Accommodating Secret Sharing Technique for Personal Remembrance via Steganography

Adnan Gutub & Maimoona Algamdi

Computer Engineering Department, Umm Al-Qura University, Saudi Arabia
Outline

• Introduction
• Secret Sharing
• Challenge: Personal Remembrance
• Solution: Steganography
• Steganography Possibilities
• Performance Study: Security, Robustness, Capacity
• Conclusion
Secret sharing

- divides secret key into shares
- distribute shares
- specified subset of shares can reconstruct back secret key.
Applications of Secret Sharing

- E-Voting Systems
- Opening Vault in Bank
- Wills and Inheritance
- Medical Agreement
Challenge: Personal Remembrance

• The secret sharing scheme generates shares

• How can users remember their shares?
Solution: Steganography

• Hiding in redundant bits

• Image Based Steganography
  • Why ??
Image Steganography Possibilities

• Pixel Indicator Technique for RGB Steganography

• Image Based Steganography Using Truth Table Based on RGB Indicator

• Triple-A: Secure RGB Image Steganography Based on Randomization

• Vibrant Color Image Steganography using Channel Differences and Secret Data Distribution
Steganography Cover Image: Alhambra image

Performance Study:

Security:
Similarly test = Histogram

Robustness:
Distortion test = PSNR

Capacity:
bit per pixel measure
Security:
Similarly test = Histogram
Robustness:
Distortion test = PSNR

<table>
<thead>
<tr>
<th>PSNR</th>
<th>Shares size in bit</th>
<th>Alhambra (68160 pixels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vibrant color image steganography [6]</td>
<td>8-bit Model (25 bit)</td>
<td>86.7857</td>
</tr>
<tr>
<td></td>
<td>20-bit Model (42 bit)</td>
<td>85.1095</td>
</tr>
<tr>
<td>Proposed Model Using Pixel Indicator Technique</td>
<td>8-bit Model (25 bit)</td>
<td>83.6786</td>
</tr>
<tr>
<td></td>
<td>20-bit Model (42 bit)</td>
<td>83.7554</td>
</tr>
<tr>
<td>Pixel Indicator High Capacity Technique [2]</td>
<td>8-bit Model (25 bit)</td>
<td>83.7554</td>
</tr>
<tr>
<td></td>
<td>20-bit Model (42 bit)</td>
<td>82.7247</td>
</tr>
<tr>
<td></td>
<td>20-bit Model (42 bit)</td>
<td>48.8326</td>
</tr>
<tr>
<td>Truth Table Steganography [7]</td>
<td>8-bit Model (25 bit)</td>
<td>85.9225</td>
</tr>
<tr>
<td></td>
<td>20-bit Model (42 bit)</td>
<td>82.7863</td>
</tr>
</tbody>
</table>
Capacity:

<table>
<thead>
<tr>
<th>Method</th>
<th>bpp</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vibrant color image steganography</td>
<td>4.5</td>
<td>22.06%</td>
</tr>
<tr>
<td>Pixel Indicator Technique</td>
<td>11.9</td>
<td>8.3%</td>
</tr>
<tr>
<td>Triple A Steganography</td>
<td>7.30</td>
<td>13.68%</td>
</tr>
<tr>
<td>Truth Table Steganography</td>
<td>16.8</td>
<td>5.94%</td>
</tr>
</tbody>
</table>
Conclusion

• Secret Sharing Importance and Challenge of Remembrance

• Steganography

• As future works:
  • Improve the security of secret sharing.
  • Improve the usability by image-based steganography.