



# Steganography

## Art of Covert Communications

Kibbee D. Streetman

(865) 748-8947



## Presentation Goal

Purpose is to recognize the potential threat posed by hidden text or images.

### Objectives

- Define steganography.
- Identify historical examples of steganography.
- Identify uses for steganography.
- Recognize a biliteral cipher.
- Identify additional ways of hiding information (other than biliteral ciphers).
- Recognize the potential uses of steganography in illegal activities.



# STEGANOGRAPHY

## Hidden Writing

- Steganos – Greek meaning “hidden”
- Graphie – Greek meaning “to write”
- Steganography – the art and science of hidden writing or covert communication

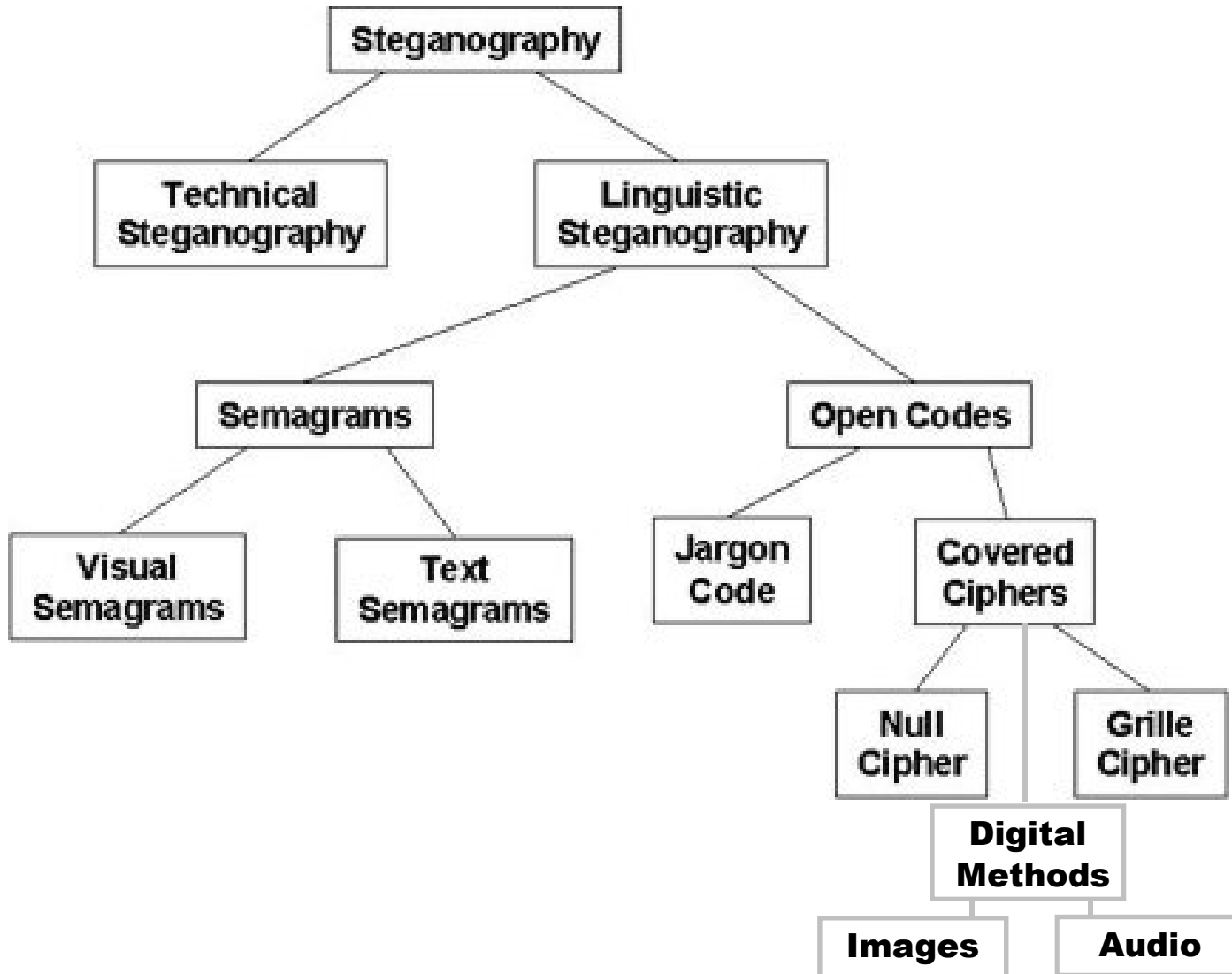
Steganography seeks to conceal the very presence of any information. May be used in conjunction with cryptography.





# STEGANOGRAPHY

## Taxonomy





# STEGANOGRAPHY

## History and Examples

- It's Greek to me (500 B.C.)
  - Shaved heads
  - Stuffed rabbits
  - Wax tablets
- Middle Ages (1400-1600 A.D.)
  - Biliteral ciphers
  - Invisible inks
  - Grilles



# STEGANOGRAPHY

## Biliteral Ciphers

- Proposed by Sir Francis Bacon (1500s)
- Uses two type fonts with slight differences
- Uses a binary number representation for message encoding

A = 00001

B = 00010

-----

I/J = 01001

-----

Z = 11001



# STEGANOGRAPHY

## Bilateral Ciphers

A	00001	O	01110
B	00010	P	01111
C	00011	Q	10000
D	00100	R	10001
E	00101	S	10010
F	00110	T	10011
G	00111	U	10100
H	01000	V	10101
I/J	01001	W	10110
K	01010	X	10111
L	01011	Y	11000
M	01100	Z	11001
N	01101		



## STEGANOGRAPHY Bilateral Cipher Example

*DOE cyber assets must be protected in compliance with the requirements of applicable national laws which require DOE to provide information security protection commensurate with their importance to DOE missions and programs.*

DOE Order 205.1, Sec.4.





# STEGANOGRAPHY

## Bilateral Ciphers

P 01111 <i>DOECY</i>	U 10100 <i>BERAS</i>	T 10011 <i>SETSM</i>	T 10011 <i>USTBE</i>	H 01000 <i>PROTE</i>	E 00101 <i>CTEDI</i>	C 00011 <i>NCOMP</i>
A 00001 <i>LIANC</i>	S 10010 <i>EWITH</i>	H 01000 <i>THERE</i>	I 01001 <i>QUIRE</i>	N 01101 <i>MENTS</i>	A 00001 <i>OFAPP</i>	C 00011 <i>LICAB</i>
O 01110 <i>LENAT</i>	K 01010 <i>IONAL</i>	E 00101 <i>LAWSW</i>	C 00011 <i>HICHR</i>	A 00001 <i>EQUIR</i>	N 01101 <i>EDOET</i>	A 00001 <i>OPROV</i>
T 10011 <i>IDEIN</i>	T 10011 <i>FORMA</i>	H 01000 <i>TIONS</i>	E 00101 <i>ECURI</i>	D 00100 <i>TYPRO</i>	R 10001 <i>TECTI</i>	O 01110 <i>ONCOM</i>
P 01111 <i>MENSU</i>	S 10010 <i>RATEW</i>	I 01001 <i>IHTTH</i>	T 10011 <i>EIRIM</i>	E 00101 <i>PORTA</i>	B 00010 <i>NCE TO</i>	O 01110 <i>DOEMI</i>
R 10001 <i>SSION</i>	I 01001 <i>SANDP</i>	S 10010 <i>ROGRA</i>	MS.	DOE Order 205.1, Sec. 4.		



# STEGANOGRAPHY

## History and Examples

- World Wars (1900s)
  - Null ciphers
  - Microdots
  - Spread spectrum
- Computer Age (20<sup>th</sup> Century)
  - Image hiding
  - Audio hiding
  - Text hiding
  - Order hiding





# STEGANOGRAPHY

## Null Ciphers

The real message is concealed within a cover message.

For example:

“Apparently neutral’s protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.”

(WWI German spy message)

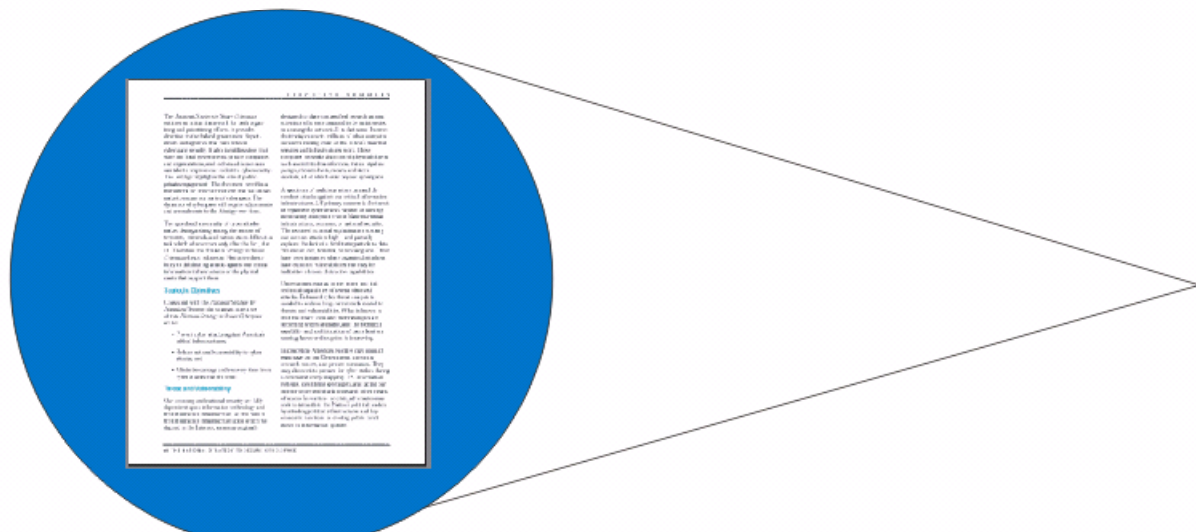




# STEGANOGRAPHY

## Microdots

- Message is photographed using “reverse microscope”
- Photographic dot is cut out with a hypodermic needle
- Place microdot on a period in a cover message

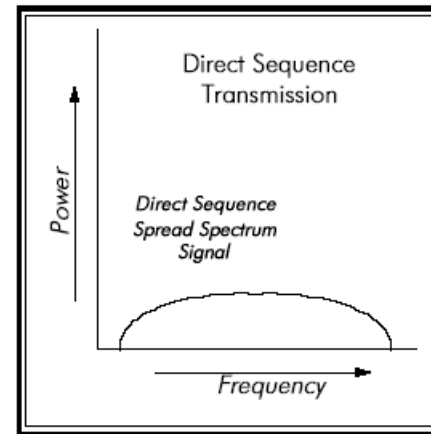
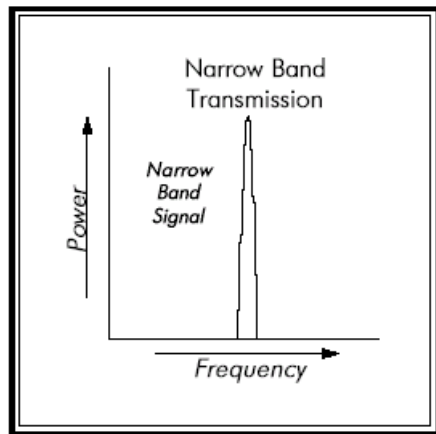




# STEGANOGRAPHY

## Spread Spectrum

- Ordinary radio transmission is at a discrete frequency
- Spread spectrum disperses signal over a broad range

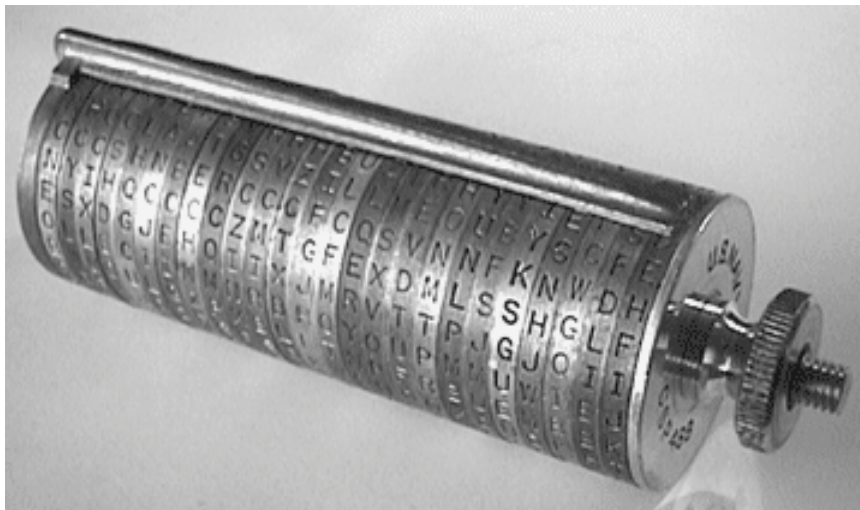




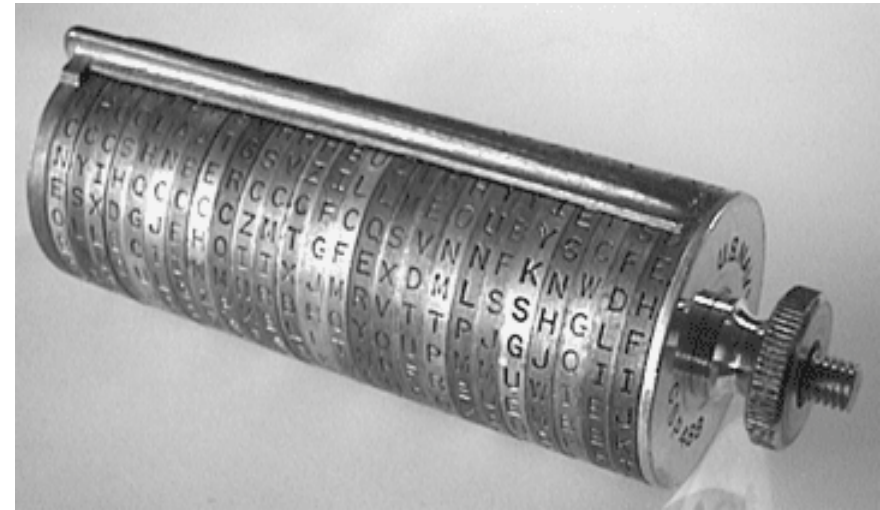
# STEGANOGRAPHY

## Hiding Information in Pictures

- Uses least significant bits in bmp or gif images
- Modifies transform coefficients in jpg images
- Can store large amounts of information
- Modified images are visually indistinguishable



A



B



## HIDING EXAMPLE

- CONSIDER HIDING “G” IN THIS FILE
- 10010101      00001101      11001001      10010110
- 00001111      11001011      10011111      00010000
  
- “G” in ASCII = 01000111
  
- NEW FILE
- 10010100      00001101      11001000      10010110
- 00001110      11001011      10011111      00010001
  
- ONLY HALF OF THE LEAST BITS CHANGED. THE NUMERIC
- VALUE OF EACH BYTE CHANGED VERY LITTLE



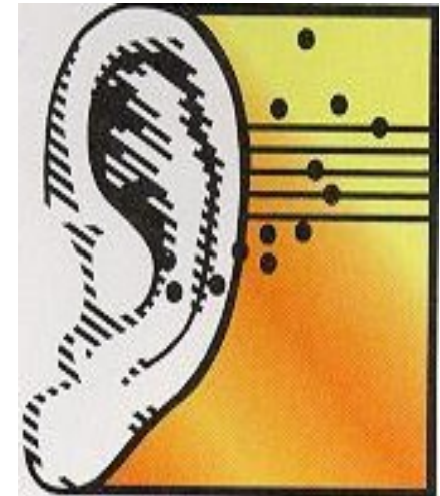


# STEGANOGRAPHY

## Hiding Information in Audio



- Uses least significant bits in wav file
- Limited storage capacity in cover file (600 bytes in 10K file)
- Audio file sounds no different to average person
- Can use frequencies above human hearing (15-20,000 cps)







# STEGANOGRAPHY

## Hiding Information in Texts

- Creates covert message as part of the process
- Uses a “Grammar Tree” to build the covert message
- Very limited message capacity
- [www.spammimic.com](http://www.spammimic.com) has a good demo

The screenshot shows the spam mimic website interface. At the top is the logo for 'spam mimic' in a stylized font. Below the logo is a horizontal line. The main text reads: 'First time here? ... Read the explanation. Hope you're using the secure connection. NEW'. Below this, there are two links: 'Encode' and 'Decode', each followed by a description: 'Encode - Turn a short message into spam' and 'Decode - Turn spam back into the original message'. At the bottom, there is a navigation menu with links for 'home', 'encode', 'decode', 'explanation', 'credits', 'faq & feedback', 'terms', and 'Français'. A copyright notice at the very bottom reads: 'Copyright © 2000-2002 spammimic.com, All rights reserved'.



# STEGANOGRAPHY

## “SPAM” Example

Dear Friend ; We know you are interested in receiving cutting-edge news . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1916 , Title 7 , Section 302 ! Do NOT confuse us with Internet scam artists . Why work for somebody else when you can become rich within 26 months . Have you ever noticed most everyone has a cellphone and most everyone has a cellphone ! Well, now is your chance to capitalize on this ! We will help you use credit cards on your website & increase customer response by 110% . You can begin at absolutely no cost to you ! But don't believe us . Mrs Simpson of Nebraska tried us and says "My only problem now is where to park all my cars" ! We are a BBB member in good standing . We beseech you - act now ! Sign up a friend and you get half off . Cheers . Dear Friend , This letter was specially selected to be sent to you ! If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our mailing list ! This mail is being sent in compliance with Senate bill 1624 ; Title 4 , Section 308 . THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich as few as 86 days ! Have you ever noticed people are much more likely to BUY with a credit card than cash plus most everyone has a cellphone . Well, now is your chance to capitalize on this . We will help you deliver goods right to the customer's doorstep & turn your business into an E-BUSINESS . The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Ms Anderson of Hawaii tried us and says "I was skeptical but it worked for me" ! We are licensed to operate in all states ! We BESEECH you - act now ! Sign up a friend and you get half off ! God Bless .



# STEGANOGRAPHY

## Hiding Information in the Order of Things

- N objects can be rearranged  $N!$  ways

$$5! = 120$$

$$10! = 3,628,800$$

$$40! = 8 \times 10^{47}$$

- N objects can be used to carry  $\log_2 N!$  Bits

$$\log_2 5! = \text{approx } 7 \text{ bits}$$

$$\log_2 10! = \text{approx } 22 \text{ bits}$$

$$\log_2 40! = \text{approx } 160 \text{ bits}$$



# STEGANOGRAPHY

## Available Software

- S-Tools
  - Freeware program for Windows
  - Hides data in GIF or .bmp images or in .wav sound files
  - Provides encryption and compression options
- Hide and Seek
  - Freeware programs for DOS
  - Hides data in GIF image files
  - File to be hidden must be no longer than 19k
- J-Steg
  - Freeware program for DOS
  - Hides data in JPEG images
  - Must convert images prior to hiding data
- Digital Picture Envelope
  - Freeware program for Windows
  - Hides data in .bmp files
  - Hides large amount of data without changing file size



**See also:** <http://www.stegoarchive.com>



# STEGANOGRAPHY

## Steganalysis – Seeing the Unseen

Steganalysis is the process of discovering and rendering useless any forms of covert communications.

- Currently more of an *art* than a *science*
- Easier to detect than to reveal
- File headers sometime contain clues
- Some steganographic methods are more vulnerable than others
  - Image Domain (bit-wise manipulation)
  - Transform Domain (algorithm and transform manipulation)



# STEGANOGRAPHY

## Steganalysis – Seeing the Unseen

- Image domain methods
  - Bit-wise methods
  - Characterized as simple systems
  - Image formats are lossless
  - Data can be directly manipulated and recovered
- Examples
  - StegoDos
  - S-Tools
  - Steganos



# STEGANOGRAPHY

## Steganalysis – Seeing the Unseen

- Transform domain methods
  - Algorithm and image transform methods
  - Typically more robust systems
  - Independent of image format
  - Detection is more difficult
- Example
  - Jpeg-Jsteg



# STEGANOGRAPHY

## Uses for Steganography

- Covert communications
  - Privacy
  - Espionage
  - Terrorism
  - Criminal activities
- Intellectual property protection
  - Digital watermarks
  - Digital signatures





# STEGANOGRAPHY Tool of Terrorist?

02/05/2001 - Updated 05:17 PM ET

## Terror groups hide behind Web encryption

By Jack Kelley, USA TODAY

WASHINGTON — Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lie the encrypted blueprints of the next terrorist attack against the United States or its allies. It sounds farfetched, but U.S. officials and experts say it's the latest method of communication being used by Osama bin Laden and his associates to outfox law enforcement. Bin Laden, indicted in the bombing in 1998 of two U.S. embassies in East Africa, and others are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites, U.S. and foreign officials say.



AP

U.S. officials say Osama bin Laden is posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites.



## STEGANOGRAPHY Tool of Terrorist?

- Results from tests by Niels Provos (University of Michigan)
  - Examined 2 million images from eBay
  - Examined 1 million images from USENET archive
  - Found 20,000 “suspicious” images
  - Dictionary attack with 1,800,000 entry dictionary
- Bottom line:
  - Not any hidden messages were found (2001)



# STEGANOGRAPHY

## Conclusions

- Steganography transmits secrets through innocuous covers
- Used in combination with cryptography
- Post 9/11 interest has been exponential
  - 1995 web search produced less than a dozen hits
  - 1996 search gave about 500 hits
  - 1998 search produced over 1,000 hits
  - 2003 search yielded 70,400 hits
  - 2004 Google search found 104,000 references
  - 2005 Google search found 230,000 references
  - 2006 Google search found 1,560,000 references



## Steganography Conclusions - Addendum

- Google now provides a fine-grained search capability that groups steganography searches by categories such as software, tools, and programs. This results in some multiple hits, nevertheless, it is clear that interest in steganography is increasing. For example in 2010:
  - Steganography had 436,000 hits
  - Steganography software had 190,000 hits
  - Steganography programs had 1,190,000 hits
  - Steganography tools had 1,580,000 hits
  - Steganography detection had 785,000 hits



# STEGANOGRAPHY

## Conclusions

- Can be used for both legitimate or criminal purposes
  - Covert communications
  - Watermarks and signatures
  - Terrorism, espionage and pornography
- Steganography software is freely available
- Steganography is difficult to detect and more difficult, if not impossible, to reveal
- Study by Purdue University in 2007 found some evidence of criminal use of steganography
- FBI has arrested 11 suspected Russian agents who were using steganography to spy in the US (June 2010)



## Russian Spies Using Steganography

**Busted Alleged Russian Spies Used Steganography To Conceal Communications. 'Deep-cover' Russian intelligence agents hid electronic messages behind computer images (Jun 29, 2010 )**

**Kelly Jackson Higgins-*DarkReading***

- In a case that smacks of a Cold War spy novel, the FBI has arrested 11 suspected Russian spies who for years had blended into day-to-day American life in the suburbs and cities. Aside from hiding their true identities and posing as legitimate American citizens, the suspects also masked their communications with their intelligence agency back home in Moscow, using an oft-forgotten form of stealth communication -- **steganography**.
- According to U.S. Department of Justice legal filings, the defendants used a **steganography tool**, one that is not available commercially, to conceal their electronic communiques with Russian officials in the so-called SVR, a Russian Federation foreign intelligence body.



# STEGANOGRAPHY

## References and Resources

- Information hiding homepage
  - <http://www.cl.cam.ac.uk/~fapp2/steganography/>
- Information and software
  - <http://www.stegoarchive.com>
- Detection software and links
  - <http://www.outguess.org/detection.php>
- Steganography links
  - <http://www.wayner.org/node/13>
- Annotated bibliography
  - [http:// www.cl.cam.ac.uk/~fapp2/steganography/bibliography/](http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/)



# STEGANOGRAPHY

## References and Resources

### ■ Books

- Disappearing Cryptography 3rd edition, by Peter Wayner
- Information Hiding Techniques for Steganography and Digital Watermarking, edited by Stefan Katzenbeisser and Fabien A. P. Petitcolas
- Hiding in Plain Sight: Steganography and the Art of Covert Communication, by Eric Cole
- Information Hiding : Steganography and Watermarking - Attacks and Countermeasures, by Neil F. Johnson, Zoran Duric, Sushil Jajodia





# STEGANOGRAPHY

## References and Resources

- Books
  - Investigators Guide to Steganography, by Gregory Kipper
  
  - Digital Watermarking and Steganography, by Ingemar Cox, Matthew Miller, Jeffrey Bloom, and Jessica Fredrick
  
- In addition,  
Amazon.com lists 175 books with *Steganography* in the title.
  
- Also check  
Steganography Analysis and Research Center (SARC)  
[www.sarc-wv.com](http://www.sarc-wv.com)