AN OVERVIEW ON HIDING AND DETECTING STEGO-DATA IN VIDEO STREAMS

Alexandre Miguel Ferreira
May 11, 2015

University of Amsterdam
AGENDA

Research Question

Background

Literature Study

Analysis

Conclusion
RESEARCH QUESTION
Which methods are available for (real-time) steganalysis on a video-stream and how can these be prevented?

- Which are the steganography methods available for video-stream?
- Which are the steganalysis methods available for video-stream?
- How can steganography be prevented on a video-stream?
BACKGROUND
What is Steganography?

The art and science of hiding communication

Originates from the ancient Greek

· *steganos* (covered)
· *graphein* (writing)

What is Steganography? History

Earliest recordings from the Greek historian Herodotus (440 BC)

- Prisoners scalp tattooed to deliver secret messages
- Wooden tables carved before applying its wax surface

On the XV century Johannes Trithemius wrote about

- Invisible inks, Coding techniques for text, Hidden messages in music

Used to send hidden messages during World War II

- Null ciphers, Image substitution, Microdots
Steganography vs Watermarking

Similar to Steganography

- On Steganography the data embedded should be covert and undetectable
- On Watermarking it does not matter, however ...
- ... any attempt to remove it should result in significant degradation of the quality of the carrier file

Commonly used to help trace the origin of files
**Steganography vs Cryptography**

Different from Steganography

- Cryptography scrambles a message so it cannot be understood
- Steganography hides the message so it cannot be seen

Both are used to protect confidential information ...

- ... therefore often confused
What is Steganalysis?

Security of a steganographic system is defined by its strength to defeat detection.

Practice of detecting the presence of messages that have been hidden using steganography.

Ideally the content of the hidden message is also determined.
What is Steganalysis? Types of Attacks

Steganalysis attacks can be active or passive

- On active attacks a steganalyst can manipulate the data
- On passive attack the steganalyst is only able to analyze the information without changing it

Attacks used by steganalysts to detect steganography on files can be:

- Visual Attacks
- Structural Attacks
- Statistical Attacks
The simplest form of attacking a steganographic system
Based on the visual analysis of the image

- Noticeable differences indicate that the image probably carries hidden information

If the carrier is not known this attacks becomes very hard
Types of Attacks - Structural Attacks

Analysis of known properties of the algorithms used to hide information

- Analysed further if found any properties of these algorithms

Outputs a lot of false positives

- Used to highlight images which show signs of possible embedding

Depends a lot on if the carrier file is known
Types of Attacks - Statistical Attacks

Statistical analysis done using mathematical formulas

· Much more effective than the Visual or Structural attacks

It is successful even without knowing the carrier file ...

· ... however it fails to determine the hidden data’s size
LITERATURE STUDY
Big variety of techniques used to camouflage information:

- **Injection**
  - By far the simplest steganographic technique
  - Hides a message in parts of a file that are “ignored” by the application

- **Substitution**
  - Identify areas of a file of least relevance
  - Replace this data with the hidden information
  - Does not modify the size of the container file ...
    - ... therefore the steganographic capacity of the file is limited
Steganographic Techniques (2)

List Significant Bits Manipulation

- LSB Sequential Insertion
- LSB Pseudo Random Insertion
  - Pseudo Random Number Generator (PRNG) is used to randomly hide the secret bits of the message into the LSB of the carrier file

Source: http://lvee.org/uploads/abstract_file/file/111/2.png
**Transform Domain**

Generally used on compressed container files, such as JPEG or MPEG

- **Discrete Cosine Transform**
  - Algorithm works by using quantization
    - Rounding values of least important parts (not noticeable by the human eye)
  - Image is split into smaller areas to be transformed via DCT
    - Quantization on the frequencies is then applied
    - This is the stage where the secret message is injected
  - Finally the image is compressed
    - No impact on the integrity of the secret message

- **Discrete Wavelet Transform**
  - Makes it possible to raise the level of robustness of the information being hidden
  - If the threshold is too high the stego-file has detectable differences
Compression

Regards reducing and removing redundant video data ...

- ... with no undesirable effects on the visual quality

Lossless Compression

- Every single bit of data that was originally in the file remains after the file is uncompressed

Lossy Compression

- Discards the points which are difficult to identify by the human eye
- Resulting image is similar to the original image
- Generally used on video and sound
**Video Container Format**

Contains the various components of a video

- Such as the stream of images or the sound

Source: [https://msdn.microsoft.com/](https://msdn.microsoft.com/)
ANALYSIS
Create some stego-videos

- *OppenPuff*

Perform known attacks

- Visual Attack
- Statistical Attack
- Structural Attack
The users to hide information in a wide range of carrier formats

- 3gp, Mp4, Mpeg II, etc.

Possible to hide data in more than a single carrier file

2 important factors were taken into consideration

- Embedding efficiency
- Embedding payload
Based on Niels Provos paper *Defending Against Statistical Steganalysis*

- which states "steganalysis resistance and performance are incompatible trade-offs"

Performed by

- Reproducing both the original and stego videos
- Comparing and analysing individual frames from the original and from the stego-file
Program *ent* used to perform this attack

- **Entropy** - Information density of the contents of the file
- **Chi-square Test**
  - greater than 99% and less than 1% - almost surely not random
  - between 99% and 95% or between 1% and 5% - considered suspect
  - between 90% and 95% or between 5% and 10% - not sure to be suspect
- **Arithmetic Mean** - Result of the sum of all the bytes in the file divided by the its length
- **Monte Carlo Value for Pi** - If the sequence is close to random, the value will approach the correct value of $\pi$
- **Serial Correlation Coefficient** - Calculates how much each byte in the file depends on the previous byte
Values are very similar and do not raise any suspicious upon the stego-file

<table>
<thead>
<tr>
<th></th>
<th>Original</th>
<th>Stego</th>
<th>Expected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entropy</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Chi-square Test</td>
<td>0.01%</td>
<td>0.01%</td>
<td>N/A</td>
</tr>
<tr>
<td>Arithmetic Mean</td>
<td>127.0006</td>
<td>126.5138</td>
<td>127.5</td>
</tr>
<tr>
<td>Monte Carlo</td>
<td>3.025822076</td>
<td>3.010476826</td>
<td>π</td>
</tr>
<tr>
<td>Value for Pi</td>
<td>0.147440</td>
<td>0.154106</td>
<td>0.0</td>
</tr>
<tr>
<td>Serial Correlation</td>
<td>Coefficient</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Based on the comparison of the original file and the stego-file

- hexdump of both files was analyzed
Last four bytes of the header are changed

- These bytes are an offset pointing to the beginning of the header that belongs to the MOOV box ...
- ... which defines the timescale, duration, display characteristics of the movie, as well as sub-boxes containing information for each track in the movie

hexdump of both files is different since some bytes were inserted outside this box
Pattern followed throughout the stego-file, outside the MOOV box
Although it could not be proved ...

- ... these bytes might be related to the size of the file being hidden
- ... as well as the password(s) used to encrypt the message

Assumption is made based on Niels Provos paper

- Stated that "32 state bits are hidden, 16 bits for a seed and 16 bits for an integer containing the length of the message being hidden"

*Important to notice that the video container format may change, therefore the optimal location of the moov box will be depend on this*
While analysing in detail the MOOV box, it was noticed that the bytes were modified.
Secret information is hidden inside the MOOV box.

Once again it could not be proved ... 

... due to two reasons:

- The fact that the secret information is encrypted
- The use of deniable steganography techniques
Pursuits to make the analysis and/or examination of evidence difficult or impossible to conduct

- Encryption and steganography among the ways

Relies on several weaknesses of the forensic process

- Human element, dependency on tools

There is always the chance of being detected using these techniques

- Resisting to these unpredictable attacks is also possible ...
- ... even when forced to provide a valid password to extract the data
Camouflage based technique

· Even if the steganalyst is able to state that data is being hidden, allows the breaker to convincingly deny that fact

*OpenPuff* implements deniable steganography

· Possible to hide two different messages in the cover file
  · One which contains the sensitive data
  · One which although is plausible to be considered sensitive, the user is willingly to give away

One of the reasons why the statistical attacks are ineffective
CONCLUSION
Techniques used on images and audio can also be applied to videos

- Most common use the spatial domain (LSB) and the frequency domain (DCT)

Statistical analysis can reveal the presence of hidden data

- However it is a difficult process to carry out
- Hidden information tends to be nearly impossible to be detectable

Best way to prevent steganography would be to alter or destroy files which are considered suspicious

- New video compression methods where less redundant bits are available is also a possibility
The attacks performed proved to be insufficient to determine the hidden information

- It would be interesting to assess if the hidden information can be retrieved
Questions?