Enhancing Image Steganography via Stego Generation and Selection

IEEE ICASSP 2021

Tingting Song, Minglin Liu, Weiqi Luo*, Peijia Zheng
Sun Yat-sen University
Outline

1/ Traditional & Adversarial Embedding
2/ Proposed Method
3/ Experiments
4/ Conclusion
Outline

1/ Traditional & Adversarial Embedding

2/ Proposed Method

3/ Experiments

4/ Conclusion
Traditional & Adversarial Embedding

- **Traditional Embedding**: 
  - Embedding messages according to a handcrafted cost function

- **Adversarial Embedding**: 
  - Automatic learning by adversarial attack
  - Modifying costs according to the gradient of networks
  - Aim to deceive CNN-based steganalyzers
Traditional Embedding

Cover \( X \)

Cost Function

Init Cost

STC

Stego \( Y \)

Adversarial Embedding

Updated Cost

STC

Adv \( Z \)

Steganalyzer (CNN Classifier)

gradient

train
Outline

1/ Traditional & Adversarial Embedding
2/ Proposed Method
3/ Experiments
4/ Conclusion
Proposed Framework

Step #1: Steganalytic Network Training
(Training Set)

Step #2: Stego Generation
(Test Set)

Step #3: Stego Selection
(Test Set)
• Step #1: Steganalytic Network Training

• **Step #2: Stego Generation**

![Cover Example](image1)

![Larger gradients with p](image2)

![Smaller costs with p](image3)

![Selected Units](image4)

\[
\begin{align*}
\rho_{i,j}^+(x, y) &= \begin{cases} 
\rho_{i,0}^+(x, y) & g_i(x, y) < 0 \\
\rho_{i,0}^+(x, y) + \alpha & g_i(x, y) > 0 
\end{cases} \\
\rho_{i,j}^-(x, y) &= \begin{cases} 
\rho_{i,0}^-(x, y) & g_i(x, y) < 0 \\
\rho_{i,0}^-(x, y) + \alpha & g_i(x, y) > 0 
\end{cases}
\end{align*}
\]
• Step #3: Stego Selection

Outline

1/ Traditional & Adversarial Embedding
2/ Proposed Method
3/ Experiments
4/ Conclusion
Settings

- **Database:**
  - 10,000 images in BOSSBase-v1.01 & 10,000 image in BOWS2 are resized to 256x256, random shuffle
  - 8000 for training, 2000 for evaluation --- step #1
  - 10,000 for testing --- step #2 & #3

- **Key Parameters**
  - Number of new generated stego: \( m = 100 \)
  - Cost enhance parameter: \( \alpha = 2 \)
  - Top gradient & low cost: \( p \in [0.25, 1.25] \times \text{payload} \)
## Security Performances

<table>
<thead>
<tr>
<th>Method</th>
<th>Payload</th>
<th>SRM Original</th>
<th>Proposed</th>
<th>MaxSRMd2 Original</th>
<th>Proposed</th>
<th>Deng-Net Original</th>
<th>Proposed</th>
<th>SRNet Original</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>WOW</td>
<td>0.1 bpp</td>
<td>56.53</td>
<td>55.03*</td>
<td>65.27</td>
<td>61.07*</td>
<td>66.96</td>
<td>61.78*</td>
<td>66.98</td>
<td>62.81*</td>
</tr>
<tr>
<td></td>
<td>0.2 bpp</td>
<td>63.82</td>
<td>62.40*</td>
<td>72.46</td>
<td>68.55*</td>
<td>77.14</td>
<td>72.98*</td>
<td>76.43</td>
<td>72.63*</td>
</tr>
<tr>
<td></td>
<td>0.3 bpp</td>
<td>70.40</td>
<td>68.20*</td>
<td>77.91</td>
<td>74.55*</td>
<td>83.36</td>
<td>80.23*</td>
<td>82.89</td>
<td>79.33*</td>
</tr>
<tr>
<td></td>
<td>0.4 bpp</td>
<td>76.26</td>
<td>74.38*</td>
<td>81.97</td>
<td>79.25*</td>
<td>87.68</td>
<td>85.31*</td>
<td>86.85</td>
<td>84.69*</td>
</tr>
<tr>
<td>MiPOD</td>
<td>0.1 bpp</td>
<td>54.56</td>
<td>53.32*</td>
<td>56.24</td>
<td>54.39*</td>
<td>58.06</td>
<td>54.39*</td>
<td>58.57</td>
<td>56.30*</td>
</tr>
<tr>
<td></td>
<td>0.2 bpp</td>
<td>60.00</td>
<td>58.63*</td>
<td>63.08</td>
<td>59.53*</td>
<td>68.12</td>
<td>63.38*</td>
<td>67.37</td>
<td>63.29*</td>
</tr>
<tr>
<td></td>
<td>0.3 bpp</td>
<td>65.34</td>
<td>63.20*</td>
<td>68.18</td>
<td>64.25*</td>
<td>74.85</td>
<td>69.74*</td>
<td>73.86</td>
<td>69.73*</td>
</tr>
<tr>
<td></td>
<td>0.4 bpp</td>
<td>70.35</td>
<td>67.91*</td>
<td>73.16</td>
<td>69.37*</td>
<td>80.42</td>
<td>75.93*</td>
<td>78.48</td>
<td>74.59*</td>
</tr>
<tr>
<td>S-UNIWARD</td>
<td>0.1 bpp</td>
<td>55.86</td>
<td>54.88*</td>
<td>59.61</td>
<td>56.96*</td>
<td>61.93</td>
<td>58.70*</td>
<td>61.75</td>
<td>59.30*</td>
</tr>
<tr>
<td></td>
<td>0.2 bpp</td>
<td>63.16</td>
<td>61.85*</td>
<td>66.88</td>
<td>63.21*</td>
<td>72.90</td>
<td>69.47*</td>
<td>71.25</td>
<td>68.21*</td>
</tr>
<tr>
<td></td>
<td>0.3 bpp</td>
<td>70.01</td>
<td>68.33*</td>
<td>72.44</td>
<td>68.50*</td>
<td>80.69</td>
<td>77.60*</td>
<td>78.68</td>
<td>75.36*</td>
</tr>
<tr>
<td></td>
<td>0.4 bpp</td>
<td>75.97</td>
<td>74.02*</td>
<td>77.48</td>
<td>73.98*</td>
<td>85.49</td>
<td>83.97*</td>
<td>83.56</td>
<td>82.20*</td>
</tr>
<tr>
<td>HILL</td>
<td>0.1 bpp</td>
<td>53.60</td>
<td>52.72*</td>
<td>58.62</td>
<td>55.33*</td>
<td>61.48</td>
<td>55.32*</td>
<td>61.48</td>
<td>56.39*</td>
</tr>
<tr>
<td></td>
<td>0.2 bpp</td>
<td>59.45</td>
<td>56.93*</td>
<td>65.02</td>
<td>60.76*</td>
<td>69.96</td>
<td>64.04*</td>
<td>69.48</td>
<td>64.53*</td>
</tr>
<tr>
<td></td>
<td>0.3 bpp</td>
<td>64.51</td>
<td>62.84*</td>
<td>69.84</td>
<td>65.91*</td>
<td>76.35</td>
<td>71.77*</td>
<td>75.51</td>
<td>71.35*</td>
</tr>
<tr>
<td></td>
<td>0.4 bpp</td>
<td>70.10</td>
<td>68.15*</td>
<td>74.57</td>
<td>70.96*</td>
<td>80.95</td>
<td>76.77*</td>
<td>80.03</td>
<td>76.24*</td>
</tr>
<tr>
<td>CMD-HILL</td>
<td>0.1 bpp</td>
<td>52.36</td>
<td>51.96*</td>
<td>56.71</td>
<td>54.03*</td>
<td>58.08</td>
<td>53.29*</td>
<td>59.06</td>
<td>55.48*</td>
</tr>
<tr>
<td></td>
<td>0.2 bpp</td>
<td>56.03</td>
<td>55.21*</td>
<td>61.27</td>
<td>58.12*</td>
<td>66.34</td>
<td>60.25*</td>
<td>65.75</td>
<td>61.67*</td>
</tr>
<tr>
<td></td>
<td>0.3 bpp</td>
<td>60.04</td>
<td>59.10*</td>
<td>65.26</td>
<td>62.22*</td>
<td>72.19</td>
<td>66.75*</td>
<td>71.04</td>
<td>67.27*</td>
</tr>
<tr>
<td></td>
<td>0.4 bpp</td>
<td>64.40</td>
<td>63.61*</td>
<td>68.89</td>
<td>66.43*</td>
<td>76.32</td>
<td>72.13*</td>
<td>75.19</td>
<td>70.64*</td>
</tr>
</tbody>
</table>
Success Rate

\[ R_S = \frac{\sum_{\forall c_i \in C} I(F - SGS(c_i) \neq s_i,0)}{|C|} \]

- \( F - SGS \): enhancing steganography \( F \) using the proposed method
- \( F - SGS(c_i) \): final selected stego for an input cover \( c_i \)
- \( I(*) \): indicator function
- \( |C| \): number of elements in test set \( C \)
Cost Modification Rate

Table 2: Average cost modification rates (%) for different steganography and payloads

<table>
<thead>
<tr>
<th></th>
<th>0.1 bpp</th>
<th>0.2 bpp</th>
<th>0.3 bpp</th>
<th>0.4 bpp</th>
</tr>
</thead>
<tbody>
<tr>
<td>WOW-SGS</td>
<td>0.44</td>
<td>0.72</td>
<td>0.76</td>
<td>0.67</td>
</tr>
<tr>
<td>MiPOD-SGS</td>
<td>0.39</td>
<td>0.92</td>
<td>1.20</td>
<td>1.03</td>
</tr>
<tr>
<td>S-UNIWARD-SGS</td>
<td>0.50</td>
<td>1.38</td>
<td>2.32</td>
<td>3.04</td>
</tr>
<tr>
<td>HILL-SGS</td>
<td>0.47</td>
<td>0.78</td>
<td>0.81</td>
<td>0.73</td>
</tr>
<tr>
<td>CMD-HILL-SGS</td>
<td>0.38</td>
<td>0.60</td>
<td>0.62</td>
<td>0.63</td>
</tr>
</tbody>
</table>

Over 99% of original costs would not changed!
Contributions

- New framework for enhancing existing steganography
- Great security improvement

Future Works

- Apply in JPEG steganography
- More pre-trained classifiers
- Other generate methods and select methods
THANKS

Enhancing Image Steganography via Stego Generation and Selection

Email: songtt3@mail2.sysu.edu.cn