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

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

In this supplementary document we demonstrate an additional experimental results from [1] and [2] plotted against our theoretical upper bound. Figures S-1 to S-4 demonstrates the results obtained from [1] and figures S-5 to S-11 are obtained from [2].

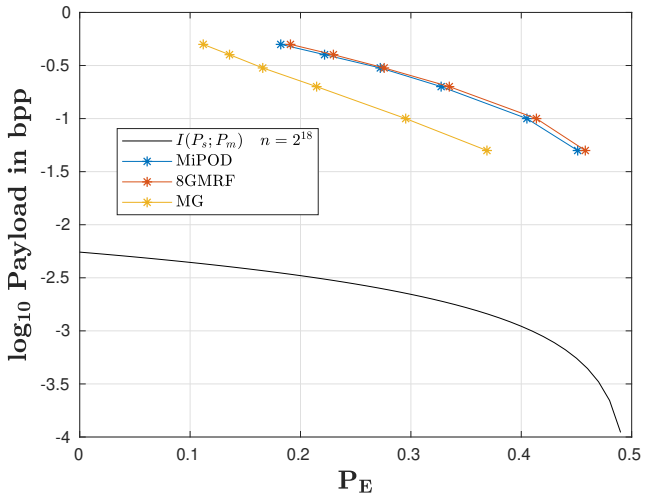

Fig. S-1: Results from [1] comparing steganographic methods: MiPOD, 8-GMRF and MG with steganalyzer utilizing SRM feature.

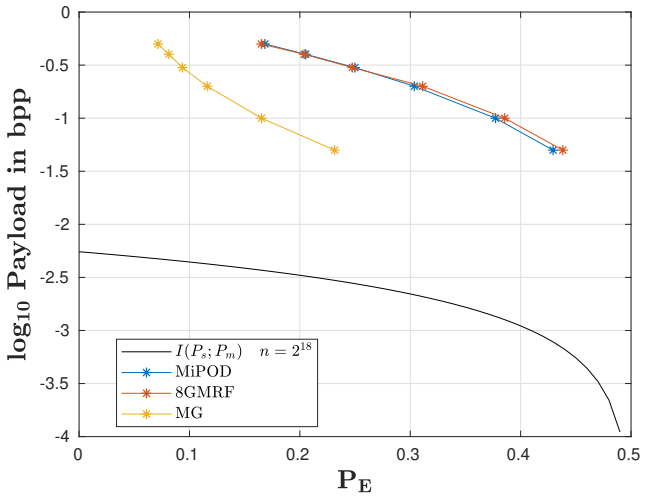

Fig. S-2: Results from [1] comparing steganographic methods: MiPOD, 8-GMRF and MG with steganalyzer utilizing maxSRMd2 feature.

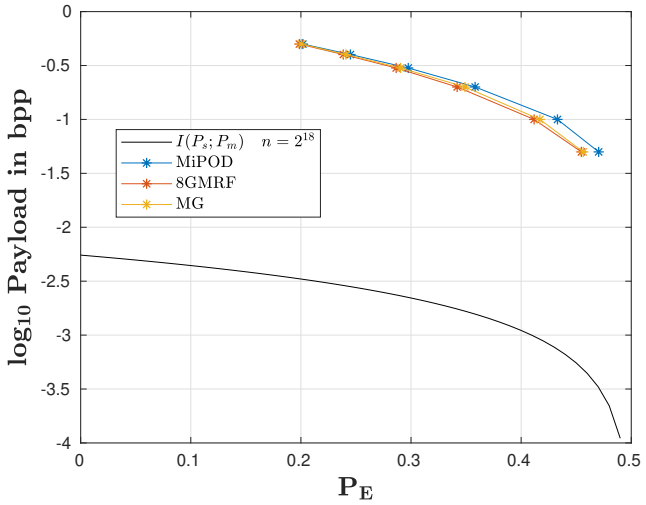

Fig. S-3: Results from [1] comparing steganographic methods: HiLL, MiPOD and 8-GMRF enhanced by filtered cost using ensemble 1.0 classifier with steganalyzer utilizing SRM feature.

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@ymail.com, amrashry@mtc.edu.eg, a.s.elliethy@mtc.edu.eg, haly@ieee.org).

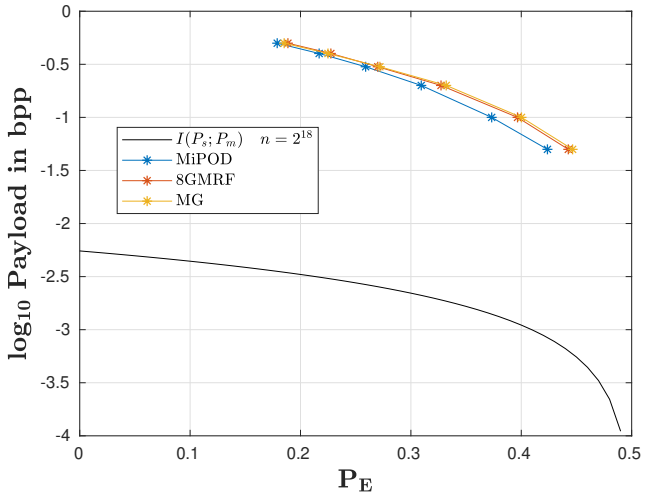

Fig. S-4: Results from [1] comparing steganographic methods: HiLL, MiPOD and 8-GMRF enhanced by filtered cost using ensemble 1.0 classifier with steganalyzer utilizing maxSRMd2 feature.

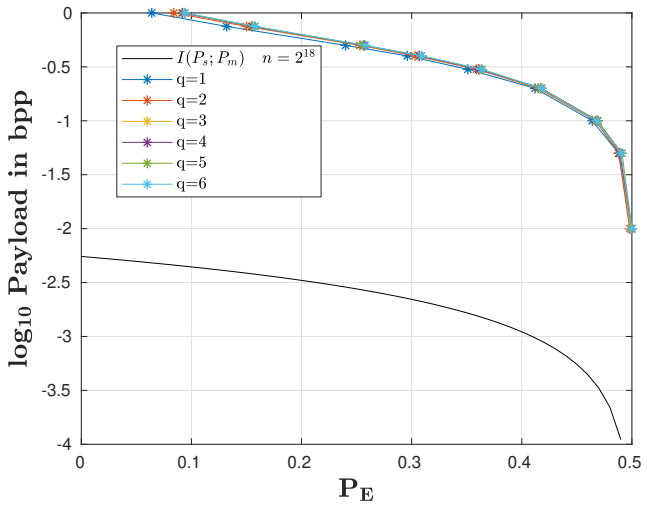

Fig. S-5: Comparing our theoretically calculated limit with results of the Gaussian version of the HILL algorithm in [2] with different q values in a $(2q+1)$-ary embedding with steganalyzer utilizing maxSRMd2 feature.

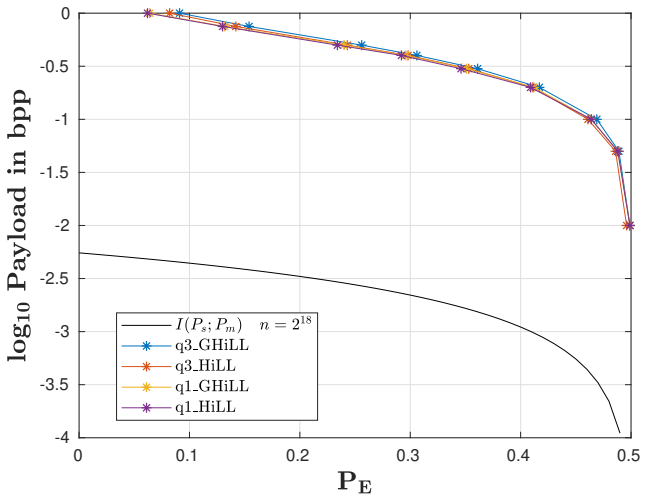

Fig. S-6: Results from [2] comparing HILL steganographic method and its modified Gaussian version with $q=1,3$ with steganalyzer utilizing maxSRMd2 feature.

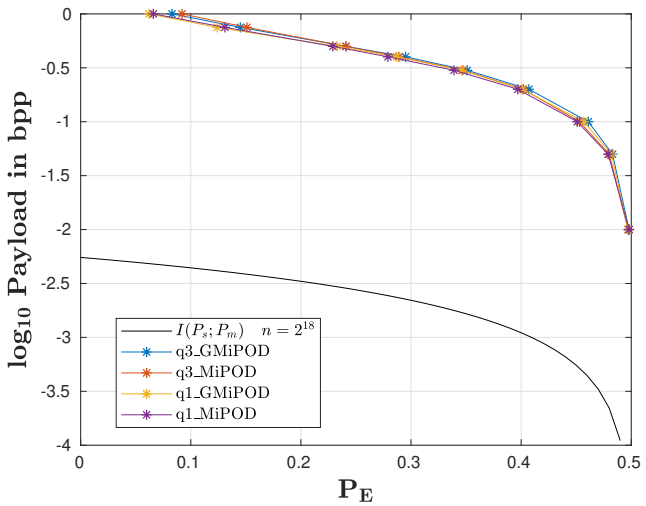

Fig. S-7: Results from [2] comparing MiPOD steganographic method and its modified Gaussian version with $q=1,3$ with steganalyzer utilizing maxSRMd2 feature.

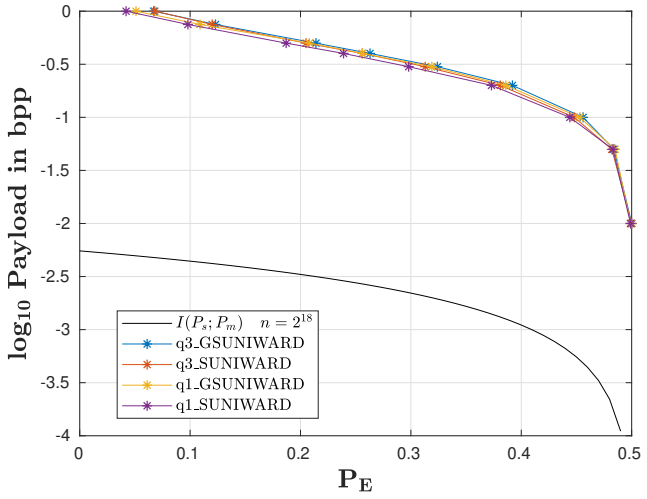

Fig. S-8: Results from [2] comparing SUNIWARD steganographic method and its modified Gaussian version with $q = 1, 3$ with steganalyzer utilizing maxSRMd2 feature.

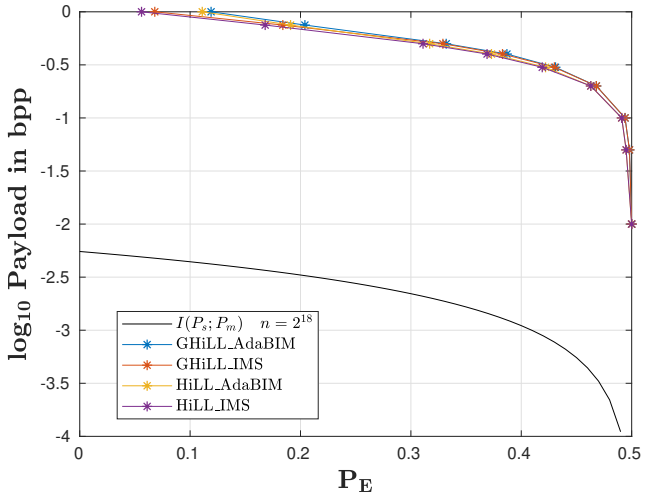

Fig. S-9: Results from [2] comparing HILL steganographic method and its modified Gaussian version with two different batching strategies, IMS with batch size 128 and $AdaBIM$ with adaptive batch size against steganalyzer utilizing maxSRMd2 feature.

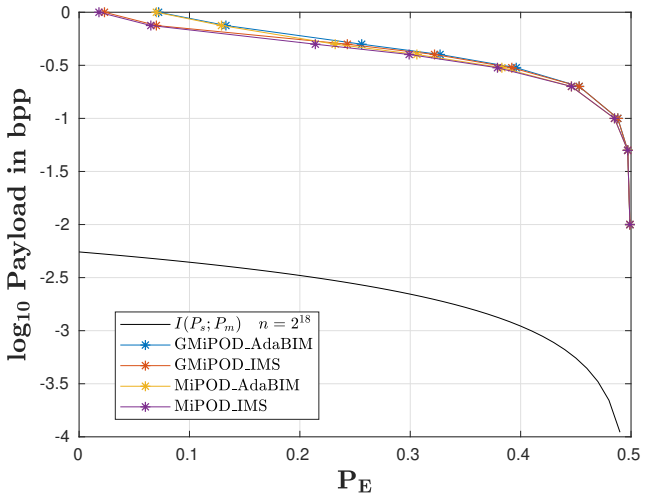

Fig. S-10: Results from [2] comparing HILL steganographic method and its modified Gaussian version with two different batching strategies, IMS with batch size 128 and $AdaBIM$ with adaptive batch size against steganalyzer utilizing maxSRMd2 feature.

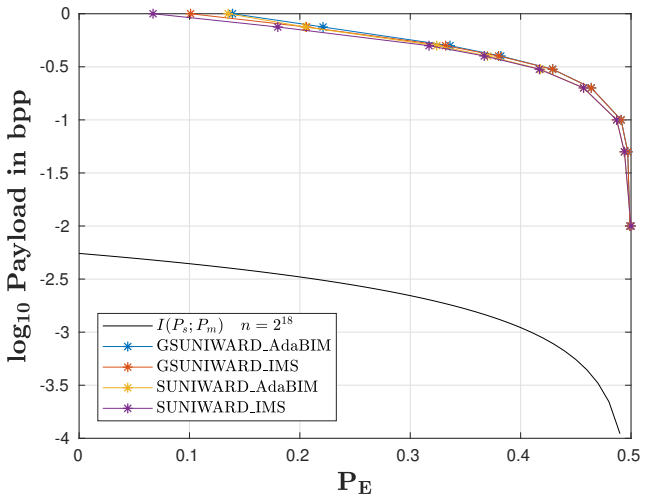

Fig. S-11: Results from [2] comparing HILL steganographic method and its modified Gaussian version with two different batching strategies, IMS with batch size 128 and $AdaBIM$ with adaptive batch size against steganalyzer utilizing maxSRMd2 feature.

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. Cham: 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, 2020.