

James P. Cavanagh

Global Telecom & Security Consultant

Presents

Introduction to Steganography

An Online Briefing for Webtorials
December 2001

[www.
consultant-
registry
.com](http://www.consultant-registry.com)



www.webtorials.com

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

Presenter

James P. Cavanagh

Global Telecommunications Consultant



jcavanagh@consultant-registry.com

[www.
consultant-
registry
.com](http://www.consultant-registry.com)

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

Outline

Introduction to Steganography

- Why is this Important?
- Steganography Definition
- Steganography vs Encryption
- Problem of Steganography
- Applications
- Steganalysis
- Null Cipher Example
- Word Shifting Example
- LSB Modification Example
- Software
- Steganography and Business
- Conclusion



Steganography, like encryption, has been practiced since ancient times

Why is this important?

Introduction to Steganography

While steganography has been used in some form of fashion since ancient times it has become one of the technologies of choice for facilitating global terrorism. CIA Director George Tenet testified before the US Congress in February 2001 that steganography and encryption are the two primary computer means used by Osama Bin Laden to coordinate terrorism.

Definition

Introduction to Steganography

"Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present."

[Markus Kuhn 1995-07-03].

Steganography vs Encryption

Introduction to Steganography

***Encryption* is the practice of systematic information scrambling so that it may be unscrambled later.**

while

***Steganography* is the practice of information hiding.**

Problem of Steganography

Introduction to Steganography

Steganography + Encryption = Big Trouble for Law Enforcement



© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

Applications

Introduction to Steganography

- **Used to Hide Information in Plain View**
 - Under wax on Tablets (Demeratus / Ancient Greece)
 - On Shaved Heads of Messengers
 - Inside of other binary files
- **Three Types of Applications**
 - "Good"
 - "Bad"
 - "Neutral"
 - Your opinion of the categorization may differ

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

"Good" Applications

Introduction to Steganography

- **Digital "Watermarking"**
 - Identification of Source of Material
 - Establish Ownership
 - Often Identify Licensee
- **Copy Protection Schemes**
 - Reduce Software Piracy
 - Enhance Prosecution Efforts
- **Only Works Against "The Masses"**
- **The Professionals Have Broken All Systems to Date**
- **The Professionals Will Break All Systems in the Future**

"Bad" Applications

Introduction to Steganography

- **Pornographers (Hide/Transfer Illegal Pornography)**
- **Terrorists***
- **Others wishing to hide information in plain view**

***It is believed that Osama Bin Laden may have used steganography to hide plans for the attack on World Trade Center and Pentagon. It has been proven that his co-conspirators did.**

“Neutral” Applications

Introduction to Steganography

- **Free Speech Advocates (For any reason they want)**
- **Researchers**
 - To develop new steganographic techniques**
 - To unravel existing techniques and find hidden information**
- **Hobbyists / Amateurs**

Applications

Introduction to Steganography

- **“Paper” Methodologies**
- **“Digital” Methodologies**
 - Used on Many Common File Types**
 - GIF
 - BMP
 - MP3
 - WAV
 - JPG
 - Can be virtually undetectable / untraceable**

Steganalysis

Introduction to Steganography

Steganalysis is the process of identifying hidden content.

“Finding files tainted by steganography is akin to looking for a piece of straw in a haystack - forget the needle.”

**- Neil Johnson,
Center for Secure Information Systems**

Null Cipher Example

Introduction to Steganography

Simple Example (null cipher)

Bob: Oh please! End Roger and Tom's indecision over Nana! Oh, Nana!

Tom: Hal is determined, even though he eventually gets under Nana's skin in normal times! His eventual picking at Roger knew no end! Even during a moment amongst people!

Nana: All lies, so often!

Would this sample script make it past the censors?

Null Cipher Example

Introduction to Steganography

Simple Example (null cipher)

Bob: Oh please! End Roger and Tom's indecision over Nana! Oh, Nana!

Tom: Hal is determined, even though he eventually gets under Nana's skin in normal times! His eventual picking at Roger knew no end! Even during a moment amongst people!

Nana: All lies, so often!

Now look at the first letter of each word of dialog for the hidden message.

Word Shifting Example

Introduction to Steganography

Simple Example (word shifting)

He had a heart attack. Living with them was difficult. In the morning, at 8:00 am, he would eat breakfast and leave. No doubt it was he who took out the trash and walked the dog before he went to work.

Sentence One

This text looks safe enough ... doesn't it?

Word Shifting Example

Introduction to Steganography

Simple Example (word shifting)

He had a heart attack . Living with them was difficult. In the morning, at 8:00 am , he would eat breakfast and leave. No doubt it was he who took out the trash and walked the dog before he went to work.

Sentence Two

A small spacing change is made before and after message words.

Word Shifting Example

Introduction to Steganography

Simple Example (word shifting)

He had a heart **attack** . Living with **them** was difficult. **In** **the** morning, at 8:00 am , he would eat breakfast and **leave**. **No** **doubt** it was he who took out the trash and walked the dog before he went to work.

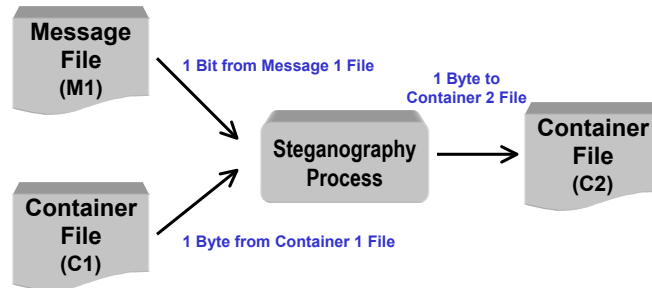
Result

When the two documents are combined, this is the result.

LSB Modification Example

Introduction to Steganography

Third Example (LSB Modification)



© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

LSB Modification Example

Introduction to Steganography

Third Example (LSB Modification)

Steganography
Process

If C1 byte = 00100101 and M1 bit = 1 then resulting C2 byte is unchanged.
(Likewise if both bits are '0' then the C2 byte is unchanged)

If C1 byte = 00100101 and M1 bit = 0 then resulting C2 byte is 00100100.

The difference is very subtle, and is almost undetectable in a MP3 or GIF File.
JPG is not as good for steganography, but some programs do use them.

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

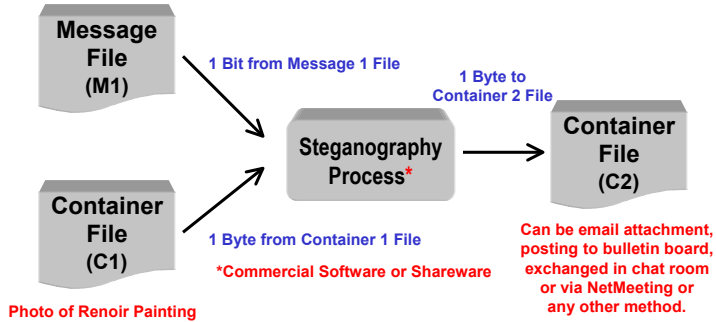
LSB Modification Example

Introduction to Steganography

Third Example (LSB Modification)

The Internet is the modern day equivalent of the "dead drop".
- FBI Agent

Aerial Reconnaissance Photo



Example from Neil Johnson's <http://www.jjtc.com/Steganography/>

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

LSB Modification Example

Introduction to Steganography

Third Example (LSB Modification)



Message File 1

+



Container File 1

=

Example from Neil Johnson's <http://www.jjtc.com/Steganography/>

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

LSB Modification Example

Introduction to Steganography

Third Example (LSB Modification)



Message File 1

+



Container File 1

=



Container File 2

Example from Neil Johnson's <http://www.jjtc.com/Steganography/>

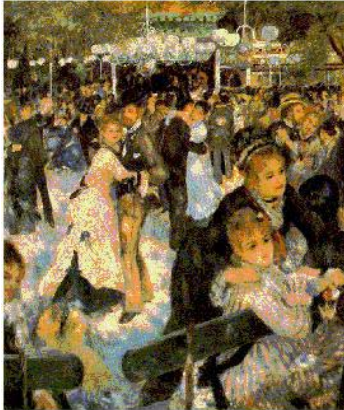
© 2001 James P. Cavanagh, All Rights Reserved

jcavanagh@consultant-registry.com

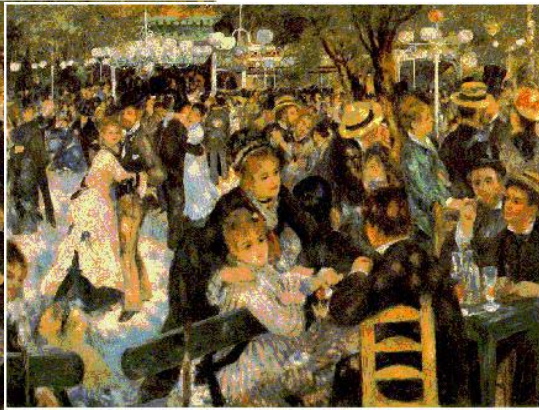
LSB Modification Example

Introduction to Steganography

Third Example (LSB Modification)



Container File 1



Container File 2

Example from Neil Johnson's <http://www.jjtc.com/Steganography/>

© 2001 James P. Cavanagh, All Rights Reserved

jcavanagh@consultant-registry.com

Software

Introduction to Steganography

Software

Commercial

Stealthencrypt

DataMark Technologies (StegMark, StegSafe, StegCom, StegSign)

Others

Freeware / Shareware

Hide and Seek, LSB of GIF Files

StegoDos, Embeds data in LSB of screen images

White Noise Storm, embeds data in LSB of screen images

S-Tools, variety of file types (GIF, WAV, BMP) plus encryption

JPEG-JSTEG4, uses JPG files to hide content

Others

Good information source: <http://stegoarchive.com/>

Steganography and Business

Introduction to Steganography

What Can Business Do to Counter Steganography?

- **Assess the Need/Importance of Multimedia Files**
 - *Does the organization need GIF, JPG, BMP, etc?*
 - *Are these files/attachments needed just internally or externally?*
 - *Filter these file types at the fire wall*
 - *FTP*
 - *eMail*
 - *Other*
- **Check for / delete Inactive User Accounts**
- **Be Aware of Files of Unknown/Questionable Origin**
 - *Your system may be used as an intermediate "drop"*
 - **Perform a file audit**
 - **Question / Challenge users on unusual files**

Conclusion

Introduction to Steganography

Used to Hide Information in Plain View

There are "good", "bad" and "neutral" applications

Used on Many Common File Types

Complimentary to Cryptography

Used for Copy protection as well as sending terrorist messages

A MAJOR problem for Law Enforcement

Take Action:

Don't be an unknowing accomplice to terrorism

Check your own file systems

Decide which multimedia file types are needed

Block / delete / question unusual files



© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

The End

Thanks for Watching!

For additional information or
to arrange for a steganography
or network or infrastructure security
presentation or consultation
for your organization please contact:

Karen Kaye
+1.770.263.7675
kkaye@consultant-registry.com

Additional steganography and security information is available at:
www.consultant-registry.com

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com