Extracting Hidden Messages in Steganographic Images

By
Tu-Thach Quach

Presented At
The Digital Forensic Research Conference
DFRWS 2014 USA Denver, CO (Aug 3rd - 6th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http://dfrws.org
Extracting Hidden Messages in Steganographic Images

Tu-Thach Quach

Sandia National Laboratories

DFRWS 2014
August 4, 2014

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL85000.
Simple LSB Steganography

\[
\begin{array}{ccc}
0 & 1 & 1 \\
7 & 8 & 7 \\
7 & 8 & 9 \\
8 & 8 & 9 \\
\end{array}
\]
Simple LSB Steganography

0 1 1

0111

7 8 7
7 8 9
8 8 9
Simple LSB Steganography

\[
\begin{array}{c|c|c}
0 & 1 & 1 \\
\end{array}
\]

0110

\[
\begin{array}{c|c|c}
6 & 8 & 7 \\
7 & 8 & 9 \\
8 & 8 & 9 \\
\end{array}
\]
# Simple LSB Steganography

```
\[ \begin{array}{ccc}
0 & 1 & 1 \\
\end{array} \]
```

```
1000
```

```
\[ \begin{array}{ccc}
8 & 8 & 7 \\
7 & 8 & 9 \\
8 & 8 & 9 \\
\end{array} \]
```
Simple LSB Steganography

\[
\begin{array}{ccc}
0 & 1 & 1 \\
\end{array}
\]

\[
\begin{array}{ccc}
1000 \\
\end{array}
\]

\[
\begin{array}{ccc}
8 & 8 & 7 \\
7 & 8 & 9 \\
8 & 8 & 9 \\
\end{array}
\]
Simple LSB Steganography

```
  0 1 1
0111
  8 7 7
  7 8 9
  8 8 9
```
Simple LSB Steganography

\[
\begin{array}{ccc}
0 & 1 & 1 \\
8 & 7 & 7 \\
7 & 8 & 9 \\
8 & 8 & 9 \\
\end{array}
\]

0111
Simple LSB Steganography

\[
\begin{array}{ccc}
0 & 1 & 1 \\
\hline
8 & 7 & 7 \\
7 & 8 & 9 \\
8 & 8 & 9 \\
\end{array}
\]
Simple LSB Steganography

\[
\begin{array}{ccc}
0 & 1 & 1 \\
8 & 7 & 7 \\
7 & 8 & 9 \\
8 & 8 & 9 \\
\end{array}
\]
Simple LSB Steganography

- Distortion not distributed over image
Simple LSB Steganography

- Distortion not distributed over image
- Message can be extracted
Simple LSB Steganography

Use embedding key to distribute payload over image
Simple LSB Steganography

- Use embedding key to distribute payload over image
- Message can be extracted if embedding key is known (shared by sender and receiver)
Group-Parity Steganography

- Use $k$ pixels to embed a single bit
- First bit: $0 = 8 + 8 \mod 2$
Matrix Embedding

- Use $k$ pixels to embed $q$ bits
- Change at most 1 pixel in each group
Forensic Goal

Extract hidden messages
Forensic Goal

Extract hidden messages

Approaches:

- Embedding key search
Forensic Goal

Extract hidden messages

Approaches:

- Embedding key search
- Payload location
Scenario

![Camera Diagram]
Scenario

C:\Photos
  ImageA.tif
  ImageB.tif
  ...
  ImageZ.tif
Scenario
Residuals

Cover image: \( \mathbf{c} = (c_1, \ldots, c_n) \)

Stego image: \( \mathbf{s} = (s_1, \ldots, s_n) \)
Residuals

Cover image: \( \mathbf{c} = (c_1, \ldots, c_n) \)

Stego image: \( \mathbf{s} = (s_1, \ldots, s_n) \)

Residual \( r_i \) is

\[
 r_i = |c_i - s_i|. 
\]
Payload Location: Simple LSB
Payload Location: Simple LSB

On average: $\log_2 m$ images to locate payload.

---

Payload Location: Group-Parity
Payload Location: Group-Parity
Payload Location: Group-Parity
Payload Location: Group-Parity

On average: $8k^2 \log(km)$ images to locate payload.

Payload Location

No logical information to arrange located payload
No logical information to arrange located payload

Observation:

- Residuals provide logical information if payload size is not fixed
Logical Information

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>1</strong></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Logical Information

```
0 1 0
2 0 0
0 0 0
```
Logical Information
Logical Information

Payload pixels: 2, 4, 9
**Logical Information**

- **Payload pixels:** 2, 4, 9
- **$r_4 > r_2 > r_9$**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>2</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Logical Information

Payload pixels: 2, 4, 9

$r_4 > r_2 > r_9$

Order located payload in descending mean residuals to obtain message
Logical Information

If payload size varies from 1 through $m$:

$$E[R_i] > E[R_j]$$

for all logical payload pixels $i, j$ where $i < j$. 

Logical Information

If payload size varies from 1 through $m$:

$$E[R_i] > E[R_j]$$

for all logical payload pixels $i, j$ where $i < j$.

If payload size is uniformly distributed:

$$E[R_i] = \frac{m + 1 - i}{2m}.$$
No Cover Images

What if C:\Photos deleted?
No Cover Images

What if C: \ Photos deleted?

Approach:

- Estimate cover images
Experiments

- Image set: BOSSbase 9074 grayscale images $512 \times 512$

- Embedding algorithms: simple LSB and group-parity steganography

- Payload size: between 1 and 32 (uniformly distributed)

- Metric: Minimum edit distance

- Cover estimator: Markov random field
Known Cover: Simple LSB Residuals
Known Cover: Group-Parity Residuals
Known Cover: Minimum Edit Distance

<table>
<thead>
<tr>
<th>Images</th>
<th>Simple LSB</th>
<th>Group-Parity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>8.0</td>
<td>9.5</td>
</tr>
<tr>
<td>2000</td>
<td>5.6</td>
<td>4.2</td>
</tr>
<tr>
<td>3000</td>
<td>3.3</td>
<td>2.8</td>
</tr>
<tr>
<td>4000</td>
<td>2.0</td>
<td>1.8</td>
</tr>
<tr>
<td>5000</td>
<td>1.6</td>
<td>1.2</td>
</tr>
<tr>
<td>6000</td>
<td>1.0</td>
<td>0.8</td>
</tr>
<tr>
<td>7000</td>
<td>1.0</td>
<td>0.0</td>
</tr>
<tr>
<td>8000</td>
<td>0.6</td>
<td>0.0</td>
</tr>
<tr>
<td>9000</td>
<td>0.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>
Unknown Cover: Simple LSBR Residuals

![Graph showing Mean residual vs Logical payload pixel]
Unknown Cover: Minimum Edit Distance

<table>
<thead>
<tr>
<th>Images</th>
<th>Replacement</th>
<th>Matching</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>24.7</td>
<td>27.4</td>
</tr>
<tr>
<td>2000</td>
<td>24.7</td>
<td>27.3</td>
</tr>
<tr>
<td>3000</td>
<td>23.8</td>
<td>26.4</td>
</tr>
<tr>
<td>4000</td>
<td>23.3</td>
<td>26.3</td>
</tr>
<tr>
<td>5000</td>
<td>23.3</td>
<td>25.7</td>
</tr>
<tr>
<td>6000</td>
<td>23.0</td>
<td>25.7</td>
</tr>
<tr>
<td>7000</td>
<td>22.3</td>
<td>25.2</td>
</tr>
<tr>
<td>8000</td>
<td>21.9</td>
<td>25.2</td>
</tr>
<tr>
<td>9000</td>
<td>21.8</td>
<td>25.0</td>
</tr>
</tbody>
</table>
Conclusions

- Exposes vulnerability in block-based embedding algorithms
- Many challenges in practice
- May improve with advances in cover estimation
- Image collection may contain several embedding keys
Thank You

tong@sandia.gov