Graded Exercise on Steganography and Steganalysis

Multimedia Security & Forensics

University of Innsbruck

Submission deadline: 22 April 2015, 11:00 AM by e-mail to rainer.boehme@uibk.ac.at.

Steganalysis as decision problem

1.a. You will find a dataset on OLAT with values of a decision criterion as well as labels ("stego" and "cover") for the ground truth. Draw the corresponding empirical ROC curve. **2 P**

1.b. Determine the equal error rate (EER). **1 P**

LSB replacement and histogram attack

2.a. Use sequential LSB replacement to embed the encrypted message `011011011010` into the following signal:

$$\boldsymbol{x}^{(0)} = (43, 45, 38, 34, 40, 45, 44, 41, 37, 47, 39, 39)$$

1 P

2.b. You will find eight greyscale images on OLAT. Some of them contain a secret message embedded with sequential LSB replacement. Please find out, which ones. (You may document solution approaches in order to justify uncertain decisions, if necessary.) **4(+1) P**

Syndrome coding

3.a. Form the parity check matrix $\boldsymbol{H}$ for a $(15, 11)$-Hamming code. **1 P**

3.b. Embed the sequence $\boldsymbol{m} = (1, 0, 1, 0)^\mathsf{T}$ into a cover block with (pre-existing) steganographic semantic $\boldsymbol{b}^{(0)} = (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)^\mathsf{T}$. Minimize the number of embedding changes. **1 P**

3.c. Is it also possible to embed this sequence with *exactly two* changes? **1 P**

3.d. Is it also possible to embed this sequence without changing any of the first five positions? **1 P**

---

max. 12 P