Bauhaus Universität Weimar
Dr. Andreas Jakoby
July 16 2019

Summer Term 2019
Digital Watermarking and Steganography

# Group 11 - Exam Exercise

Discuss and implement a solution algorithm NoninvertibleEmbedder (and and the corresponding detector) of Lecture 13. Use the following modifications:

1. Use the DC-coefficients (upper left corner of the $8 \times 8$-block decomposition) of the Cb color channel after the standard jpg-transformation of all $8 \times 8$-block (except of the outer blocks) for the embedding.
2. Use the PRNG of Blum, Blum, and Shup with the primes $p = 59999$ and $q = 60107$ to determine the ordering of the $\ell$ most significant coefficients for the embedding (and the detection). Use 20151208 as initial value of xi.

Implement and run the AttackAgainstNoninvertibleEmbedder to analyse the strengths and weaknesses of the system.