Institute of Computer Science, University of Bern
Privacy and Data Security, HS 2021

Prof. Christian Cachin
Orestis Alpos, Luca Zanolini

Exercise 11

11.1 Information-theoretic steganography (6pt)

Three covertext sources A–C are available with distributions as follows:

A	a	b	c	d	e
P_A	0.1	0.12	0.15	0.2	0.43

B	a	b	c	d	e	f
P_B	0.15	0.15	0.15	0.15	0.15	0.25

C	a	b	c	d	e	f	g	h
P_C	0.1	0.1	0.1	0.14	0.14	0.14	0.14	0.14

Consider the simple binary example stegosystem shown in class (slide 19), also described in the literature [Cac04, Example 3]. Which of the covertexts is best suited for embedding a one-bit message? Use this and evaluate the resulting bound on the security of the stegosystem.

11.2 Practical steganography (4pt)

This exercise uses *steghide*, a steganography program that is able to hide data in various kinds of image and audio files. It does not change color or sample frequencies and is therefore resistant to detection by first-order statistical tests. The method first describes given coverdata using a graph, in which modifiable samples are represented as vertices. A message is then embedded by swapping the two samples adjacent to edges in the graph [HM05].

1. Download and run *steghide* from `http://steghide.sourceforge.net/`. Due to its age (last modified 2003!), it may be difficult to compile on modern platforms. At least on Debian and Ubuntu Linux, it is available as a precompiled package.
2. Select an image not larger than ca. 1000px $\times$ 1000px and multiple hidden messages of size 1kB, 10kB, ..., 100kB. Be aware that hidden messages are first compressed!

   Explore the results of embedding progressively more information. Do you find a tool that detects differences between some of your pictures?

   You may find the following websites useful:

   `https://www.lipsum.com`
   `https://www.diffchecker.com/image-diff/`
   `https://online-image-comparison.com`

   Return your image with the longest hidden message and do not forget to include the passphrase in the email.

$\Longrightarrow$

References

[Cac04] C. Cachin, *An information-theoretic model for steganography*, Inf. Comput. **192** (2004), no. 1, 41–56, https://doi.org/10.1016/j.ic.2004.02.003.

[HM05] S. Hetzl and P. Mutzel, *A graph-theoretic approach to steganography*, Communications and Multimedia Security, 9th IFIP TC-6 TC-11 International Conference, CMS 2005, Salzburg, Austria, September 19-21, 2005, Proceedings (J. Dittmann, S. Katzenbeisser, and A. Uhl, eds.), Lecture Notes in Computer Science, vol. 3677, Springer, 2005, https://doi.org/10.1007/11552055_12, pp. 119–128.