STEGANOGRAPHY

Sergey Grabkovsky

WHICH OF THESE HAS A HIDDEN MESSAGE?

- Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

- We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.

- Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

ALL OF THEM

- Fi**s**hing fr**e**shwater be**n**ds an**d** sa**l**twater co**a**sts re**w**ards an**y**one fe**e**ling st**r**essed. Re**s**ourceful an**g**lers us**u**ally fi**n**d ma**s**terful le**a**pers fu**n** an**d** ad**m**it sw**o**rdfish ra**n**k ov**e**rwhelming an**y**day.

  - Send lawyers, guns, and money.

- We_*explor*e new steganographic and cryptographic algorithms and techniques throughout_*the* world to produce_*wid*e variety and security in the electronic_*web* called the Internet.

  - Explore the world wide web

- A**p**parently n**e**utral's p**r**otest i**s** t**h**oroughly d**i**scounted a**n**d i**g**nored. I**s**man h**a**rd h**i**t. B**l**ockade i**s**sue a**f**fects p**r**etext f**o**r e**m**bargo o**n** b**y**products, e**j**ecting s**u**ets a**n**d v**e**getable o**i**ls.

  - Pershing sails from N.Y June I

A DEFINITION

- Steganography is the art of hiding a message within a cover.

- The purpose of steganography is so that if anyone looks, they won't know that anything is hidden.

- You should only be able to extract a message if you know how it was hidden.

A LITTLE HISTORY

- One of the first documents describing steganography comes from Greece, from the Histories of Herodotus.

- In ancient Greece text was written on wax covered tablets.

- In one story Demeratus wanted to notify Sparta that Xerxes intended to invade Greece.

- He scraped the wax off of the tablets, and wrote the message on the underlying wood.

A LITTLE (MORE) HISTORY

- Invisible Ink
  - Used as recently as World War II. Almost exclusively at the beginning.
  - Common sources include: milk, vinegar, fruit juices, and urine.
  - Improved with the development of technology. Inks that can react to various chemicals were developed.
  - Some messages have to be "developed" much like photographs.

DIGITAL STEGANOGRAPHY

- Encodes messages in digital files.
- Formats that could potentially contain hidden messages:
  - AVI, GIF, JPG, BMP, EXE, .NET Assemblies, MIDI files, ZIP, and WAV.
- Commonly messages are encoded in either audio or image files.

A SIMPLE TECHNIQUE

- Append data that is to be hidden to the end of the file.

- Format-independent

- Quick & dirty

- Doesn't affect the file content.

A SIMPLE TECHNIQUE

- Append data that is to be hidden to the end of the file.

- Format-independent
- Quick & dirty
- Doesn't affect the file content.

Or does it?

A PROBLEM

- Consider MP3 files.
- They have ID tags at the end of the file.
- Appending extra information to MP3's would corrupt this information.

A DETECTION

- This method is very easy to detect if the file format has its size in the header, like BMP's.

- This method is still easy to detect if the size is not in the header, since the message has to store its own size somehow at the end of the file.

A CHOICE OF FORMATS

- Image and audio files are an obvious choice.
- Let's focus on images.

A REPRESENTATION OF IMAGES

- How are images represented in memory?
  - RGB: A byte for red, a byte for green, and a byte for blue.
  - Depending on the underlying system, it might be ordered BGR or RGB.

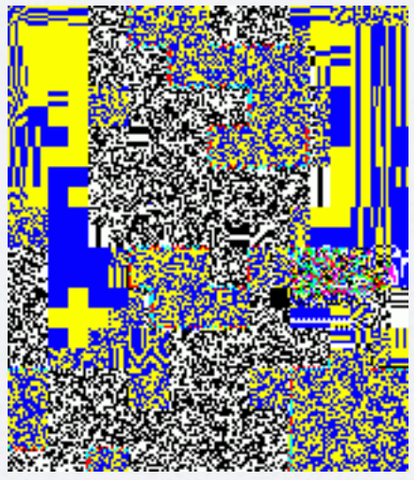
A BETTER METHOD

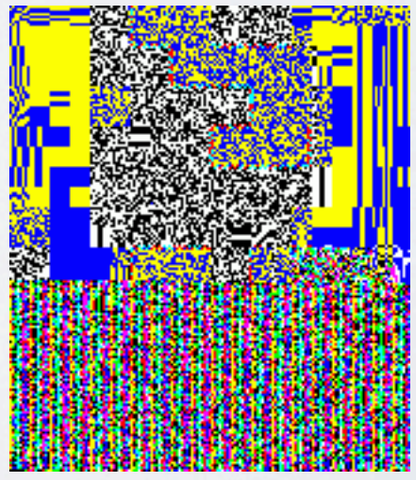
- Change the least significant bit to the data's bit.
- Example: we are hiding the letter 'a'. Its ASCII representation is 97, its binary would be 01100001.
- If we were using the naive approach, we would store the data in a linear manner. Starting from the first byte, we would change the least significant bit to 0, change the LSB of the second byte to 1, and so on.

A REALITY

- This method is very insecure, as it leaves a clear pattern and changes statistical properties of the image.

- Need to change stride either pseudo-randomly or depending on a password.





AN INTERESTING IDEA

- Another way to improve this technique is to have the software that is encoding the hidden message change the statistical properties of the image.

- This way there is no statistical difference between an image with a hidden message and a normal image.

A VARIATION

- This technique can be extended to image files with a palette, such as GIF.

- Images with a palette only store color information in the palette entries. That way they can use 1 byte per pixel instead of 3.

- We would simply have to change the least significant bit of each palette entry to comply with our encoding.

A PALETTE PROBLEM

- This introduces many duplicate entries into the palette.

A VARIATION AGAIN

- This technique could also be extended to JPEG images.
- The conversion process to a JPEG is a bit long, but here's the basics:
  - An image is converted to JPEG's color space.
  - Color subsampling - average out multiple adjacent pixels to one wherever possible.
  - Discrete Cosine Transform - represent 8x8 parts as coefficients.
  - Quantization - smooth out the curve.
  - Reordering - reorder the pixels into a zig-zag order.
  - Lossless Compression - Use Run Length Encoding and Differential Pulse Code Modulation to lower the size.

A TRICK OF QUANTIZATION

- With JPEG's, we don't actually store the message in the image data.
- Instead, we store the message in the quantization step.
- In order to store data, we use LSB again.
- Store in coefficients.

AN UNFORTUNATE TURN OF EVENTS

- Unfortunately, all of the methods described above are detectable.

- There is currently no steganographically secure way to store a hidden message.

- Even changing the statistics of the image isn't secure.

- A program called *stegdetect* supports detection of all existing techniques on images, as well as automated detection of new steganographic messages.

A CONCLUSION

- Modern steganography techniques are nowhere near steganographically secure.

- Any existing method can be detected (at least for images).

- It is not ready for use for anything extremely important.

- With any steganographic technique, data should be encrypted first.

A REFERENCE PAGE

- Neil F Johnson. Steganography. Technical Report. November 1995.
- Gary C Kessler. An Overview of Steganography for the Computer Forensics Examiner. Forensic Science Communications. July 2004.
- Guillermito. http://www.guillermito2.net/stegano/. 2002-2004.
- Corinna John. http://www.binary-universe.net/.
- Niels Provos. http://www.outguess.org/. September 2004.
- Niels Provos. http://www.outguess.org/detection.php. September 2004.