

Supplementary Document for: “Information-Theoretic Bounds for Steganography in Multimedia”

Hassan Y. El-Arsh, Amr Abdelaziz, *Member, IEEE*, Ahmed Elliethy, *Member, IEEE*,
Hussein A. Aly, *Senior Member, IEEE*, and T. Aaron Gulliver, *Senior Member, IEEE*

In this document, experimental results from [1] and [2] are compared with the theoretical upper bound. Figures S-1 to S-4 give the results from [1] and Figures S-5 to S-11 give the results from [2].

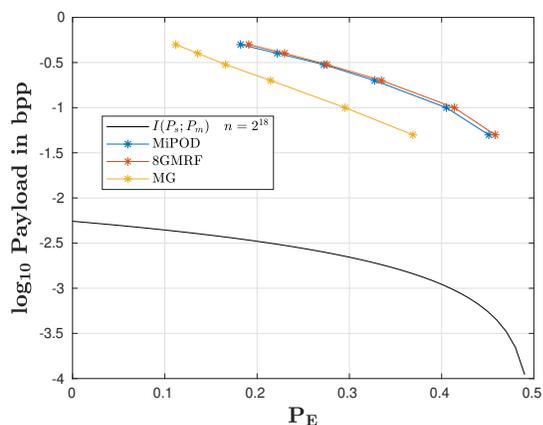


Fig. S-1: Results from [1] for the MiPOD, 8-GMRF, and MG steganographic methods with steganalysis using SRM.

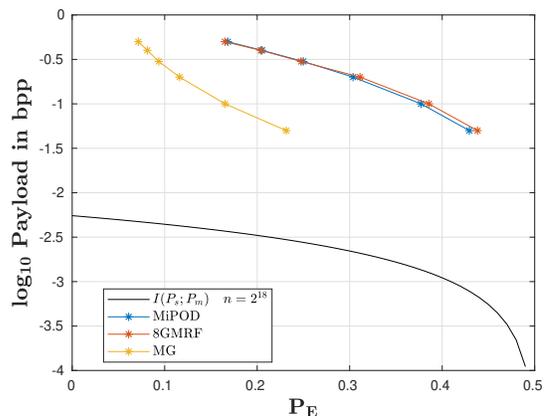


Fig. S-2: Results from [1] for the MiPOD, 8-GMRF, and MG steganographic methods with steganalysis using maxSRMd2.

REFERENCES

- [1] Y. Tong, J. Ni, and W. Su, “Image steganography using an eight-element neighborhood Gaussian Markov random field model,” in *Digital Forensics and Watermarking*, H. Wang, X. Zhao, Y. Shi, H. J. Kim, and A. Piva, Eds. Chengdu, China: Springer International Publishing, 2020, pp. 247–255.
- [2] M. Sharifzadeh, M. Aloraini, and D. Schonfeld, “Adaptive batch size image merging steganography and quantized Gaussian image steganography,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 867–879, Jul. 2020.

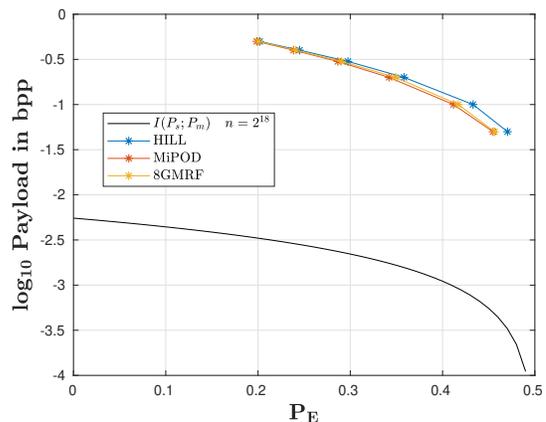


Fig. S-3: Results from [1] for the MiPOD and 8-GMRF (both enhanced using low-pass filtered cost) and HILL steganographic methods and the ensemble 1.0 classifier with steganalysis using SRM.

H. Y. El-Arsh, Amr Abdelaziz, A. Elliethy, and H. A. Aly are with Dept. of Computer Engineering, Military Technical College, Cairo, Egypt. (e-mail: hassan.yakout@gmail.com, amrashry@mtc.edu.eg, a.s.elliethy@mtc.edu.eg, haly@ieee.org). T. Aaron Gulliver: Dept. of Electrical & Computer Engineering University of Victoria, Canada. (e-mail: agullive@ece.uvic.ca)

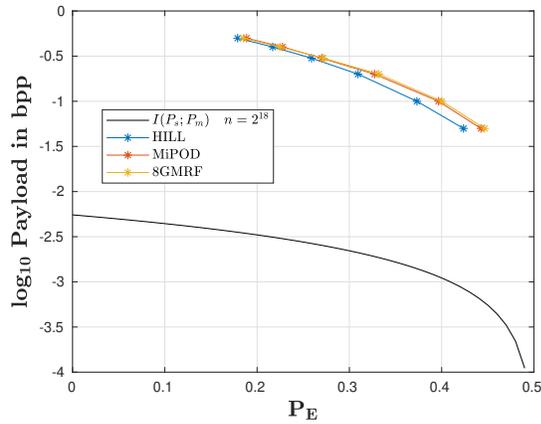


Fig. S-4: Results from [1] for the MiPOD and 8-GMRF (both enhanced using low-pass filtered cost) and HILL steganographic methods and the ensemble 1.0 classifier with steganalysis using maxSRMd2.

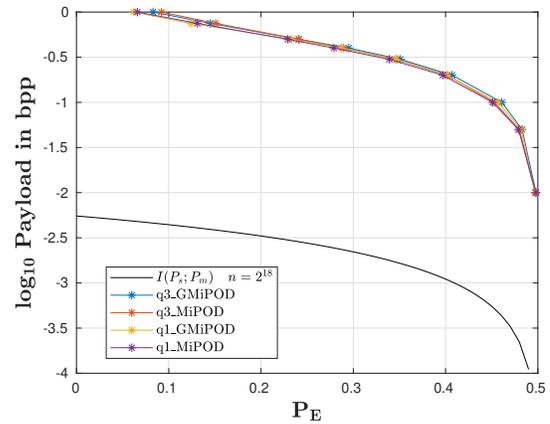


Fig. S-7: Results from [2] for the MiPOD steganographic method and the modified Gaussian version for $q = 1, 3$ with steganalysis using maxSRMd2.

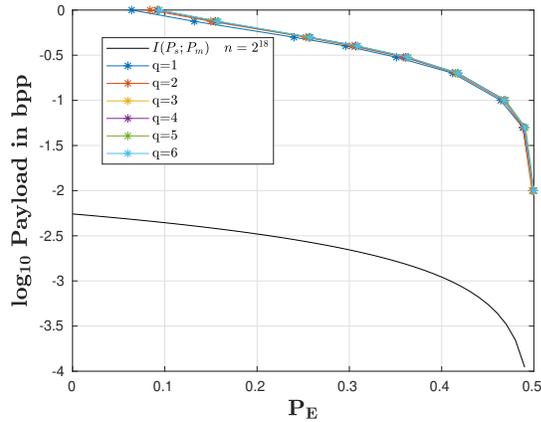


Fig. S-5: Results for the Gaussian version of the HILL algorithm in [2] with different q values in a $(2q + 1)$ -ary embedding with steganalysis using maxSRMd2.

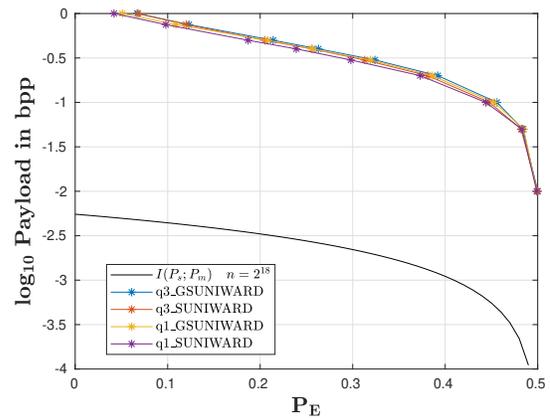


Fig. S-8: Results from [2] for the SUNIWARD steganographic method and the modified Gaussian version for $q = 1, 3$ with steganalysis using maxSRMd2.

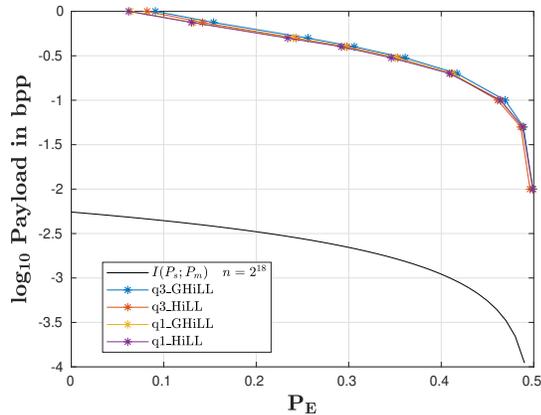


Fig. S-6: Results from [2] for the HILL steganographic method and the modified Gaussian version for $q = 1, 3$ with steganalysis using maxSRMd2.

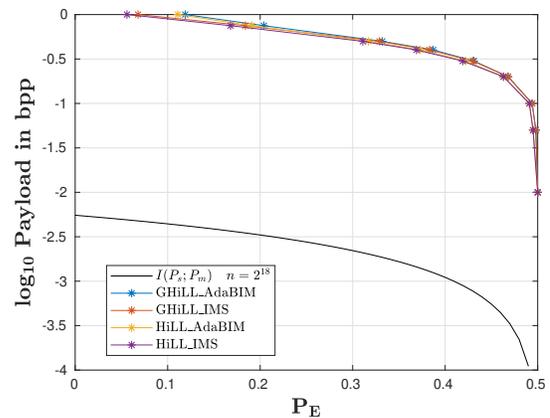


Fig. S-9: Results from [2] for the HILL steganographic method and the modified Gaussian version with two batching strategies, IMS with batch size 128 and AdaBIM with adaptive batch size, with steganalysis using maxSRMd2.

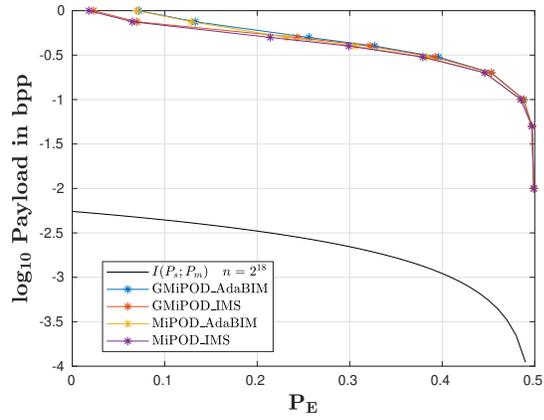


Fig. S-10: Results from [2] for the MiPOD steganographic method and the modified Gaussian version with two batching strategies, IMS with batch size 128 and AdaBIM with adaptive batch size, with steganalysis using maxSRMd2.

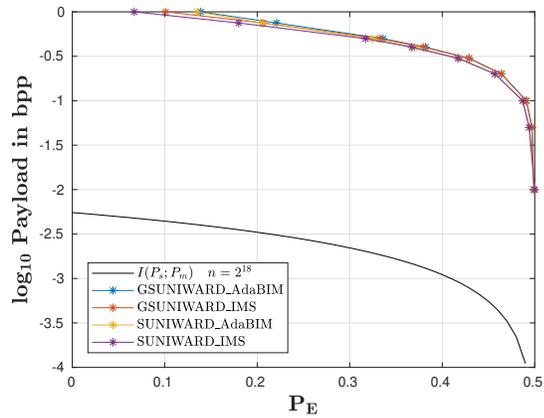


Fig. S-11: Results from [2] for the SUNIWARD steganographic method and the modified Gaussian version with two batching strategies, IMS with batch size 128 and AdaBIM with adaptive batch size, with steganalysis using maxSRMd2.