Esteganografía, esteganálisis e Internet

Descubriendo el reverso de Internet : web mining, mensajes ocultos y secretos aparentes

Colmenarejo, 22 de Febrero de 2007

Arturo Ribagorda Garnacho
Juan M. Estévez-Tapiador
Julio César Hernández Castro

INSTITUTO JUAN VELÁZQUEZ DE VELASCO
de Investigación en Inteligencia para la Seguridad y la Defensa
Universidad Carlos III de Madrid

Agenda

1. Introducción histórica
2. Esteganografía en la era digital
3. Esteganálisis
4. Mensajes ocultos e Internet
5. Casos prácticos, trabajos en curso y resultados

Agenda

1. **Introducción histórica**
2. Esteganografía en la era digital
3. Esteganálisis
4. Mensajes ocultos e Internet
5. Casos prácticos, trabajos en curso y resultados

Cifrado vs. Ocultación de la información

- Preferida por muchos autores clásicos (Aeneas el Táctico, John Wilkins, Trithemius, ...), a pesar de disponer ya de métodos para cifrar la información.

- **No despierta sospechas**

- ¿Por qué tanto interés ahora?
  - http://www.usatoday.com/tech/columnist/2001/12/19/maney.htm
  - Realmente siempre ha sido utilizada en otros contextos
  - Protección de derechos de autor *(watermarking* y *fingerprinting)*
  - Aplicaciones:
    - Agencias militares y de inteligencia
    - Criminales (y policía)
    - Civiles contra las restricciones impuestas por el Estado
    - Muy relacionadas con técnicas de anonimato (dinero electrónico, servicios de localización, voto electrónico, etc.)

Esteganografía

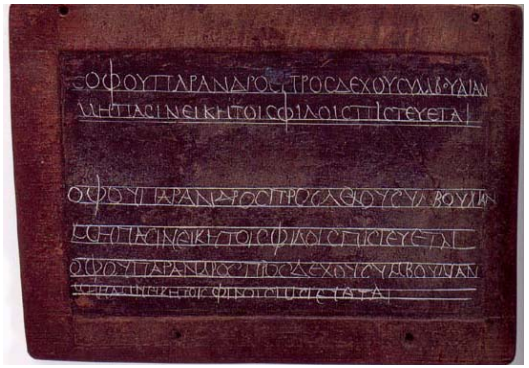
- Ocultación de la información en un canal encubierto (*covert channel*) con el propósito de prevenir la detección del mensaje oculto.

- Protección de la información ocultando la existencia de la comunicación misma.
  - La información se encuentra inmersa *sutilmente* en un vehículo.
  - Se revela sólo aplicando un procedimiento adecuado.

- Áreas relacionadas:
  - *Watermarking*
  - *Fingerprinting*

Esteganografía clásica

Heródoto (484 AC-425 AC)



- 23 Septiembre 480 AC
- Demarato (exiliado en Susa)…

"Como el peligro de que lo descubrieran era muy grande, sólo había una manera en que podía contribuir a que pasara el mensaje: retirar la cera de un par de tablillas de madera, escribir en la madera lo que Jerjes planeaba hacer y luego cubrir el mensaje con cera. De esta forma, las tablillas, al estar aparentemente en blanco, no ocasionarían problemas con los vigías del camino. Cuando el mensaje llegó a su destino, nadie fue capaz de adivinar el secreto, hasta que la hija de Cleomenes, Grogo, que era la esposa de Leónidas, lo vaticinó y les dijo a los demás que si quitaban la cera encontrarían algo escrito debajo, en la madera. Se hizo así; el mensaje quedó revelado y fue leído, y después fue comunicado a los demás griegos."

Esteganografía clásica

Técnicas antiguas

- China: bolas de cera engullidas
- Giovanni Porta (s. XV): huevo duro
  - Tinta con alumbre y vinagre
- Tintas invisibles
  - *Básicas:* sustancias con alto contenido en carbono (leche, orina, zumo de limón, zumo de naranja, zumo de manzana, zumo de cebolla, solución azucarada, miel diluida, coca cola diluida, vino, vinagre, agua jabonosa, …)
  - *Más sofisticadas:* aparecen tras una reacción química, o tras ser expuestas a luz en una cierta longitud de onda (IR, UV, …)

Esteganografía clásica

Francesco Colonna (1499) *Hypnerotomachia Poliphili*

(Ed. Aldus Manutius)

http://mitpress.mit.edu/e-books/HP/

Esteganografía clásica

Primera letra de los 38 capítulos:

‘Poliam frater Franciscus Columna peramavit’
(‘El hermano Francesco Colonna ama apasionadamente a Polia’).

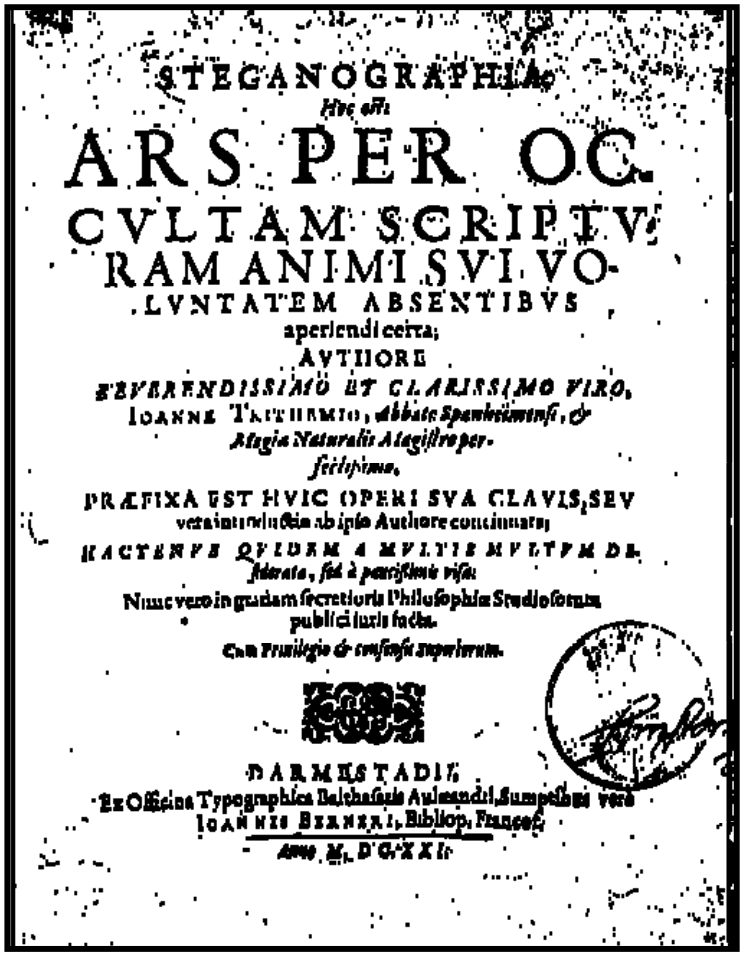
ΓΥΜΝΟΣ ΗΝ ,ΕΙ ΜΗ ΑΝ ΘΗΡΙ-
ΟΝ ΕΜΕΚΑΛΥΨΕΝ.ΖΗΤΕΙ.ΕΥ-
ΡΗΣΗΔΕΔΕΑΣΟΝ ΜΕ.

NVDVS ESSEM, BESTIANIME
TEXISSET, QVAERE, ET INVE
NIES-MESINITO.

Ian Caldwell, Dustin Thomason (2004)
“The Rule of Four” (Ficción)

Esteganografía clásica

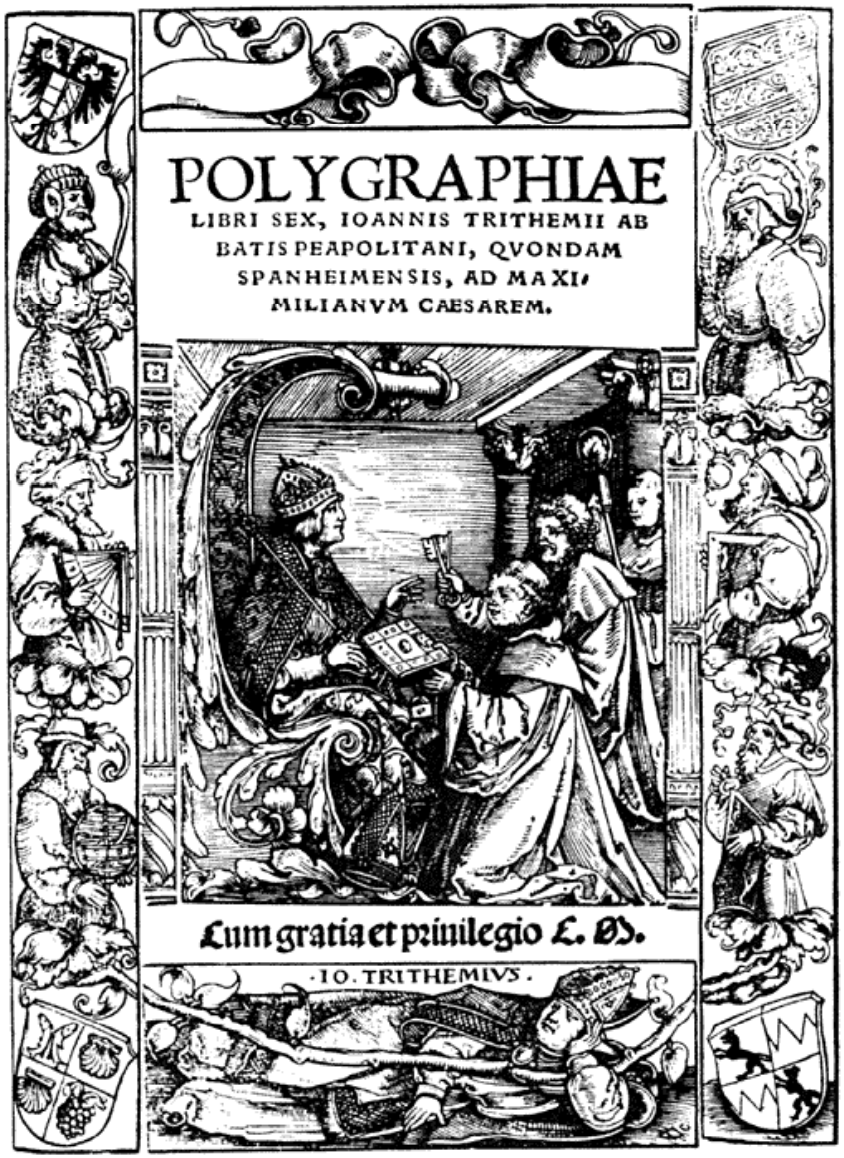
Ioannis Trithemius (1462-1516)
Steganographia (1499)


STEGANOGRAPHIAE
Hoc est:
ARS PER OC.
CVLTAM SCRIPTV
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimensi, &
Magia Naturalis Magistro per-
fectissimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
veram methodum ab ipso Autore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
siderata, sed à paucissimis visa:
Nunc vero in gratiam secretioris Philosophiæ Studiosorum
publici iuris facta.
Cum Privilegio & consensu superiorum.
DARMSTADII,
Ex Officina Typographica Balthasaris Aulmandi, Sumptibus vero
IOANNIS BERNERI, Bibliop. Francof.
Anno M. DC. XXI.

http://www.esotericarchives.com/tritheim/stegano.htm

Esteganografía clásica

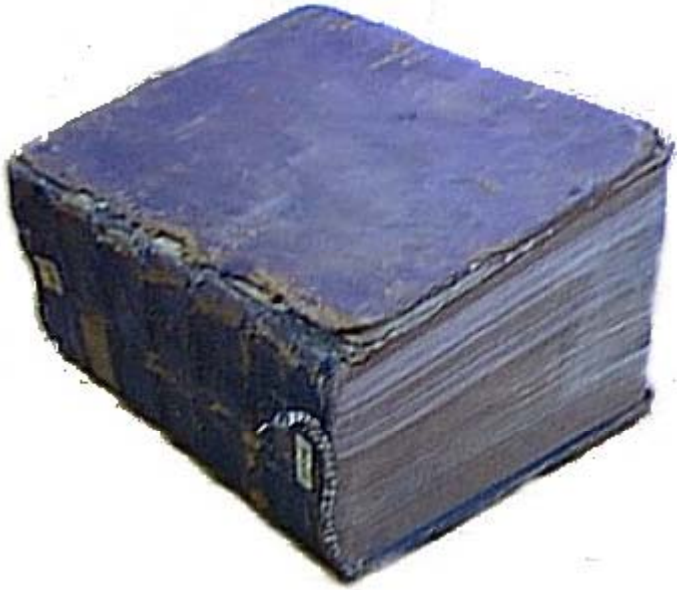
Polygraphiae libri sex, Ioannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Ceasarem (1518)

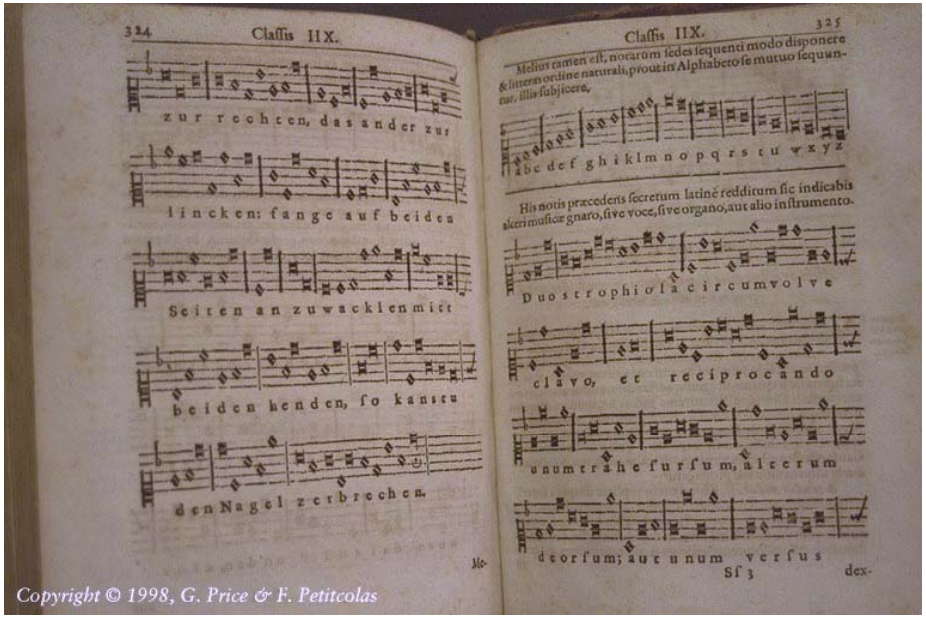


Esteganografía clásica

Gaspar Schott (1665) *Schola steganographica*

http://www.petitcolas.net/fabien/steganography/steganographica/index.html





Un caso reciente

Salutations, Mr. Robertson of CIS 5371. The Florida Society of Math and Cryptography is proud to present you with an small exam for qualification into our society. The key for passing is studying. Cryptography is rigorous and only those with patience in themselves pass. We have an exam PO Box in Tallahassee. But please submit by 12/12.

Un caso reciente

Salutations, Mr. Robertson of CIS 5371. The Florida Society of Math and Cryptography is proud to present you with an small exam for qualification into our society. The key for passing is studying. Cryptography is rigorous and only those with patience in themselves pass. We have an exam PO Box in Tallahassee. But please submit by 12/12.

The Cryptography exam key is in PO Box 1212.

Cable WWII

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

Cable WWII

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

PERSHING SAILS FROM NY JUNE 1

Cable WWII (otro canal)

APPARENTLY NEUTRAL'S PROTEST IS THROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BY-PRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

Cable WWII (otro canal)

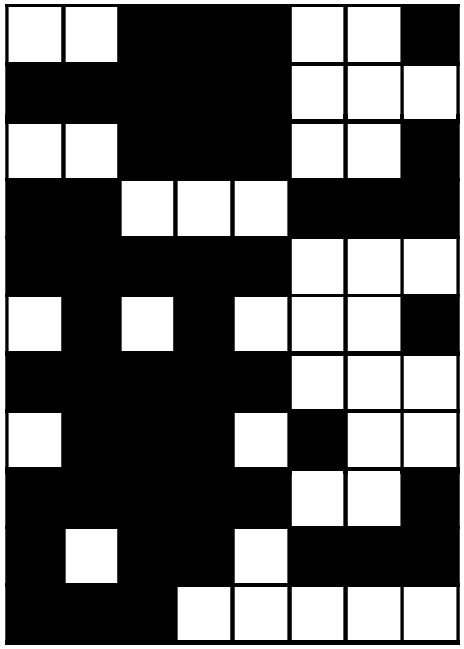
APPARENTLY NEUTRAL'S PROTEST IS THROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BY-PRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

PERSHING SAILS FROM NY JUNE 1

Más complicado

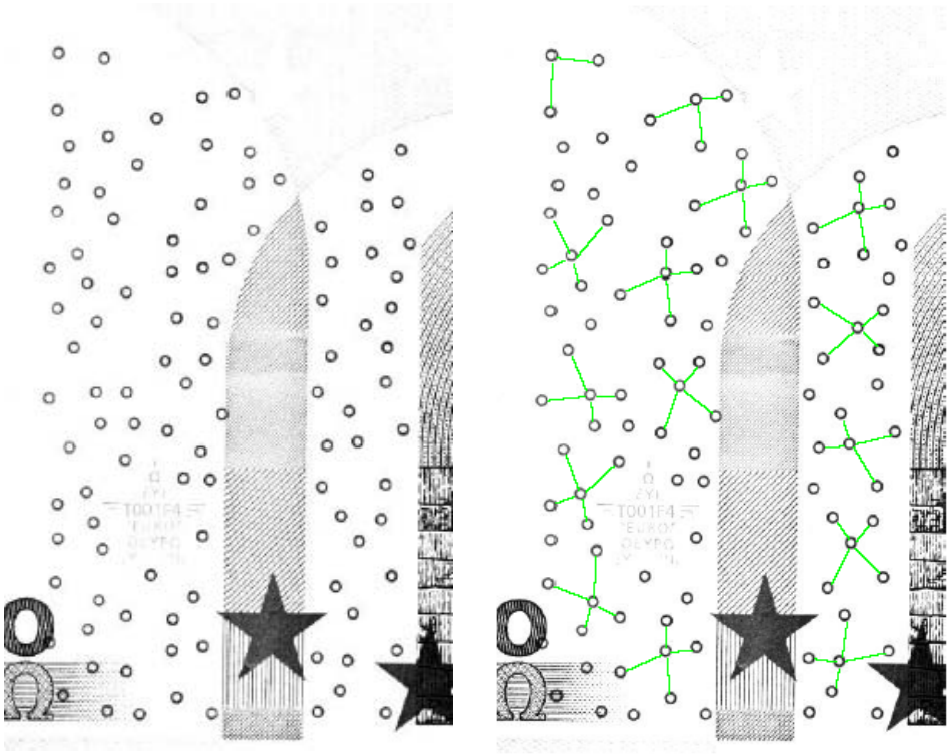
"Debe lograrse que la suma ceda el sitio a la inversa genial o someter hacia debajo algo […]"

D	e	b	e		l	o	g
r	a	r	s	e		q	u
e		l	a		s	u	m
a		c	e	d	a		e
l		s	i	t	i	o	
a		l	a		i	n	v
e	r	s	a		g	e	n
i	a	l		o		s	o
m	e	t	e	r		h	a
c	i	a		d	e	b	a
j	o		a	l	g	o	

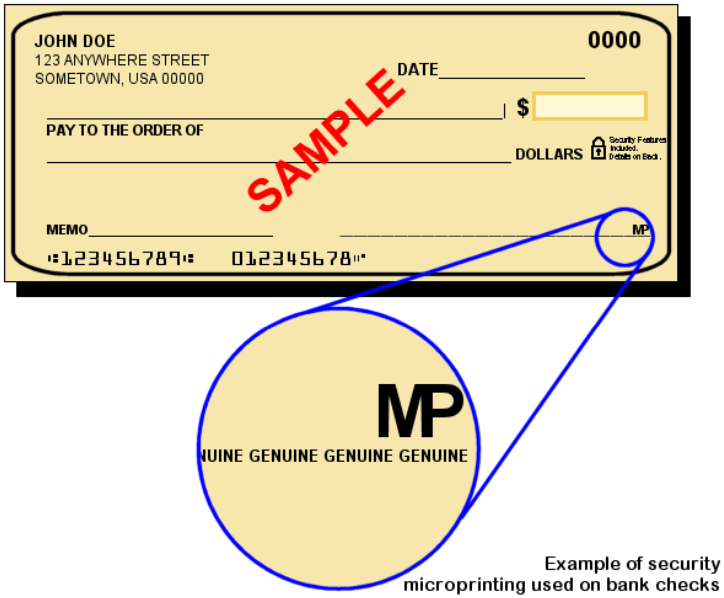


D	e			l	o	
					q	u
e				s	u	
		c	e	d		
				i	o	
a		l		i	n	
				g	e	n
i			o		s	o
					h	
	i			d		
			a	l	g	o

Como medida de seguridad



Como medida de seguridad

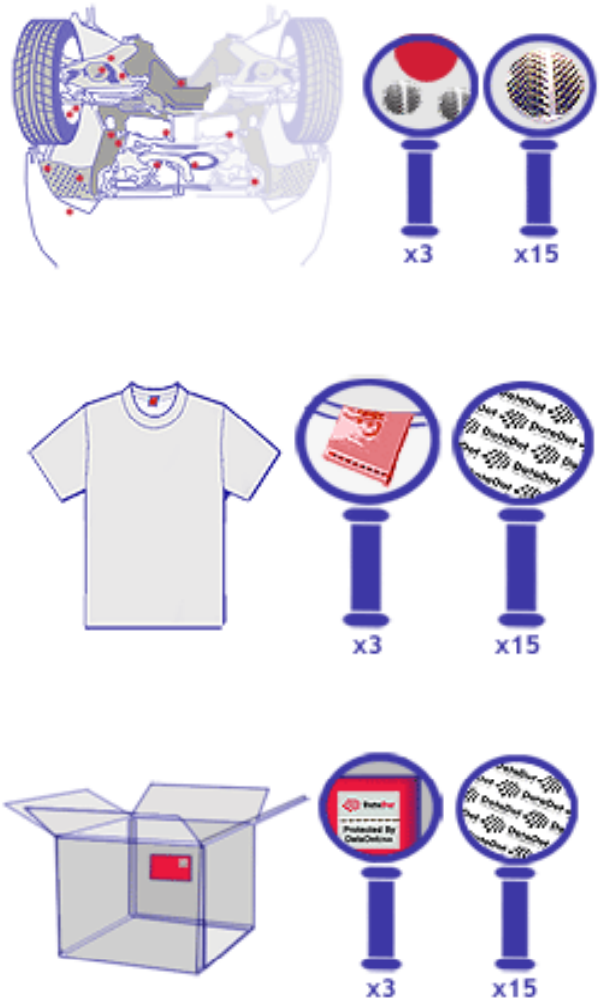


Example of security microprinting used on bank checks

- Otras aplicaciones (tarjetas de crédito/acceso, eDNI, …)

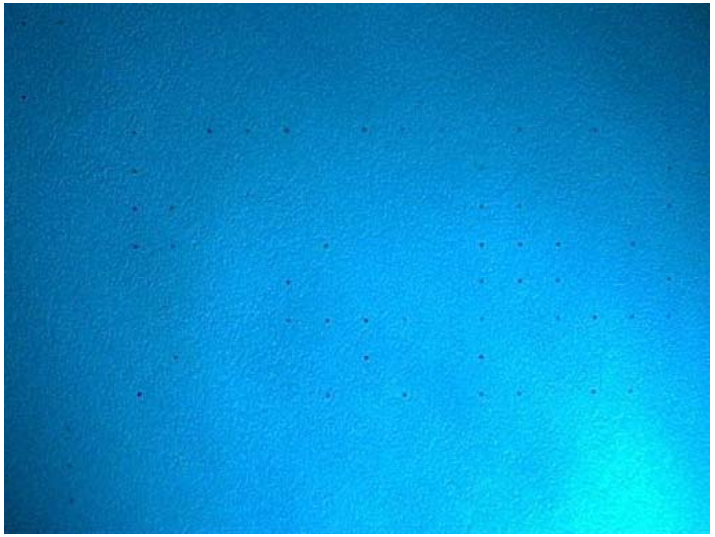
Más aplicaciones

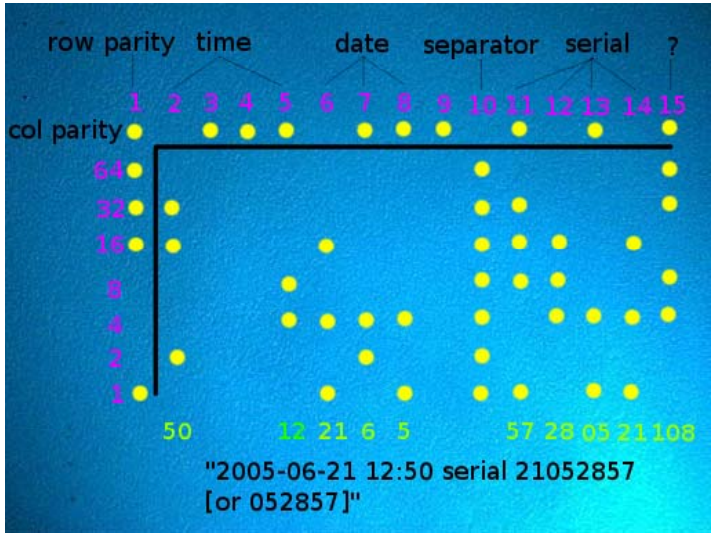
http://www.datadotdna.com/nz

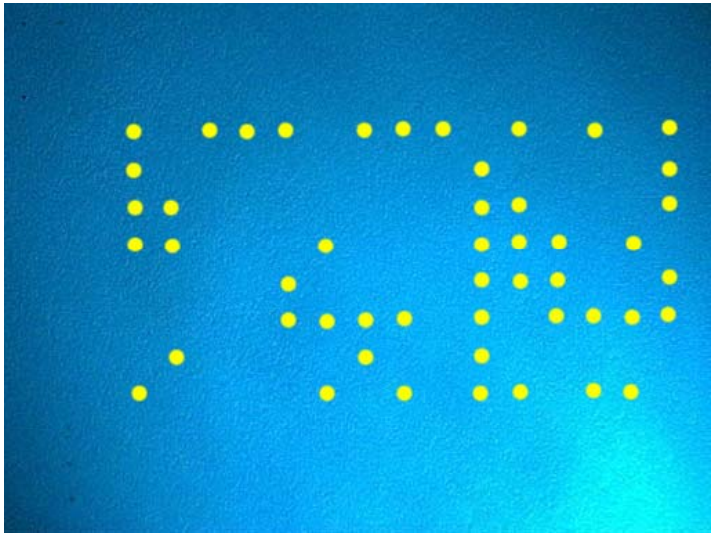


Más recientemente

http://www.eff.org/Privacy/printers/







Agenda

1. Introducción histórica
2. **Esteganografía en la era digital**
3. Esteganálisis
4. Mensajes ocultos e Internet
5. Casos prácticos, trabajos en curso y resultados

Esteganografía moderna

- Esteganografía “clásica”: métodos completamente oscuros
  - Protección basada en desconocer el canal encubierto específico que se está usando.

- Esteganografía moderna: uso de canales digitales:
  - Archivos de texto (inc. páginas web, código fuente, ...)
  - Audio digital
  - Imágenes y vídeo
  - Ejecutables
  - Protocolos de comunicaciones
  - ...

- Cumplimiento de los principios de Kerckhoffs:
  - Su seguridad no debe depender del desconocimiento del algoritmo utilizado (éste debe ser público para ser analizado), sino tan sólo de un secreto o clave.

Modelo

El problema del prisionero (J. Simpson, 1983)

¿Cómo pueden comunicarse dos prisioneros (e.g. para acordar un plan de fuga) si están en celdas separadas y todos los mensajes que intercambian pasan a través de un guardián?

Claves:

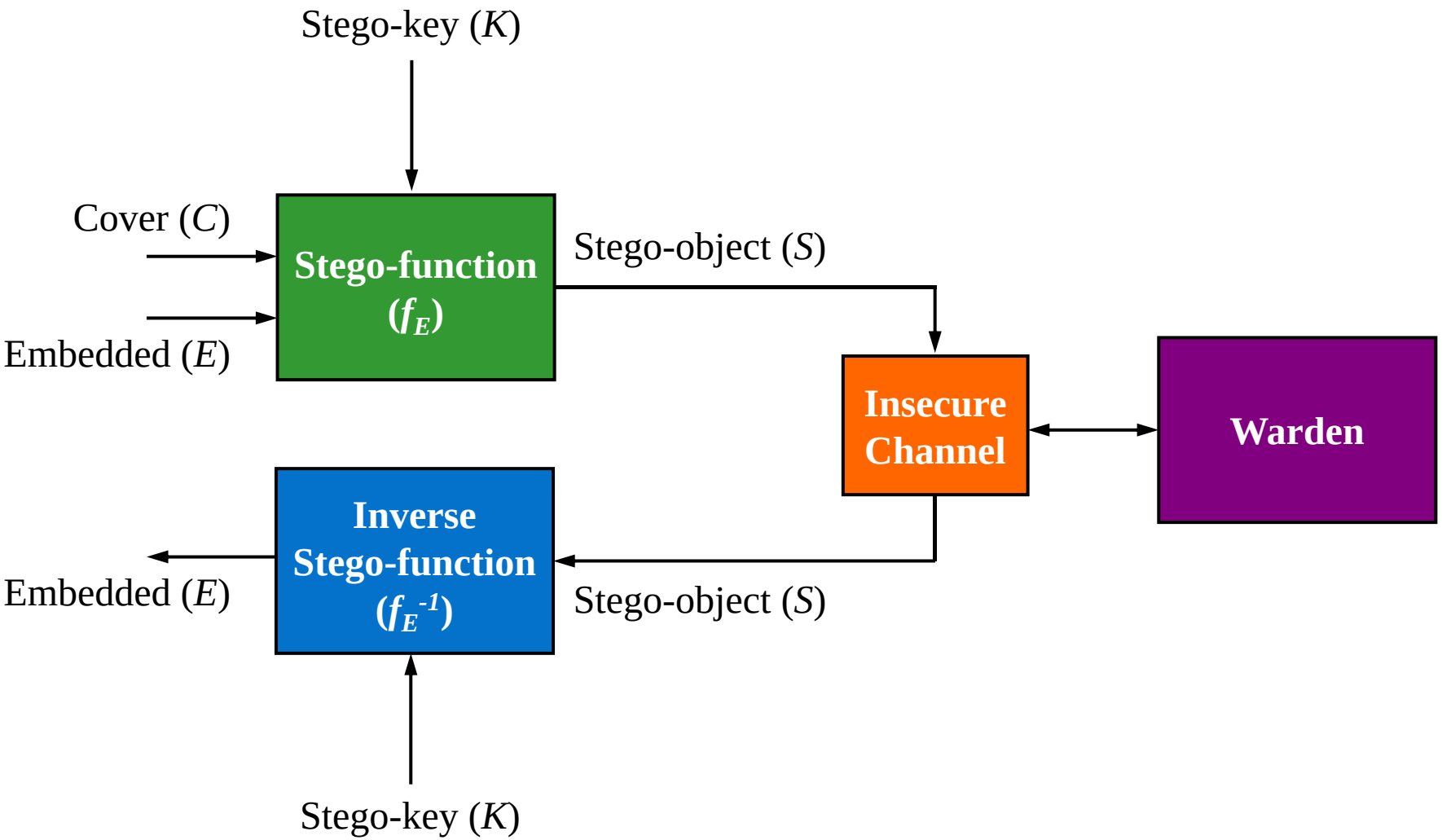
- No se puede usar (sólo) criptografía
- Los mensajes deben parecer inocuos
- El esquema debe estar preacordado entre las partes

Modelo

Definiciones

- **Mensaje oculto:** mensaje a enviar.
- **Objeto encubridor:** objeto en el que el mensaje oculto será insertado.
- **Estegoobjeto:** objeto encubridor conteniendo el mensaje oculto.
- **Guardián:** alguien que monitoriza la comunicación
  - **Pasivo:** sólo lectura
  - **Activo:** puede efectuar modificaciones ligeras
  - **Malicioso:** puede hacer cualquier cosa (no es realista en muchas situaciones)

Estegosistema



Estegosistema

Características

- **Capacidad:** cantidad de información que puede ser ocultada.
- **Seguridad:** dificultad para un tercero de detectar información oculta
- **Robustez:** cantidad de modificaciones que el medio puede soportar antes de que se pierda la información oculta

Esteganografía en texto

- SNOW: http://www.darkside.com.au/snow/
  - Espacios en blanco, compresión y cifrado
- Texto: http://www.ecn.org/crypto/soft/texto.zip
  - Facilitar intercambio de binarios (especialmente cifrados) de forma aparentemente inofensiva
  - Uuencoded/PGP armored<->English
- Texthide: http://www.compris.com/TextHide/en/
  - Comercial, rephrasing, muchos productos asociados
- SpamMimic: http://www.spammimic.com/
  - Gramáticas independientes de contexto

Esteganografía en texto

- NICEText: http://www.ctgi.net/nicetext/index.html
  - Muy bueno, múltiples opciones
- Stegparty: http://www.madchat.org/crypto/stegano/unix/bin2text/stegparty.txt
  - Pequeños cambios en puntuación y escritura
- c2txt2c: http://www.sip.fi/~lm/c2txt2c/
- wbStego99: http://www.wbailer.com/wbstego
- ByteShelter I: www.mazzoft.com/bs1

Esteganografía en imágenes

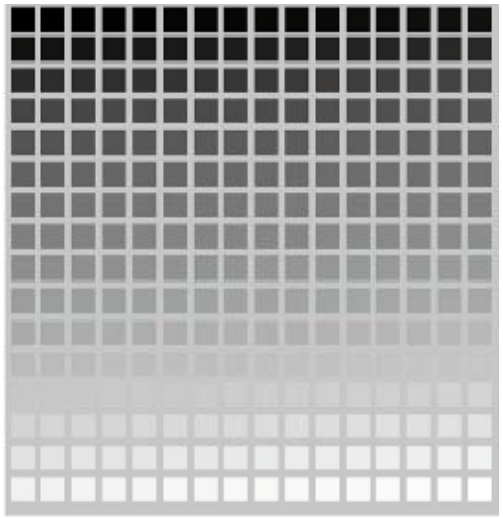
- Imagen = matriz de números

- Cada número (píxel) codifica un color:
  - RGB 24 bits

    00 00 00 00 00 00 00000000 00000000 00000000

    FF FF FF 255 255 255 11111111 11111111 11111111
  - Escala de grises 8 bits:

    número de 0 a 256



Esteganografía en imágenes

Método LSB

- Píxeles originales (9 bytes)

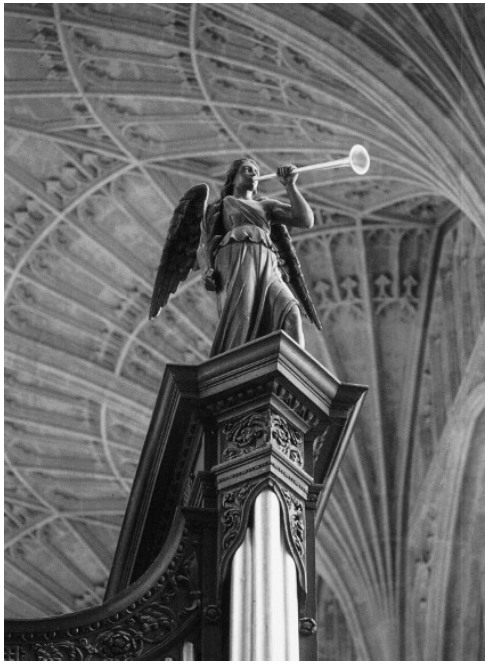
```
(1101101 00100100 101000011)
(0001111 00101101 111011111)
(0000111 00100111 100000111)
```

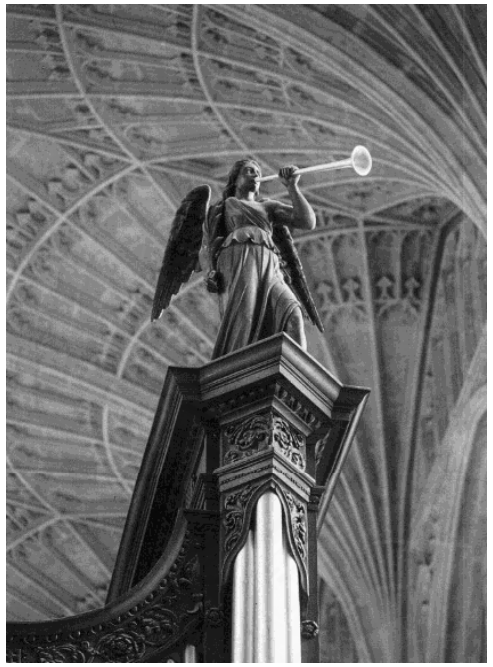
- Mensaje a insertar (8 bits): 'A' (10010111)

- Nuevos píxeles

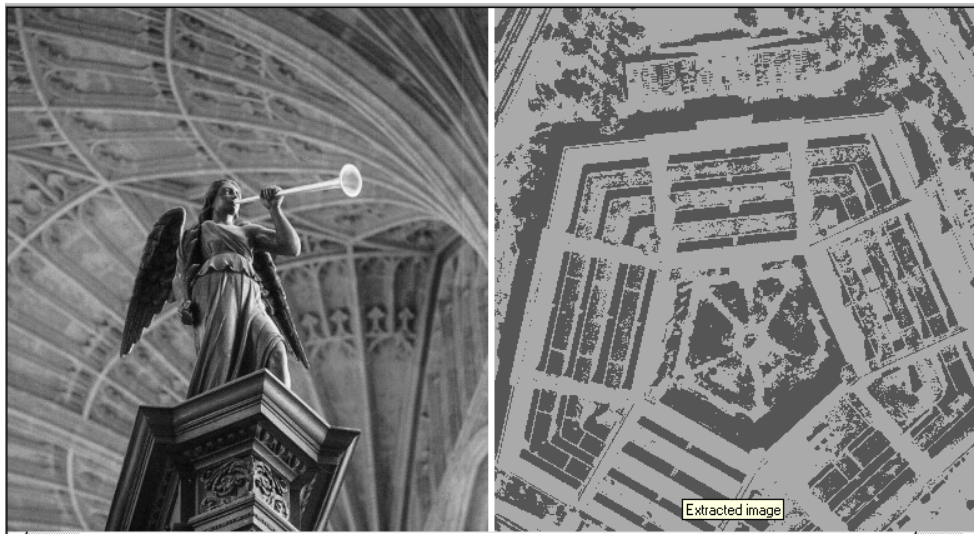
```
(1101101 00100100 101000010)
(0001111 00101100 111011111)
(0000111 00100111 100000111)
```

Esteganografía en imágenes

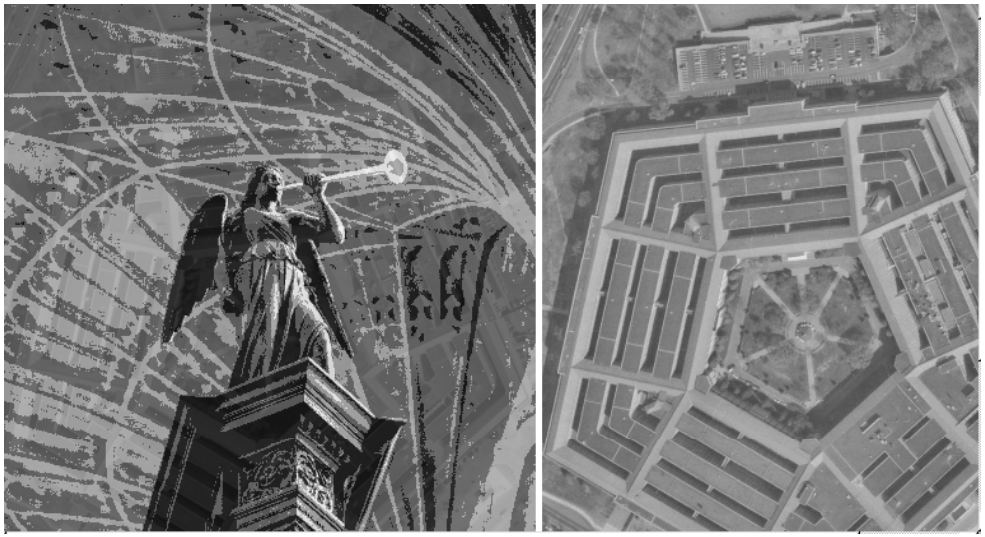

+

=


Esteganografía en imágenes



Uso de 2 bits originales



Uso de 5 bits originales

Esteganografía en imágenes

- La elección de la imagen es muy importante:
  - **Malas candidatas:** Imágenes con poca variabilidad de colores y/o con regiones uniformes.
  - **Buenas candidatas:** Imágenes naturales (no artificiales), con mucha variación de tonos y/o colores.

Esteganografía en imágenes

- Los métodos anteriores carecen de robustez
- La información oculta podría ser eliminada mediante
  - Transcodificación
  - Compresión de la imagen
  - Filtrados
  - Inserción aleatoria de ruido
  - Modificación de propiedades (luminancia, etc.)
- Aplicaciones como el *watermarking* o el *fingerprinting* necesitan esquemas más robustos:
  - La eliminación de las marcas ocultas debe conllevar una pérdida significativa de la calidad de la señal.

Esteganografía en imágenes

- La mayoría de la esteganografía moderna sobre imágenes trabaja en el dominio transformado (DCT, Wavelet, ...)
- Los coeficientes son "manipulados" para insertar la información deseada.
- Ejemplo:
  1. Calcular la DCT de la imagen
  2. Sustituir los coeficientes menores que un cierto valor umbral por bits de la información a ocultar
  3. Calcular DCT^{-1} de la imagen
  4. Almacenar

  (La extracción es trivial aplicando el procedimiento inverso)

Esteganografía en audio

- MP3stego
  - http://www.petitcolas.net/fabien/steganography/mp3stego/
  - También para watermarking
  - Esteganálisis: Análisis estadístico basado en valores del Average Reservoir (99%)

  JC Hernandez, JM Estevez, A Ribagorda, B Ramos, "Blind Steganalysis of MP3stego", *Computers & Security* (en revisión)

- Muchos otros para WAV y otros formatos – no/menos comprimidos

Esteganografía en otros medios

- TCP/IP

  Covert channels

  – http://www.firstmonday.dk/issues/issue2_5/rowland/

  – Cliente y servidor disponibles en C

  Paper TIFS

Esteganografía en otros medios

- Ejecutables: Hydan
  - Redundancia en el conjunto de instrucciones. Se definen conjuntos funcionalmente equivalentes de inst. y se usan unos u otros.
  - También watermarking & traitor tracing
    http://www.crazyboy.com/hydan/

Original code			*Encoding 00*		
83 e8 30	sub	%eax, $0x30	83 c0 d0	add	%eax, $-0x30
83 f8 36	cmp	%eax, $0x36	83 f8 36	cmp	%eax, $0x36
77 e5	ja	$-27	77 e5	ja	$-27
83 c0 08	add	%eax, $0x8	83 c0 08	add	%eax, $0x8
89 04 24	mov	%eax, [%esp]	89 04 24	mov	%eax, [%esp]
Encoding 01			*Encoding 11*		
83 c0 d0	add	%eax, $-0x30	83 e8 30	sub	%eax, $0x30
83 f8 36	cmp	%eax, $0x36	83 f8 36	cmp	%eax, $0x36
77 e5	ja	$-27	77 e5	ja	$-27
83 e8 f8	sub	%eax, $-0x8	83 e8 f8	sub	%eax, $-0x8
89 04 24	mov	%eax, [%esp]	89 04 24	mov	%eax, [%esp]

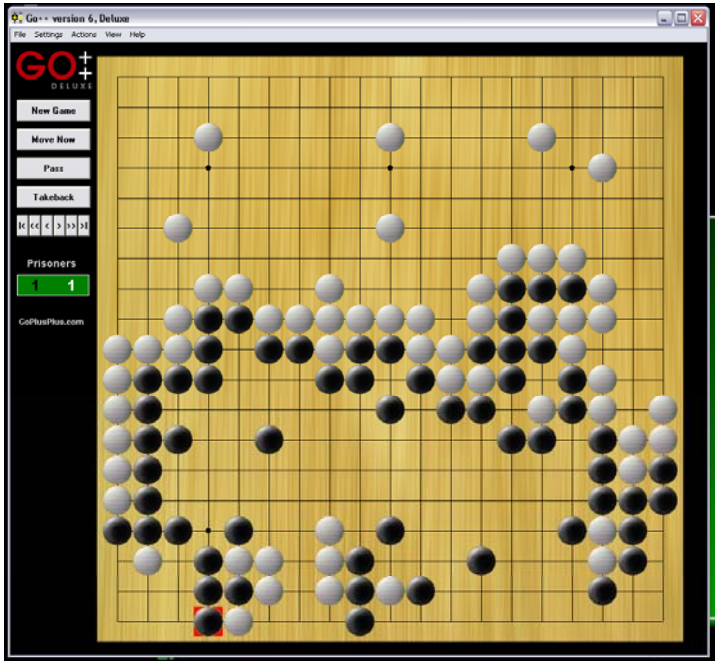
Esteganografía en otros medios

- Espacio en disco y estructuras del FS
  - Diskhide
    ftp://ftp.bke.hu/pub/mirrors/sac/security/diskhide.zip
  - Magic Folders (MF)
    http://www.pc-magic.com
  - StegFS y plausible deniability
- Wrapster
  - Cuando Napster sólo permitía compartir ficheros mp3s
  - http://wrapster.softonic.com/ie/10042

Esteganografía en otros medios

JC Hernandez, I. Blasco, JM Estevez, A Ribagorda, “Steganography in games: A general methodology and its application to the game of Go”, *Computers & Security*, 25(2006):64-71.

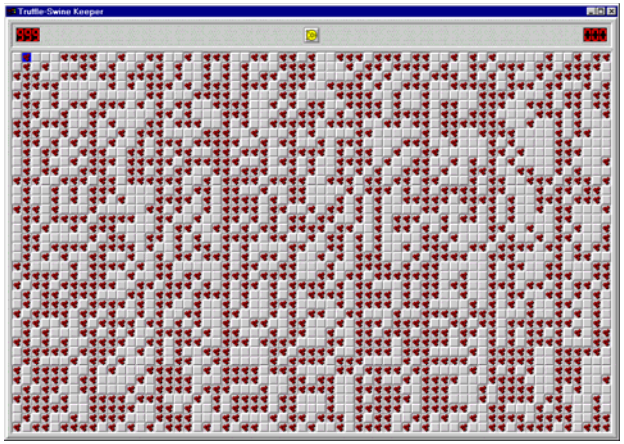
http://www.sourceforge.net/projects/stegogo



Esteganografía en otros medios

Esteganografía en otros medios

$m = b_1 b_2 \cdots b_n$



b_1 b_2

10010110 10010100 1011010 · · · 1101
01101101001001001110101 · · · 1000
01110011010101011100100 · · · 0010
. . . . . .
10010110000100100101100 · · · 1000

```
/*      efdtt.c     Author:  Charles M. Hannum <root@ihack.net>              */
/*      Thanks to Phil Carmody <fatphil@asdf.org> for additional tweaks.     */
/*      Length:  434 bytes (excluding unnecessary newlines)                  */
/*      Usage is:  cat title-key scrambled.vob | efdtt >clear.vob            */

#define m(i)(x[i]^s[i+84])
unsigned char x[5],y,s[2048];main(n){for(read(0,x,5);read(0,s,n=2048);write(1,s
,n))if(s[y=s[13]%8+20]/16%4==1){int i=m(1)17^256+m(0)8,k=m(2)0,j=m(4)17^m(3)9^k
*2-k%8^8,a=0,c=26;for(s[y]-=16;--c;j*=2)a=a*2^i&1,i=i/2^j&1<<24;for(j=127;++j<n
;c=c>y)c+=y=i^i/8^i>>4^i>>12,i=i>>8^y<<17,a^=a>>14,y=a^a*8^a<<6,a=a>>8^y<<9,k=s
[j],k="7Wo~'G_\216"[k&7]+2^"cr3sfw6v;*k+>/n."[k>>4]*2^k*257/8,s[j]=k^(k&k*2&34)
*6^c+~y;}}
```

Algunas herramientas esteganográficas

EzStego	online.securityfocus.com/tools/586/scoreit/
F5	wwwrn.inf.tu-dresden.de/~westfeld/f5.html
Hide and Seek v4.1	ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/
Hide and Seek for Win95	ftp.hacktic.nl/pub/crypto/incoming/
Hide4PGP	www.heinz-repp.onlinehome.de/Hide4PGP.htm
Jpeg-Jsteg	ftp://ftp.funet.fi/pub/crypt/steganography/
Mandelsteg	ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/
MP3Stego	www.cl.cam.ac.uk/~fapp2/steganography/mp3stego/
OutGuess	www.outguess.org/download.php
Steganos	www.steganos.com/en/
S-Tools v4	members.tripod.com/steganography/stego/s-tools4.html
White Noice Storm	ftp://ftp.esua.berkeley.edu/pub/cypherpunks/steganography/

Lista más extensa en http://www.jjtc.com/Steganography/toolmatrix.htm

Agenda

1. Introducción histórica
2. Esteganografía en la era digital
3. **Esteganálisis**
4. Mensajes ocultos e Internet
5. Casos prácticos, trabajos en curso y resultados

Esteganálisis

- Detectar la existencia de comunicaciones que pretendan pasar por ocultas e, idealmente, recuperar su contenido.
- Es a la esteganografía lo que el criptoanálisis a la criptografía.
- Idea básica:

  La esteganografía es *invasiva*, i.e. deja huellas en el medio utilizado como transporte

Esteganálisis

Esquema general de la esteganografía

1. Identificación de bits redundantes en el medio encubierto (los que pueden ser modificados sin degradar considerablemente su calidad de forma detectable).

2. Seleccionar un subconjunto de los bits redundantes para ser reemplazados por los del mensaje secreto.

- La modificación de estos bits suele cambiar las propiedades estadísticas/entrópicas del medio encubierto.
- Gran número de técnicas esteganalíticas se basan en la detección de estos cambios.

ENT: http://www.fourmilab.ch/random/

Algunos procedimientos

- Tests estadísticos
  - Detectar modificaciones esteganográficas mediante la observación de desviaciones respecto a la *norma* de algunas propiedades estadísticas.
  - E.g. en general, la entropía aumenta.

- Este simple modelo ya presenta limitaciones importantes:
  - Falsos positivos al procesar gran cantidad de contenidos
  - Dificultad en la elección de la norma
  - Posibilidad de utilizar, tras el proceso de ocultamiento, técnicas adicionales para *acercar* a la norma el estegoobjeto
  - En general, muy dependientes del tamaño del mensaje oculto
  - Muy dependientes del medio (diferente cantidad de redundancia intrínseca)

Algunos procedimientos

- Ideas adicionales:
  - Al embeber información cifrada de forma criptológicamente segura, ésta se comporta como una secuencia aleatoria de bits, lo que provoca, en general:
    - Aumento de la entropía
    - Coeficiente de correlación bajo
    - Baja la diferencia entre la frecuencia de los colores (imágenes)
    - Bajan las diferencias entre los coeficientes DCT
    - Aumenta el número de parejas de colores *muy similares* adyacentes
  - Estos fenómenos pueden medirse cuantitativamente (e.g. mediante un test chi-cuadrado)

Algunos procedimientos

- Cada algoritmo esteganográfico opera de una forma concreta
- Analizando muchos casos, pueden encontrarse patrones específicos de herramientas concretas
- Se puede llegar a detectar, no sólo la existencia de contenidos ocultos, sino también con qué herramienta se ocultaron y cuánta información hay oculta

Agenda

1. Introducción histórica
2. Esteganografía en la era digital
3. Esteganálisis
4. **Mensajes ocultos e Internet**
5. Casos prácticos, trabajos en curso y resultados

Mensajes ocultos e Internet

- Experiencia de Niels Provost y Peter Honeyman (UMi, 2001)
- Motivación: artículo sobre AlQaeda y la esteganografía mediante imágenes de EBay y grupos de USENet
  - http://www.usatoday.com/tech/columnist/2001/12/19/maney.htm
- Desarrollaron un marco para la detección de contenidos ocultos (inicialmente, sólo en imágenes):
  - Descarga automática de imágenes: *crawl*
  - Análisis (distinguidor): *stegdetect*
  - Rotura distribuida de las sospechosas: *stegbreak* + librerías
- Analizaron 2.000.000 de imágenes de EBay y 1.000.000 más de grupos de noticias de USENet

Mensajes ocultos e Internet

- *stegdetect* es capaz de detectar los patrones correspondientes a:
  - *JSteg* y *JSeg-Shell*
  - *JPHide*
  - *Outguess*

- Muchas limitaciones:
  - Hay programas de no detecta (e.g. *Outguess 0.2* y otros muchos)
  - Ratio de FP alta para algunos algoritmos
  - Ratio de FN alta

Mensajes ocultos e Internet

Resultado del experimento: NADA

¿Por qué no se detectó nada? (*Explicación de los autores*)

- "No hay un uso significativo de la esteganografía en Internet
- La investigación se realizó sobre fuentes en las que normalmente no se encuentran contenidos ocultos
- La gente que usa esteganografía:
  - No utilizan los sistemas que *stegdetect* detecta
  - Los usuarios de sistemas esteganográficos escogen claves excelentes"

Parcialmente ciertas.

Mensajes ocultos e Internet

Además: herramientas de burlado del esteganálisis

- StirMark
  - Image Watermarking Robustness Test
  - http://www.cl.cam.ac.uk/~mgk25/stirmark.html
  - Distorsionar watermarks – múltiples técnicas
  - Muy útil para diversas aplicaciones no académicas
  - http://digitalphotography.weblogsinc.com/2005/07/29/steganography-with-flickr/

- Mosaïc attack
  - Contra los spiders que buscan información con copyright en la web
  - http://www.petitcolas.net/fabien/watermarking/2mosaic/index.html
  - 2Mosaic: incluso webmasters para evitar image download

Agenda

1. Introducción histórica
2. Esteganografía en la era digital
3. Esteganálisis
4. Mensajes ocultos e Internet
5. **Casos prácticos, trabajos en curso y resultados**

Casos prácticos, trabajos en curso y resultados

Algunos resultados científicos

- "Beware of the security software".
  Information Systems Security Journal, Jan. 2004.

- "Blind Steganalysis of MP3stego".
  Computers & Security (en revisión)

- “Steganography in games: A general methodology and its application to the game of Go”
  Computers & Security, 25(2006):64-71.
  (Código fuente en http://sourceforge.net/projects/stegogo/)

- "On the distinguishability of distance-bounded permutations in ordered channels"
  IEEE Transactions on Information Forensics and Security (en revisión)

Casos prácticos, trabajos en curso y resultados

Proyectos

- Herramienta esteganalítica: *Under the carpet*
  - Versión preliminar: http://sourceforge.net/projects/underthecarpet/
  - Útil tanto para esteganálisis como para análisis forense.

- Ampliación en curso:
  - Esteganálisis de Hydan
  - Esteganálisis textual (SNOW, wbstego, etc.)
  - Esteganálisis gramatical (mimicry y variantes)

Casos prácticos, trabajos en curso y resultados

Proyectos

- Análisis de contenidos ocultos en Internet
  - En la línea del trabajo de Provost y Honeyman: medir hasta qué punto la esteganografía está siendo utilizada en Internet.
  - Hasta el momento, herramienta limitada:
    - Esteganografía textual
    - Web "pública"
  - Objetivos:
    - Esteganálisis más exhaustivo (e.g. *Under the carpet*)
    - Búsqueda más exhaustiva/guiada en la red

Preguntas

Arturo Ribagorda Garnacho
Juan M. Estévez-Tapiador
Julio César Hernández Castro
{arturo, jestevez, jcesar}@inf.uc3m.es

Universidad Carlos III de Madrid