Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority

Nouf Al-Otaibi and Adnan Gutub

Umm Al-Qura University (UQU)
Makkah, Saudi Arabia

Thursday 25th December 2014
Outline

• Motivation
• Cryptography vs. Steganography
• System Overview
• System Implementation Interface
• Testing
• Results & Comparison
Motivation:

• **Flexibility:** User Security Priority
• **PC data dependant** (Steganography)
• **Storage of Secure Text**
Cryptography vs. Steganography

- Cryptography
  - Converting secret data to unreadable forms...
  - Unconverting it back to the readable form

- Steganography
  - Hiding existence of a secret data (from observation)
Cryptography

Hiding

Key = Z  ←  Same  →  Key = Z

Retrieve

Secret Data

Z

Lock

Secret Data

Z

Key = Z
Public Key (Assymetric) Cryptosystems (PKC)

- Why public key cryptography?
- Key Distribution and Management is difficult in symmetric cryptosystems: DES, AES (Rijndael) over large networks.
- Electronic Signatures
- Other cryptographic functions such:
  - Key Exchange
  - Secret Key Derivation
  - Secret Sharing functions
Asymmetric Key Cryptography

• Instead of one key, have two
  ▫ public key
  ▫ private key

• Use one key to encode/encrypt
• Use other key to decode/decrypt
Simple Example of PKC
Non-mathematical
Basic Applications

- Confidentiality
  - Hiding contents of messages exchanged in a transaction
Basic Applications

• Authentication
  ▫ Ensuring that the origin of a message is correctly identified

Entity authentication
Basic Applications

- **Confidentiality**
  - Hiding contents of messages exchanged in a transaction
- **Authentication**
  - Ensuring that the origin of a message is correctly identified
- **Integrity**
  - Ensuring that only authorized parties are able to modify computer system assets and transmitted information
- **Non-repudiation**
  - Requires that neither of the authorized parties deny the aspects of a valid transaction
Steganography & Cryptography

- **Cryptography**
  - Converting messages to unreadable forms...
  - Unconverting it back to the readable form

- **Steganography**
  - Hiding the existence of a message
Overview: Steganography model for PC storage

Basic Steganography System

Sensitive Secret Text Data

Cover Steganography Image

Security System

Image Base

Steganography

Output: Stego-Image

Hiding Sensitive Secret Text Data on Personal Computers

Adnan Gutub
Thursday 25th December 2014
AET-2014, Dubai, UAE
Steganography: Image based

- Hiding in LSBs
- Example: embedding 200 => (11001000)

- Pixel 1: 00101101
  00011101
  11011100
- Pixel 2: 10100110
  11000101
  00001101
- Pixel 3: 11010010
  10101100
  01100011
System interface showing:
bits statistics to give full flexibility for user priority

process of hiding text
Testing: 30 images
security relation to data dependency

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>28</td>
<td>29</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Image 28]</td>
<td>![Image 29]</td>
<td>![Image 30]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NUMBER OF BITS FROM DIFFERENT TESTING’S HIDING IN 30 FIXED SIZE IMAGES

<table>
<thead>
<tr>
<th>pic</th>
<th>Number of Bits Different</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>29815</td>
</tr>
<tr>
<td>2</td>
<td>26533</td>
</tr>
<tr>
<td>3</td>
<td>33489</td>
</tr>
<tr>
<td>4</td>
<td>17086</td>
</tr>
<tr>
<td>5</td>
<td>21409</td>
</tr>
<tr>
<td>6</td>
<td>25637</td>
</tr>
<tr>
<td>7</td>
<td>27421</td>
</tr>
<tr>
<td>8</td>
<td>22656</td>
</tr>
<tr>
<td>9</td>
<td>13747</td>
</tr>
<tr>
<td>10</td>
<td>41327</td>
</tr>
<tr>
<td>11</td>
<td>30186</td>
</tr>
<tr>
<td>12</td>
<td>22396</td>
</tr>
<tr>
<td>13</td>
<td>57930</td>
</tr>
<tr>
<td>14</td>
<td>33535</td>
</tr>
<tr>
<td>15</td>
<td>37988</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>pic</th>
<th>Number of Bits Different</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>7749</td>
</tr>
<tr>
<td>17</td>
<td>26096</td>
</tr>
<tr>
<td>18</td>
<td>9222</td>
</tr>
<tr>
<td>19</td>
<td>27502</td>
</tr>
<tr>
<td>20</td>
<td>27149</td>
</tr>
<tr>
<td>21</td>
<td>27656</td>
</tr>
<tr>
<td>22</td>
<td>29447</td>
</tr>
<tr>
<td>23</td>
<td>23343</td>
</tr>
<tr>
<td>24</td>
<td>39382</td>
</tr>
<tr>
<td>25</td>
<td>29820</td>
</tr>
<tr>
<td>26</td>
<td>11169</td>
</tr>
<tr>
<td>27</td>
<td>28081</td>
</tr>
<tr>
<td>28</td>
<td>12339</td>
</tr>
<tr>
<td>29</td>
<td>89512</td>
</tr>
<tr>
<td>30</td>
<td>26230</td>
</tr>
</tbody>
</table>
Testing Results: 30 images
security relation to data dependency
Remarks

- Implemented visual basic platform
- Flexible Stego-system =>
  - user security priority
  - Useful for hiding text on PC
- Image Based Stego: fully dependant on the PC data available
Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority

Adnan Gutub
Thursday 25th December 2014
AET-2014, Dubai, UAE
Thanks for the opportunity

Questions?

Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority

Nouf Al-Otaibi and Adnan Gutub
Umm Al-Qura University (UQU), Makkah, Saudi Arabia