Colorado State University
Department of Computer Science

The Art of Hiding in Plain Sight

Addy Moran, Erin Doan

Introduction

Steganography is defined as hiding a message or piece of data in an object in such a way that its existence is not apparent. Although steganography has been around for around 2500 years, it is still very relevant today (Judge 4).

In the past, the main use of steganography was for passing secret messages in wartimes. One example is the use of tattooing a message on a messenger's head. Once the hair grew back the soldier could be sent onto the recipient (Judge 5). This technique was popular because it did not rely on the messenger's memory and was hidden from the eye if the messenger ran into adversaries.

Other examples include the use of invisible ink and microdots, which were developed by Germans in WWII (Judge 6). In modern times, steganography has greatly expanded with advancement of technology.

Applications and Examples

Steganography is most commonly known for ensuring privacy of hidden data. Other applications include: protection of data, authentication of data, and copyrighting data. Protection of data is needed in instances like Intellectual Property where the data isn't sensitive in nature, but the sender would like to keep it from the public so that it is not stolen.

An example of authentication is for placing marker so that the recipient can verify who sent the message. An example of the use of authentication was by British Prime Minister Margaret Thatcher. She had word processors programmed to encode the identity of authors using word spacing, so that she could trace leaks of sensitive documents (Judge 14).

Modern uses are divided into two categories: Textual and Digital. Examples of textual and digital steganography used today can be found in studies by Ibrahim (103) and Judge (7-20).

Textual

- Word Spacing
- Line Spacing
- Semantic methods
- Syntactic methods
- Feature Coding
- Use of Special Characters

Digital

- Phonograph Record Steganography
- PhotoTiled images
- ASCII art
- Still Image Steganography
  - text, executables, mp3
- DNA Steganography

Hiding a Message in an Image

Original Image

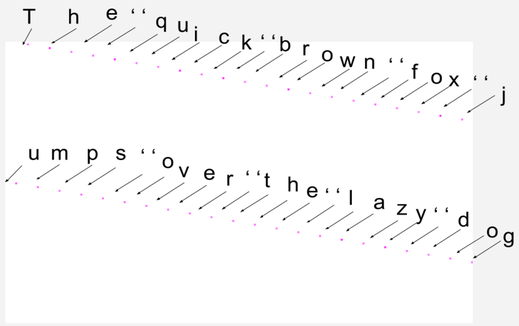
Hidden Message: 41.872509, -87.624713.23-03-18.13:15.

Adjusted Green Pixel Values

Adjusted Blue Pixel Values

Adjusted Red Pixel Values

Algorithm



Hidden Message: The quick brown fox jumps over the lazy dog
Message Size: 43

To Encrypt:

1. Compute how often a pixel needs to be changed. This is based off of the image size and the message size. (floor(image size / message size))
2. Set either the red, green, or blue RGB value to the ASCII value of the letter.

To Decrypt:

Assumptions:

- You know the message size
- You know which color channel was changed (red, green, or blue)

1. Compute how often a pixel was changed. (floor(image size / message size))
2. Convert ASCII value of the red, green, or blue value to corresponding character (for example convert 97 to 'a').

Quiz QR

QR to website

Discussion

- When hiding messages the following can make an impact:
  - image size
  - message size
- You can encrypt by changing different color channels (red, green, and blue values) and the alpha channels (transparency).
- JPEG and GIF images are lossy so when encrypting you need to save the new image in a lossless format (ie. PNG)

Conclusion

Steganography has been in use for thousands of years, however, in the current technological era hiding messages has gotten easier but detecting them has gotten more difficult. Due to the many different ways to hide a message such as changing images, video, or audio files, cryptography isn't the only form of sending secret messages effectively.

References

Judge, James C. Steganography: past, present, future. No. UCRL-ID-151879. Lawrence Livermore National Lab., CA (US), 2001.

Ibrahim, Rosziati, and Teoh Suk Kuan. "Steganography algorithm to hide secret message inside an image." arXiv preprint arXiv:1112.2809 (2011).