita la automatización de la detección en diferentes fuentes de datos (próximamente) y Xstegsecret una herramienta visual que comentaremos a continuación.

Actualmente las herramientas desarrolladas en este proyecto están realizadas en JAVA JDK1.5 (multiplataforma) y están liberadas bajo licencia GPL.

## 2. ¿Qué detecta StegSecret beta v0.1?.

StegSecret es un proyecto ambicioso que pretende implementar el mayor número de procedimientos estegoanalíticos para dar una mayor fiabilidad a los resultados que se muestren a los analistas. Existe mucha información a considerar, pero especialmente en StegSecret se están implementando los ataques más robustos publicados en congresos científicos.

Estos últimos años diferentes personas han publicado herramientas y diferentes ataques (ver pagina web-sección documentación). Herramientas gratuitas, por ejemplo, como StegDetect. El mayor problema de estas, es que son herramientas muy concretas para ciertas herramientas de ocultación, y sobre todo, no se han ido mejorando con el tiempo.

Existen algunas herramientas comerciales que se puede citar a modo de ejemplo. Por ejemplo, **StegoSuite** (WetStone Technologies) de la cual no puedo probar su “fiabilidad” porque no hay ninguna versión trial, pero por su publicidad presenta cosas interesantes que deberían tener cualquier entorno integrado de estegoanálisis como pretende StegSecret. Por ejemplo, StegWatch (que detecta información oculta en imágenes y ficheros de audio), StegAnalyst (que permite el análisis de propiedades de imágenes como el brillo, el contraste, la paleta de colores, los valores RGB de los píxeles, etc) y StegBreak (diseñado para recuperar la clave utilizada en el proceso de codificación de ciertos algoritmos F5, JPHIDE&Seek, Camouflage y Jsteg), así como una serie de escaneadores activos orientados para detectar la presencia de información oculta en una web concreta o en un dominio corporativo. Características muy interesantes a implementar....., pero StegSecret tiene una ventaja muy importante, es gratis ;)

Otras herramientas a destacar son las de la empresa BackBone Security, especialmente destacable **SAFDB** (Steganography Application Fingerprint Database)...

*“...With the hash values of all file artifacts associated with 650 digital steganography, watermarking, and other data-hiding applications, SAFDB is the most extensive steganography application hash set publicly available anywhere. SAFDB is available for a license fee of \$250.00...”*

Ay, por Dios, que poca vergüenza cobrar por esto. Por este motivo, StegSecret incorpora su propia **BDAS** (Base de datos de Aplicaciones sospechosas), auguro ;) que en un par de meses la SAFDB va a tener una seria competidora... eso sí, gratuita ;)

Visto todo esto, permite hacerse una idea del interés cada vez mayor que tiene el estegoanálisis, especialmente para múltiples empresas que intentan vender "productos mágicos" a policía, militares, servicios de inteligencia, etc. Y en muchos casos hay poco que rascar..., StegSecret pretende acercar esto al ciudadano de a pie... bueno a todo el mundo, a los anteriores también ;)

Vamos con StegSecret [XStegSecret]...

StegSecret es una herramienta desarrollada en JAVA JDK1.5-SWING con una estructura modular, en la cual todo está pensado para automatizar y simplificar la vida al estegoanalista. Actualmente en la versión beta 0.1 publicada incluye:

## **2.1. Detección de Patrones Fijos.**

Permite detección de información ocultada por ciertas aplicaciones conocidas que dejan rastros traceables, "patrones". De esta forma se ha programado una lista de reglas de patrones, que permiten detectar información ocultada con ciertas herramientas.

Son detectados "los rastros" dejados por las siguientes herramientas "esteganográficas" [versión beta 0.1] (9):

**camouflage V1.2.1, inThePicture v2, JPEGXv2.1.1, PGE (Pretty Good Envelope) v1.0, appendix v<=4, steganography v1.6.5, inPlainView, DataStash v1.5 y dataStealth v1.0.**

Estos programas ocultan información al final del fichero portador (técnica EoF) o la utilización de una técnica LSB mal implementada. Actualmente se está implementando muchas otras...

En la versión beta publicada, se permite la detección de la presencia de información oculta y observar el tamaño de los datos ocultos (cuando es posible). Actualmente se está implementando la posibilidad de recuperar la información útil (en breve).

## **2.2 Reconocimiento de la estructura de ficheros.**

El reconocimiento adecuado del formato de un fichero es esencial como primer paso para poder clasificar adecuadamente un fichero informático, y poder aplicar la técnica estegoanalítica más conveniente para el formato del fichero en cuestión.

Debido a esto, está implementado en la versión beta 0.1 el reconocimiento de la estructura de ficheros BMP, GIF y JPEG. Son los estegomedios más difundidos.

Esto además de ser útil para la clasificación, implementa de forma intrínseca procedimientos heurísticos. Reconociendo estos formatos es posible detectar información oculta al final de un fichero BMP, GIF o JPEG de forma automática (técnica EoF), independientemente de la herramienta esteganográfica que implemente esta técnica.

La técnica EoF es una técnica de ocultación trivial, pero automatizar su detección en grandes volúmenes de información requiere de procedimientos variados, un ejemplo interesante, son estas técnicas de reconocimiento de estructura de ficheros.

He comprobado que existen muchas imágenes (BMP, GIF y JPEG) que no cumplen con el formato estándar, por eso la herramienta lo alerta, cuando lo más probable es que no tenga información oculta.

### **2.3. Procedimientos EstegoForenses. Programas Sospechosos.**

He desarrollado "BDAS v0.1" (Base de Datos de Aplicaciones Esteganográficas) una base de datos con información de aplicaciones esteganográficas y programas sospechosos que podrían estar presentes en un ordenador bajo estudio. La presencia de estas herramientas puede proporcionar información adicional a un estegoanalista en sus investigaciones.

Actualmente (BDAS v0.1) detecta **40 programas sospechosos apoyados en más de 68 fuentes sospechosas**. Como, comprenderá, lo importante es la lógica para leer esta base de datos, con lo que, la base de datos aumentará rápidamente ;). Voy a intentar hacerla compatible con las diferentes herramientas forenses para que puedan utilizarla.

### **2.4. Análisis de Imágenes.**

StegSecret incluye una herramienta que permite el análisis manual de diferentes formatos gráficos. Incluye diferentes algoritmos estegoanalíticos de diferente complejidad, por ejemplo, diferentes algoritmos estadísticos.

En StegSecret b0.1 está implementado diversos ataques para ficheros BMP (8,16,24,32 bits/píxel) (en breve, para índices GIF y DCTs-JPEG). Se ha implementado:

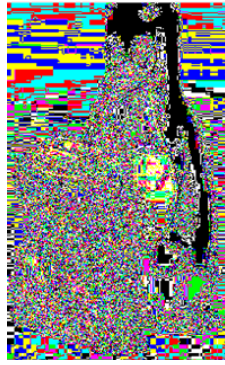
- a) **Ataques Visuales** (basados en las ideas de Andreas Westfeld)
- b) **Ataque estadístico ChiSquare** (Andreas Westfeld et al). Utilizado para detección de LSB secuencial y estimación de tamaño de información oculta.
- c) **Ataque RS** (Jessica Fridrich et al). Utilizado para detección de LSB pseudoaleatorio y estimación de tamaño.

#### **[Breve información sobre los ataques implementados]**

**Ataque Visual a Imágenes.** Basado principalmente en procesos de filtrado. Especialmente útil, para técnicas de ocultación LSB-secuencial y cubiertas con presencia de áreas de colores uniformes o saturados (0 o 255). Una de las primeras pruebas de concepto que demuestran que la información ocultada en los bits menos significativos de una imagen si **genera una alteración detectable**.



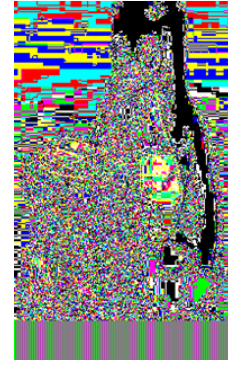
Imagen Original



Ataque Visual



Imagen con 5Kb de info oculta.



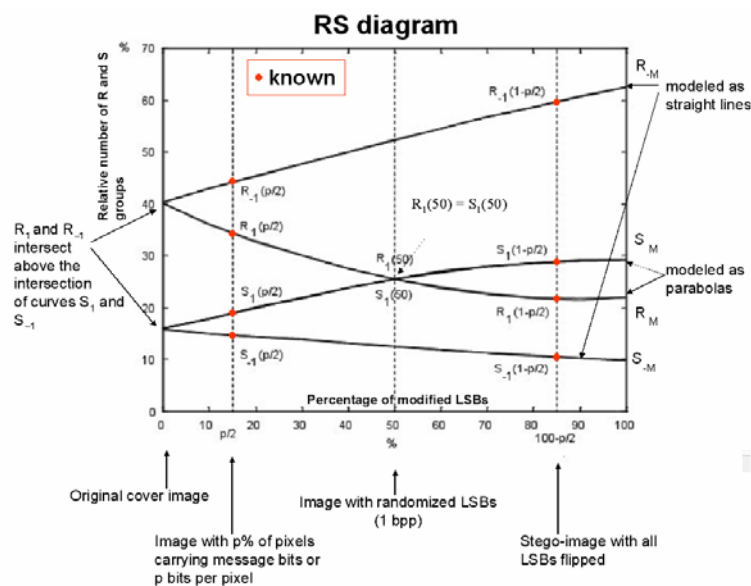
Ataque Visual

**Ataque Chi-Square.** Ataque Estadístico publicado por los investigadores Pfitzman y Westfeld que permite estimar el tamaño de la posible información ocultada en un estegomedio. **Puede ser aplicado a cualquier técnica esteganográfica**, en la cual un conjunto fijo de parejas de valores (Pairs Of Values, PoVs) comunten de un valor al otro de la pareja cuando se inserta los bits del mensaje oculto. Puede aplicarse con éxito, por ejemplo, a técnicas LSB-secuencial sobre coeficientes cuantificados DCTs, índices a una paleta de colores, LSB de pixels, etc.

$$\chi_{k-1}^2 = \sum_{i=1}^k \frac{(n_i - n'_i)^2}{n'_i}$$

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}} \Gamma\left(\frac{k-1}{2}\right)} \int_0^{\chi_{k-1}^2} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx$$

**Ataque RS.** Jessica Fridrich, M. Goljan and R. Du (SUNY Binghamton, NY) publicaron en octubre de 2001 **“Reliable Detection of LSB Steganography in Grayscale and Color Images”**. Algoritmo muy preciso (uno de los más) para la detección de LSB-pseudoaleatorio. Su precisión varía en función de la imagen, pero un valor de referencia está en torno a 0’005 bits por píxel (0’5% de la ocupación total posible). Si se oculta más información que 0,005 bits por píxel el algoritmo detectará la presencia de información oculta, y estimará el tamaño de la información enmascarada.



**Nota (breve) sobre estas técnicas:** En general, los algoritmos estegoanalíticos tienen unos determinados umbrales mínimos de detección, es decir, si se oculta una información pequeña por debajo de estos, los algoritmos estegoanalíticos no funcionan adecuadamente, del mismo modo sus resultados (su precisión) puede variar dependiendo de algunas imágenes concretas. Esto es así, porque aunque una imagen no tenga información oculta devuelve, en algunos casos, un pequeño tamaño de información oculta, unos cientos de bytes (en el mejor de los casos), por este motivo, el algoritmo si ocultamos información pequeña no puede distinguir entre imagen original e imagen oculta (límite de detección). Esto es aplicable, por ejemplo, al algoritmo RS.

El algoritmo ChiSquare, es muy buen algoritmo para detección de LSB-Secuencial especialmente, si sabes, más o menos, donde está la información oculta. Actualmente, el algoritmo se aplica de forma fija y considera que la información está ocultada desde el principio (más o menos) del fichero sospechoso, y desde ahí es de donde aplica los cálculos estadísticos. Si esto no es así, los resultados del algoritmo podría variar. Esto es la naturaleza propia de este algoritmo, estoy trabajando para flexibilizar su ejecución por parte del usuario, para aumentar la precisión de detección dentro de lo posible.

Por estos motivos (la naturaleza propia de los algoritmos estegoanalíticos en evolución) StegSecret implementa (e implementará) múltiples algoritmos (los más precisos publicados) para poder aplicarlos, a la vez, en distintas situaciones y proporcionar más información al analista para decidir si una tapadera almacena información oculta o no.

La clave está en que el analista sea consciente de los resultados que le muestra la herramienta y como interpretarlos, esto siempre será mejor, que no las herramientas que muestran “estrellitas” diciendo como de probable es que una imagen tenga información oculta. ¿Qué narices significa que una imagen tiene información oculta con un 60% de probabilidad? Un sí pero no.....

**Conclusión:** Actualmente si buscas una información ocultada con un LSB-Secuencial aplica ataques Visuales y ChiSquare a la imagen, y si buscas LSB-Pseudoaleatorio aplica RS.

Para más info, por favor, escríbeme un mail o lee los artículos de los autores.

### **3. ¿Porqué es una StegSecret se publica como beta?.**

Aunque la esteganografía y el estegoanálisis no es mi trabajo de investigación, sí es un hobby que me “entretiene” algunas horas (nunca minusvaloréis el poder del aburrimiento). La herramienta presentada es mejorable en múltiples aspectos, pero creo que es importante su difusión actual y la colaboración si alguien lo estima oportuno. Por eso, es una beta...

Falta optimizar el código, probarlo en diferentes plataforma (actualmente está probado +- en Windows XP SP2 v5.1.2600 y en Debian 2.6.20+KDE 3.5), mejorar las técnicas de filtrado, el interfaz gráfico y sobre todo aumentar las técnicas de detección. Actualmente, la técnica ChiSquare se puede flexibilizar mucho (utilizo la librería commons-math-1.0.jar, licencia Apache 2.0) y la técnica RS está basada en la implementación de Kathryn Hempstalk (Digital Invisible Ink Toolkit.) completamente funcional, aunque algo optimizable. Gracias Kathryn.

Existen muchas técnicas y procedimientos triviales que mejorarán la herramienta (en ello estamos) respecto al módulo de análisis de imágenes: mostrar información de la imagen, incorporar técnicas clásicas de filtrado, extracción de LSB, histogramas, acceso a cabeceras, etc. A parte, de algoritmos complejos que están en desarrollo. Actualmente, por ejemplo, el ataque ChiSquare muestra una gráfica

tabulada a 10KB de información oculta como mucho, de momento, lo importante es ser consciente que existe una información oculta...

Actualmente, las reglas que detectan los “patrones” dejados en estegomedios por programas esteganográficos están programadas directamente. Ya tengo diseñado un lenguaje de reglas, de forma que la incorporación futura de reglas de detección se escriba en este lenguaje y no haya que programarlas a mano.

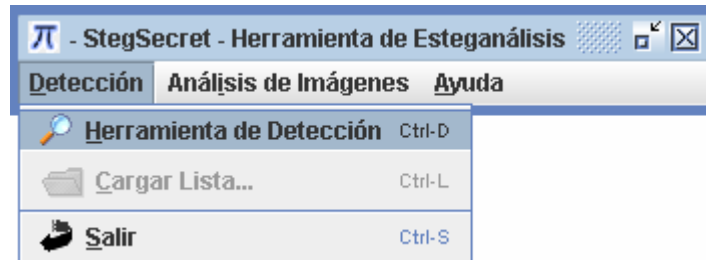
En fin, mucho curro interesante.... ¿si alguien quiere colaborar? Pago 0 euros/hora ;)

## 4. Manual de uso de XStegSecret.

### 4.1 Instalación-Ejecución de XStegSecret.

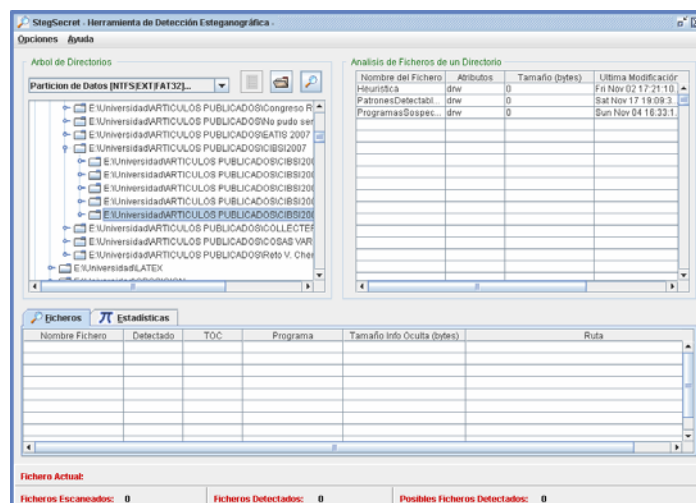
La instalación-ejecución de XStegsecret es muy sencilla.

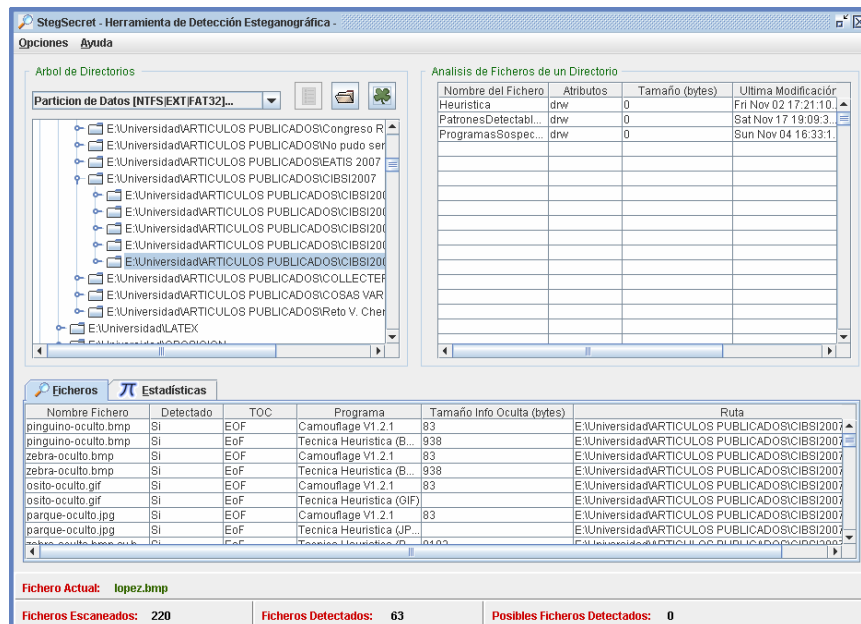
1. Bajar en un mismo directorio los ficheros, xstegsecret.jar (o su versión .exe), BDAS v.0.1 y tutorial.html.
2. Ejecutar la herramienta. #java -jar xstegsecret.jar o #xstegsecret.exe



### 4.2 Herramienta de Detección.

**Lupa:** Inicia el escaneo automática a partir de la ruta indicada en el arbol. Puede elegirse una ruta especifica utilizando el icono “carpeta”, para ello pinchar en un fichero del directorio al que se quiere acceder.





**Trébol de Cuatro Hojas** (¿Voy a tener suerte?): Icono que indica que el proceso de escaneo está activo, para parar pulsad encima.

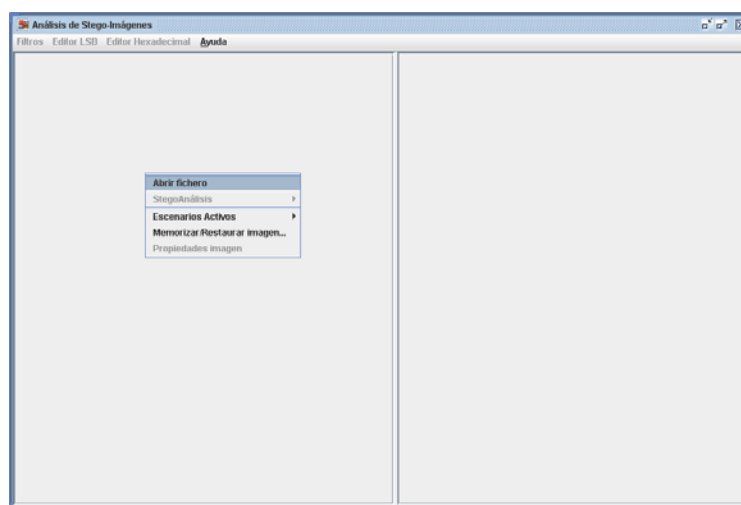
### Salvar Resultados: Opciones-> Guardar Resultados.

En los resultados viene todo tipo de información sobre el fichero donde se ha encontrado información oculta. Por ejemplo, Técnica EOF= End of File (informa de información oculta al final de fichero), LSB (información oculta en el LSB), PoS (presencia de programas sospechosos).

Como se puede observar en esta versión, la utilización de XStegsecret es muy sencilla, todo se reduce a pulsar en un botón y escanear todas las técnicas conocidas. En futuras versiones, se dará la opción de elegir que técnicas concreta de detección quiere el usuario utilizar.

## 4.2 Herramienta de Análisis de Imágenes.

La herramienta de análisis está formada por 2 escenarios (izquierda y derecha), con lo que es posible operar con 2 imágenes a la vez si se desea. Lo cual, como comprobará, es muy útil. Pulsando el botón derecho del ratón se ven las operaciones que se pueden realizar sobre cada escenario.



Al pulsar “Abrir Fichero” se puede abrir una imagen en un escenario, actualmente sólo se puede aplicar operaciones de estegoanálisis sobre ficheros BMP. Al cargar una imagen esta quedará memorizada, si usted realiza alguna operación sobre la imagen en un escenario y quiere recuperar la imagen original, pulse “Memorizar/Restaurar Imagen”.

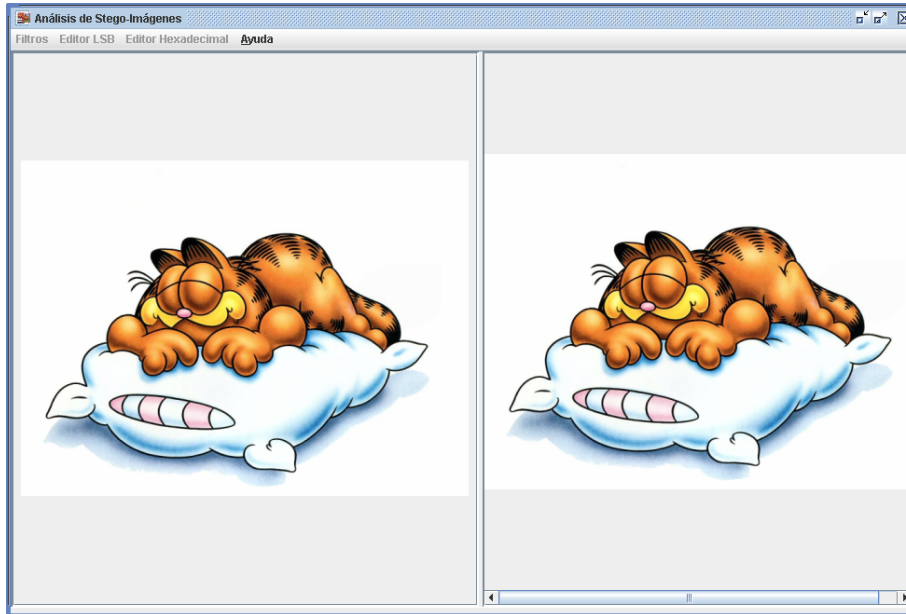
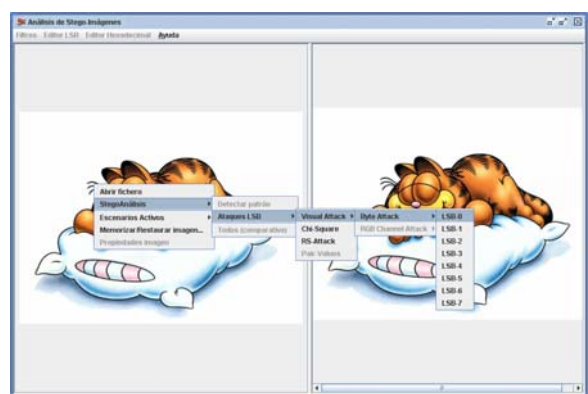
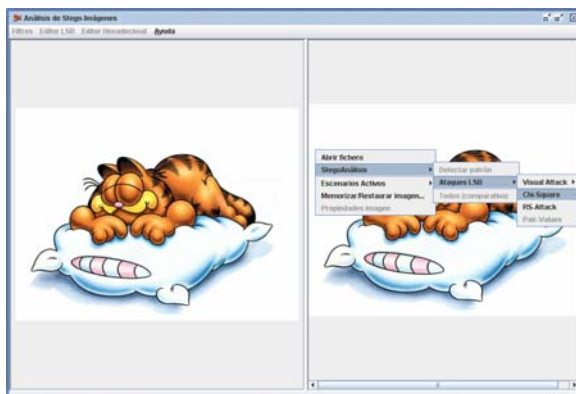
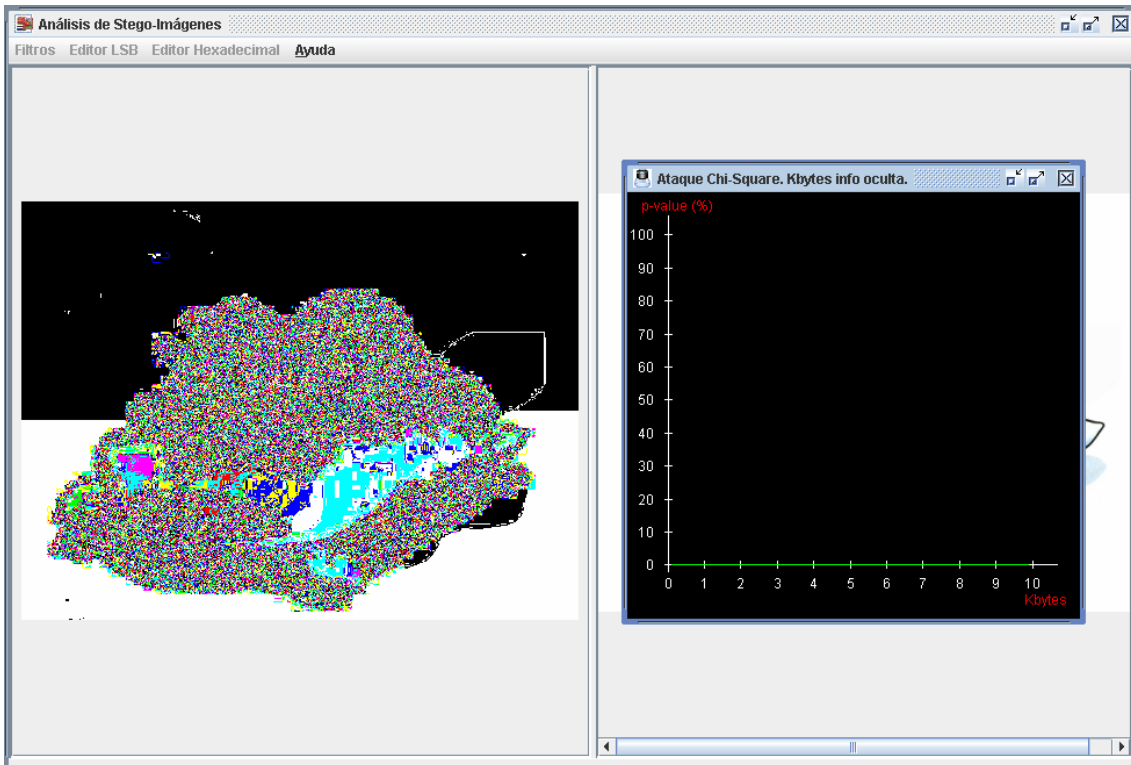


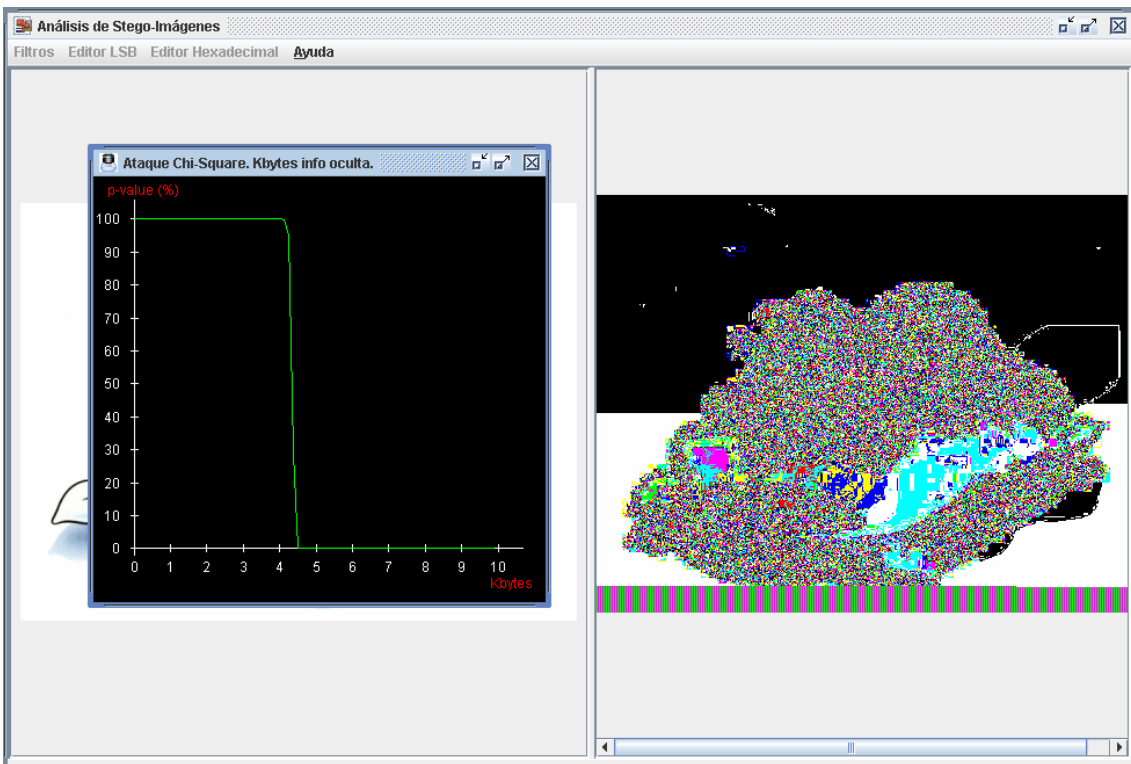
Imagen Izquierda: Garfield.bmp Imagen Derecha: garfield.4KbytesLSBsecuencial.bmp



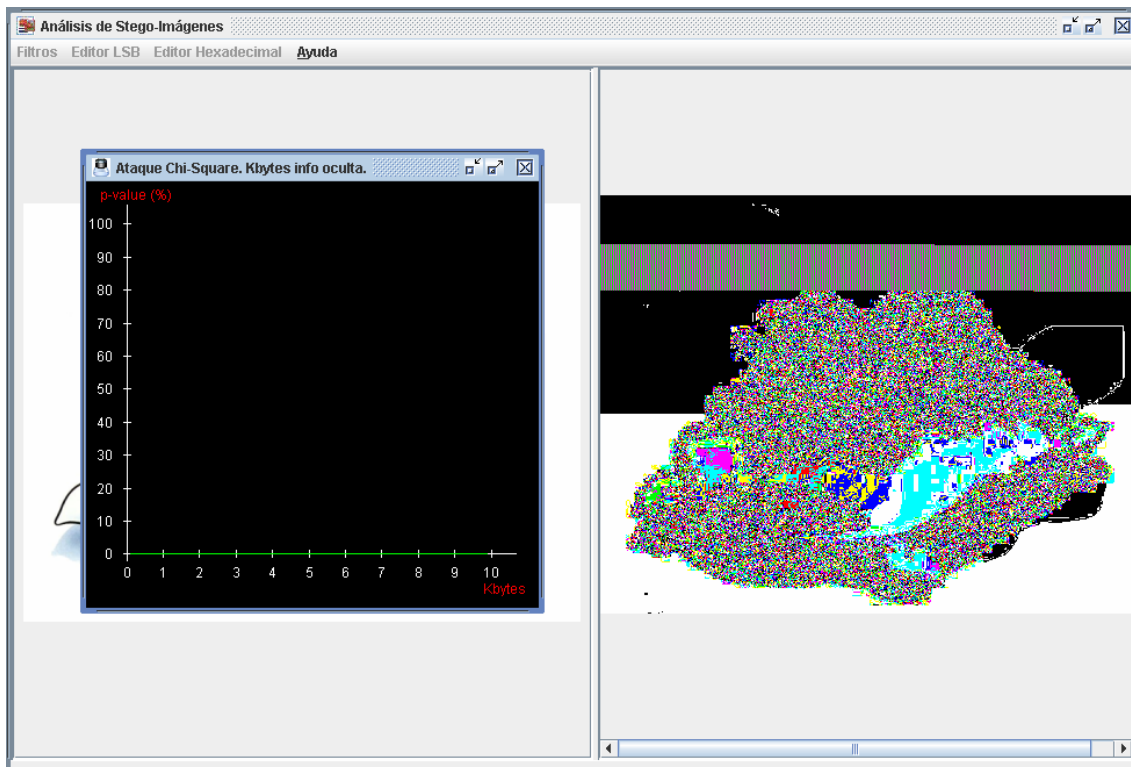
Ejecución de distintos ataques Visuales, ChiSquare y RS Attack.



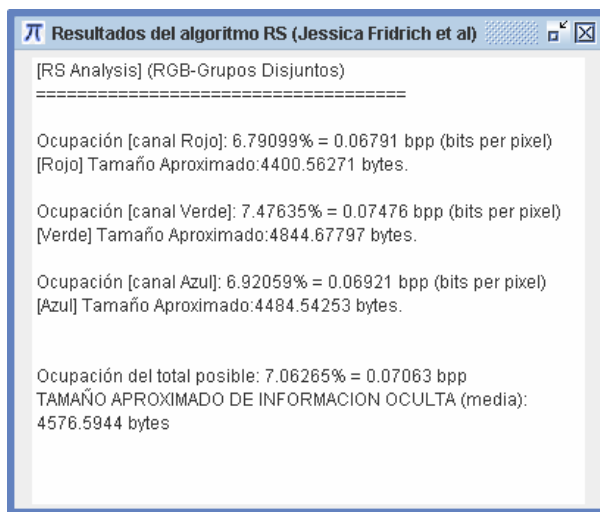
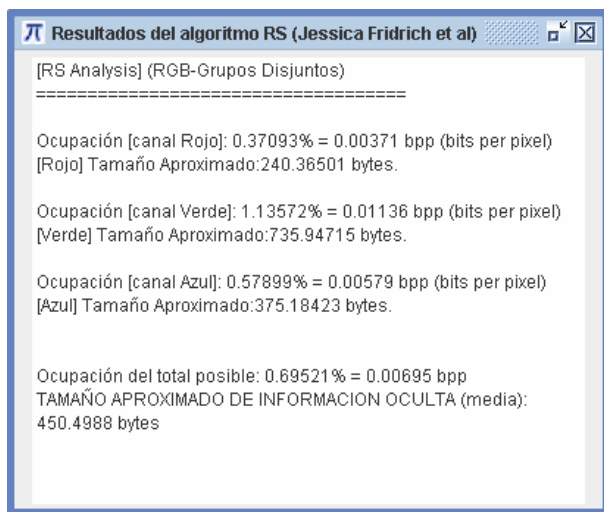
Ataque Visual (LSB0) y ChiSquare a una imagen sin información oculta.



Ataque Visual (LSB0) y ChiSquare a imagen con 4KB de info oculta por LSB secuencial.

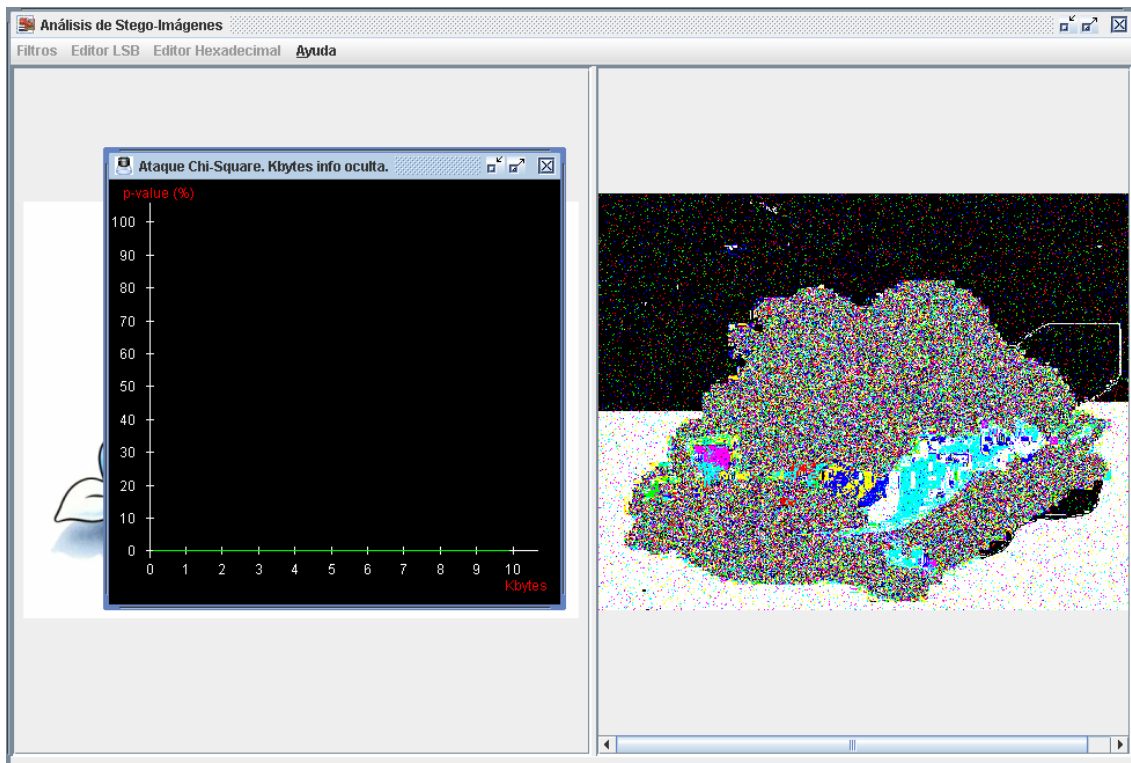


Ataque Visual (LSB0) y ChiSquare (vemos que falla) a una imagen 7KB de info oculta en el 1er LSB a partir de la posición 400.000 píxeles del fichero.



Resultado de aplicar el ataque RS a una imagen sin información oculta, garfield.bmp, (imagen izquierda) y otra a la misma imagen con 4KB de información oculta de forma pseudoaleatoria en sus píxeles, garfield.4KBLSBaleatorio.bmp (imagen derecha).

Puede observarse, que la imagen sin información oculta refleja un pequeño tamaño de información oculta, un falso positivo, o mejor dicho muestra el limite del umbral de detección para esta imagen concreta. Puede observarse en la diferencia de los 2 resultados, la precisión del algoritmo RS.



Ataque Visual (LSB0) y ChiSquare a garfield.4KBLSBaleatorio.bmp

## 5. Agradecimientos y Colaboración.

Uno de los objetivos principales de este proyecto es llamar a la colaboración para hacer más grande este proyecto. Cualquier colaboración es bien recibida...

Cualquiera puede colaborar, por ejemplo en:

1. Generar los hashes MD5 y SHA1 de aplicaciones sospechosas de ocultación de información disponibles en Internet. Útil para aumentar el tamaño de BDAS.
2. Análisis de herramientas que dejen patrones rastreables automáticamente.
3. Implementación de cualquier procedimiento estegoanalítico.

...

## 6. Sobre el Autor.

**StegSecret.** Copyright (C) 2007. **Alfonso Muñoz.** e@mail: [amunoz@diatel.upm.es](mailto:amunoz@diatel.upm.es)  
 Más info: [<http://stegsecret.sourceforge.net>].