Bauhaus Universität Weimar
Dr. Andreas Jakoby
Feb. 18 2016

Group 3 - Exam Exercise

Analyse and improve the Watermarking System from the Octave program „text2png.m“.

1. Describe within your own words how the system works.
2. How secure is the system? Discuss whether usual image transformations can manipulate the embedded payload.
3. Is it possible to copy the embedded payload to an other image?
4. Improve the system to prevent a copy attack, e.g. use and implement the following strategy:
   (a) Determine some components of the cover work that are invariant to embedding.
   (b) Use a hash function (e.g. sdbm `http://www.cse.yorku.ca/~oz/hash.html`) to generate a hash value for an invariant component of the work.
   (c) Encrypt the hash value by using RSA.
   (d) Embed the signed hash value.

   (For this it is not your task to analyse the strength of your keys.)
5. Discuss whether your solution increase the security of the system.