Supplementary Material

Static Knowledge Base Literature List

[1] S. Craver, "On public-key steganography in the presence of an active warden," in *International Workshop on Information Hiding*, 1998.

[2] J. Fridrich and M. Long, "Steganalysis of LSB encoding in color images," in *2000 IEEE International Conference on Multimedia and Expo (ICME)*, vol. 3, 2000.

[3] M. Goljan, J. Fridrich, and R. Du, "Distortion-free data embedding for images," in *International Workshop on Information Hiding*, 2001.

[4] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges*, 2001.

[5] J. Fridrich, M. Goljan, and R. Du, "Steganalysis based on JPEG compatibility," in *Multimedia Systems and Applications IV*, vol. 4518, 2001.

[6] J. Fridrich and M. Goljan, "Practical steganalysis of digital images: state of the art," in *Security and Watermarking of Multimedia Contents IV*, vol. 4675, pp. 1–13, 2002.

[7] J. Fridrich, M. Goljan, and D. Hogea, "Steganalysis of JPEG images: Breaking the F5 algorithm," in *International Workshop on Information Hiding*, 2002.

[8] J. Fridrich, M. Goljan, and D. Hogea, "New methodology for breaking steganographic techniques for JPEGs," in *Security and Watermarking of Multimedia Contents V*, vol. 5020, 2003.

[9] J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation," in *Security and Watermarking of Multimedia Contents V*, vol. 5020, 2003.

[10] J. Fridrich, M. Goljan, D. Hogea, and D. Soukal, "Quantitative steganalysis of digital images: estimating the secret message length," *Multimedia Systems*, vol. 9, no. 3, pp. 288–302, 2003.

[11] J. Fridrich, M. Goljan, and D. Soukal, "Higher-order statistical steganalysis of palette images," in *Security and Watermarking of Multimedia Contents V*, vol. 5020, 2003.

[12] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proceedings of Digital Forensic Research Workshop*, vol. 3, no. 2, 2003.

[13] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[14] A. D. Ker, "Improved detection of LSB steganography in grayscale images," in *International Workshop on Information Hiding*, 2004.

[15] J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes," in *International Workshop on Information Hiding*, 2004.

[16] J. Fridrich, M. Goljan, and D. Soukal, "Perturbed quantization steganography with wet paper codes," in *Proceedings of the 2004 workshop on Multimedia and security*, 2004.

[17] J. Fridrich and M. Goljan, "On estimation of secret message length in LSB steganography in spatial domain," in *Security, steganography, and watermarking of multimedia contents VI*, vol. 5306, 2004.

[18] B. Roue, P. Bas, and J.-M. Chassery, "Improving LSB steganalysis using marginal and joint probabilistic distributions," in *Proceedings of the 2004 workshop on Multimedia and security*, 2004.

[19] R. Böhme and A. Westfeld, "Exploiting preserved statistics for steganalysis," in *International Workshop on Information Hiding*, 2004.

[20] R. Böhme and A. Westfeld, "Statistical characterisation of MP3 encoders for steganalysis," in *Proceedings of the 2004 workshop on Multimedia and security*, 2004.

[21] R. Böhme and A. Westfeld, "Breaking Cauchy model-based JPEG steganography with first order statistics," in *European symposium on research in computer security*, 2004.

[22] A. D. Ker, "A general framework for structural steganalysis of LSB replacement," in *International Workshop on Information Hiding*, 2005.

[23] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12, no. 6, pp. 441–444, 2005.

[24] J. Fridrich, M. Goljan, and D. Soukal, "Forensic steganalysis: determining the stego key in spatial domain steganography," in *Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, 2005.

[25] J. Fridrich, M. Goljan, and D. Soukal, "Steganography via codes for memory with defective cells," in *43rd Allerton Conference on Communication, Control, and Computing*, 2005.

[26] J. Fridrich, D. Soukal, and M. Goljan, "Maximum likelihood estimation of length of secret message embedded using ±k steganography in spatial domain," in *Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, 2005.

[27] R. Böhme, "Assessment of steganalytic methods using multiple regression models," in *International Workshop on Information Hiding*, 2005.

[28] A. D. Ker, "Fourth-order structural steganalysis and analysis of cover assumptions," in *Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072, 2006.

[29] A. D. Ker, "Batch steganography and pooled steganalysis," in *International Workshop on Information Hiding*, 2006.

[30] J. Fridrich, P. Lisoněk, and D. Soukal, "On steganographic embedding efficiency," in *International Workshop on Information Hiding*, 2006.

[31] J. Fridrich, "Minimizing the embedding impact in steganography," in *Proceedings of the 8th Workshop on Multimedia and Security*, 2006.

[32] R. Böhme and A. D. Ker, "A two-factor error model for quantitative steganalysis," in *Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072, 2006.

[33] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285–287, 2006.

[34] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 111–119, 2006.

[35] A. D. Ker, "Steganalysis of embedding in two least-significant bits," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 46–54, 2007.

[36] A. D. Ker, "Derivation of error distribution in least squares steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 2, pp. 140–148, 2007.

[37] A. D. Ker, "The ultimate steganalysis benchmark?" in *Proceedings of the 9th Workshop on Multimedia & Security*, 2007.

[38] A. D. Ker, "A capacity result for batch steganography," *IEEE Signal Processing Letters*, vol. 14, no. 8, pp. 525–528, 2007.

[39] A. D. Ker, "Batch steganography and the threshold game," in *Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, 2007.

[40] J. Fridrich and P. Lisoněk, "Grid colorings in steganography," *IEEE Transactions on Information Theory*, vol. 53, no. 4, pp. 1547–1549, 2007.

[41] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: dead ends, challenges, and opportunities," in *Proceedings of the 9th Workshop on Multimedia & Security*, pp. 3–14, 2007.

[42] Y. Miche, P. Bas, A. Lendasse, C. Jutten, and O. Simula, "Advantages of using feature selection techniques on steganalysis schemes," in *International Work-Conference on Artificial Neural Networks (IWANN)*, vol. 4507, pp. 606–613, 2007.

[43] R. Böhme and C. Keiler, "On the security of 'A steganographic scheme for secure communications based on the chaos and the Euler theorem'," *IEEE Transactions on Multimedia*, vol. 9, no. 6, pp. 1325–1329, 2007.

[44] T. Pevný and J. Fridrich, "Merging Markov and DCT features for multi-class JPEG steganalysis," in *Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, 2007.

[45] A. D. Ker and R. Böhme, "Revisiting weighted stego-image steganalysis," in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819, 2008.

[46] A. D. Ker, "Perturbation hiding and the batch steganography problem," in *International Workshop on Information Hiding*, 2008.

[47] A. D. Ker, "Locating steganographic payload via WS residuals," in *Proceedings of the 10th ACM Workshop on Multimedia and Security*, 2008.

[48] F. Cayre and P. Bas, "Kerckhoffs-based embedding security classes for woa data hiding," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 1–15, 2008.

[49] R. Böhme, "Weighted stego-image steganalysis for JPEG covers," in *International Workshop on Information Hiding*, 2008.

[50] S. Craver, E. Li, J. Yu, and I. Atakli, "A supraliminal channel in a videoconferencing application," in *International Workshop on Information Hiding*, pp. 283–293, 2008.

[51] T. Pevný and J. Fridrich, "Multiclass detector of current steganographic methods for JPEG format," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 635–650, 2008.

[52] T. Pevný and J. Fridrich, "Novelty detection in blind steganalysis," in *Proceedings of the 10th ACM Workshop on Multimedia and Security*, 2008.

[53] T. Pevný and J. Fridrich, "Estimation of primary quantization matrix for steganalysis of double-compressed JPEG images," in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819, 2008.

[54] T. Pevný and J. Fridrich, "Detection of double-compression in JPEG images for applications in steganography," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 2, pp. 247–258, 2008.

[55] T. Pevný and J. Fridrich, "Benchmarking for steganography," in *International Workshop on Information Hiding*, 2008.

[56] J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography," in *Transactions on Data Hiding and Multimedia Security III*, pp. 1–22, 2008.

[57] M. Chen, J. Fridrich, M. Goljan, and J. Lukás, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, 2008.

[58] A. D. Ker and I. Lubenko, "Feature reduction and payload location with WAM steganalysis," in *Media Forensics and Security*, vol. 7254, 2009.

[59] T. Filler, A. D. Ker, and J. Fridrich, "The square root law of steganographic capacity for Markov covers," in *Media Forensics and Security*, vol. 7254, 2009.

[60] A. D. Ker, "Estimating steganographic Fisher information in real images," in *International Workshop on Information Hiding*, 2009.

[61] R. Böhme, "An epistemological approach to steganography," in *International Workshop on Information Hiding*, 2009.

[62] S. Craver, E. Li, and J. Yu, "Protocols for data hiding in pseudo-random state," in *Media Forensics and Security*, vol. 7254, 2009.

[63] T. Filler and J. Fridrich, "Wet ZZW construction for steganography," in *2009 First IEEE International Workshop on Information Forensics and Security (WIFS)*, 2009.

[64] T. Filler and J. Fridrich, "Complete characterization of perfectly secure stego-systems with mutually independent embedding operation," in *2009 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2009.

[65] T. Filler and J. Fridrich, "Fisher information determines capacity of -secure steganography," in *International Workshop on Information Hiding*, 2009.

[66] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," in *Proceedings of the 11th ACM Workshop on Multimedia and Security*, 2009.

[67] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, Cambridge University Press, 2009.

[68] T. Filler and J. Fridrich, "Minimizing additive distortion functions with non-binary embedding operation in steganography," in *2010 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2010.

[69] T. Filler and J. Fridrich, "Gibbs construction in steganography," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 705–720, 2010.

[70] T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization," in *Media Forensics and Security II*, vol. 7541, 2010.

[71] T. Filler and J. Fridrich, "Steganography using Gibbs random fields," in *Proceedings of the 12th ACM Workshop on Multimedia and Security*, 2010.

[72] J. Kodovský and J. Fridrich, "Quantitative structural steganalysis of Jsteg," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 681–693, 2010.

[73] R. Böhme, "Improved weighted stego image steganalysis," in *Advanced Statistical Steganalysis*, pp. 155–182, 2010.

[74] R. Böhme, "Models of heterogeneous covers for quantitative steganalysis," in *Advanced Statistical Steganalysis*, pp. 127–153, 2010.

[75] R. Böhme, "Using encoder artefacts for steganalysis of compressed audio streams," in *Advanced Statistical Steganalysis*, pp. 183–206, 2010.

[76] R. Böhme, "Principles of modern steganography and steganalysis," in *Advanced Statistical Steganalysis*, pp. 11–77, 2010.

[77] R. Böhme, "Detection of model-based steganography with first-order statistics," in *Advanced Statistical Steganalysis*, pp. 111–126, 2010.

[78] Q. Liu, A. H. Sung, M. Qiao, Z. Chen, and B. Ribeiro, "An improved approach to steganalysis of JPEG images," *Information Sciences*, vol. 180, no. 9, pp. 1643–1655, 2010.

[79] J. Kodovský, T. Pevný, and J. Fridrich, "Modern steganalysis can detect YASS," in *Media Forensics and Security II*, vol. 7541, 2010.

[80] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *International Workshop on Information Hiding*, 2010.

[81] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 201–214, 2010.

[82] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432–444, 2011.

[83] J. Fridrich, J. Kodovský, V. Holub, and M. Goljan, "Steganalysis of content-adaptive steganography in spatial domain," in *International Workshop on Information Hiding*, pp. 102–117, 2011.

[84] J. Kodovský, J. Fridrich, and V. Holub, "On dangers of overtraining steganography to incomplete cover model," in *Proceedings of the 13th ACM Workshop on Multimedia and Security*, 2011.

[85] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system: the ins and outs of organizing BOSS," in *International Workshop on Information Hiding*, 2011.

[86] R. Cogranne, C. Zitzmann, L. Fillatre, F. Retraint, I. Nikiforov, and P. Cornu, "A cover image model for reliable steganalysis," in *International Workshop on Information Hiding*, pp. 178–192, 2011.

[87] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 920–935, 2011.

[88] T. Pevný, J. Fridrich, and A. D. Ker, "From blind to quantitative steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 445–454, 2011.

[89] J. Kodovský and J. Fridrich, "Steganalysis in high dimensions: fusing classifiers built on random subspaces," in *Media Watermarking, Security, and Forensics III*, vol. 7880, 2011.

[90] I. Lubenko and A. D. Ker, "Steganalysis with mismatched covers: do simple classifiers help?" in *Proceedings of the ACM Workshop on Multimedia and Security*, pp. 11–18, 2012.

[91] A. D. Ker and T. Pevný, "Batch steganography in the real world," in *Proceedings of the ACM Workshop on Multimedia and Security*, pp. 1–10, 2012.

[92] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868–882, 2012.

[93] J. Kodovský and J. Fridrich, "JPEG-compatibility steganalysis using block-histogram of recompression artifacts," in *International Workshop on Information Hiding*, 2012.

[94] J. Fridrich and J. Kodovský, "Steganalysis of LSB replacement using parity-aware features," in *International Workshop on Information Hiding*, 2012.

[95] V. Holub and J. Fridrich, "Optimizing pixel predictors for steganalysis," in *Media Watermarking, Security, and Forensics 2012*, vol. 8303, 2012.

[96] J. Kodovský and J. Fridrich, "Steganalysis of JPEG images using rich models," in *Media Watermarking, Security, and Forensics 2012*, vol. 8303, 2012.

[97] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 234–239, 2012.

[98] J. Fridrich, "Effect of cover quantization on steganographic Fisher information," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 361–373, 2012.

[99] P. Schöttle, S. Korff, and R. Böhme, "Weighted stego-image steganalysis for naive content-adaptive embedding," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2012.

[100] P. Schöttle and R. Böhme, "A game-theoretic approach to content-adaptive steganography," in *International Workshop on Information Hiding*, 2012.

[101] R. Cogranne, C. Zitzmann, F. Retraint, I. Nikiforov, L. Fillatre, and P. Cornu, "Statistical detection of LSB matching in the presence of nuisance parameters," in *2012 IEEE Statistical Signal Processing Workshop (SSP)*, pp. 912–915, 2012.

[102] R. Cogranne, C. Zitzmann, F. Retraint, I. Nikiforov, L. Fillatre, and P. Cornu, "Statistical detection of LSB matching using hypothesis testing theory," in *International Workshop on Information Hiding*, pp. 46–62, 2012.

[103] T. Pevný, "Co-occurrence steganalysis in high dimensions," in *Media Watermarking, Security, and Forensics 2012*, vol. 8303, 2012.

[104] J. Makelberge and A. D. Ker, "Exploring multitask learning for steganalysis," in *Media Watermarking, Security, and Forensics 2013*, vol. 8665, 2013.

[105] V. Holub, J. Fridrich, and T. Denemark, "Random projections of residuals as an alternative to co-occurrences in steganalysis," in *Media Watermarking, Security, and Forensics 2013*, vol. 8665, 2013.

[106] J. Kodovský and J. Fridrich, "Steganalysis in resized images," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2013.

[107] V. Holub and J. Fridrich, "Random projections of residuals for digital image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1996–2006, 2013.

[108] J. Kodovský and J. Fridrich, "Quantitative steganalysis using rich models," in *Media Watermarking, Security, and Forensics 2013*, vol. 8665, 2013.

[109] J. Fridrich and J. Kodovský, "Multivariate Gaussian model for designing additive distortion for steganography," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2013.

[110] J. Fridrich, "On the role of side information in steganography in empirical covers," in *Media Watermarking, Security, and Forensics 2013*, vol. 8665, 2013.

[111] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security*, pp. 1–4, 2013.

[112] E. Zidel-Cauffet, P. Bas, and P. Chainais, "Quantification adaptative pour la stéganalyse d'images texturées," in *GRETSI 2013*, 2013.

[113] B. Johnson, P. Schöttle, A. Laszka, J. Grossklags, and R. Böhme, "Bitspotting: detecting optimal adaptive steganography," in *International Workshop on Digital Watermarking*, pp. 3–18, 2013.

[114] T. H. Thai, R. Cogranne, and F. Retraint, "Steganalysis of Jsteg algorithm based on a novel statistical model of quantized DCT coefficients," in *2013 IEEE International Conference on Image Processing (ICIP)*, 2013.

[115] A. D. Ker, P. Bas, R. Böhme, et al., "Moving steganography and steganalysis from the laboratory into the real world," in *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security*, pp. 45–58, 2013.

[116] A. D. Ker and T. Pevný, "The steganographer is the outlier: realistic large-scale steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 9, pp. 1424–1435, 2014.

[117] J. Kodovský, V. Sedighi, and J. Fridrich, "Study of cover source mismatch in steganalysis and ways to mitigate its impact," in *Media Watermarking, Security, and Forensics 2014*, vol. 9028, 2014.

[118] M. Goljan, J. Fridrich, and R. Cogranne, "Rich model for steganalysis of color images," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2014.

[119] V. Holub and J. Fridrich, "Low-complexity features for JPEG steganalysis using undecimated DCT," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 219–228, 2014.

[120] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP Journal on Information Security*, vol. 2014, no. 1, 2014.

[121] J. Kodovský and J. Fridrich, "Effect of image downsampling on steganographic security," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 752–762, 2014.

[122] V. Holub and J. Fridrich, "Challenging the doctrines of JPEG steganography," in *Media Watermarking, Security, and Forensics 2014*, vol. 9028, 2014.

[123] M. Kirchner and R. Böhme, "Steganalysis in technicolor: boosting WS detection of stego images from CFA-interpolated covers," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2014.

[124] T. H. Thai, R. Cogranne, and F. Retraint, "Statistical model of quantized DCT coefficients: application in the steganalysis of Jsteg algorithm," *IEEE Transactions on Image Processing*, vol. 23, no. 5, pp. 1980–1993, 2014.

[125] T. Pevný and A. D. Ker, "Steganographic key leakage through payload metadata," in *Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security*, 2014.

[126] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *2014 IEEE International Conference on Image Processing (ICIP)*, pp. 4206–4210, 2014.

[127] T. Denemark, J. Fridrich, and V. Holub, "Further study on the security of S-UNIWARD," in *Media Watermarking, Security, and Forensics 2014*, vol. 9028, pp. 38–50, 2014.

[128] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, and J. Fridrich, "Selection-channel-aware rich model for steganalysis of digital images," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 48–53, 2014.

[129] M. Goljan and J. Fridrich, "CFA-aware features for steganalysis of color images," in *Media Watermarking, Security, and Forensics 2015*, vol. 9409, 2015.

[130] V. Holub and J. Fridrich, "Phase-aware projection model for steganalysis of JPEG images," in *Media Watermarking, Security, and Forensics 2015*, vol. 9409, 2015.

[131] V. Sedighi and J. Fridrich, "Effect of imprecise knowledge of the selection channel on steganalysis," in *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security*, 2015.

[132] V. Sedighi, J. Fridrich, and R. Cogranne, "Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model," in *Media Watermarking, Security, and Forensics 2015*, vol. 9409, 2015.

[133] T. Denemark and J. Fridrich, "Side-informed steganography with additive distortion," in *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2015.

[134] T. Denemark and J. Fridrich, "Improving steganographic security by synchronizing the selection channel," in *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security*, 2015.

[135] P. Schöttle and R. Böhme, "Game theory and adaptive steganography," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 760–773, 2015.

[136] R. Cogranne, "A sequential method for online steganalysis," in *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2015.

[137] R. Cogranne, V. Sedighi, J. Fridrich, and T. Pevný, "Is ensemble classifier needed for steganalysis in high-dimensional feature spaces?" in *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 1–6, 2015.

[138] T. Qiao, F. Retraint, R. Cogranne, and C. Zitzmann, "Steganalysis of JSteg algorithm using hypothesis testing theory," *EURASIP Journal on Information Security*, vol. 2015, no. 1, 2015.

[139] R. Cogranne and J. Fridrich, "Modeling and extending the ensemble classifier for steganalysis of digital images using hypothesis testing theory," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2627–2642, 2015.

[140] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221–234, 2015.

[141] E. Li, S. Craver, and J. Yu, "Capacity limits of pseudorandom channels in deception problems," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1824–1834, 2015.

[142] T. Pevný and I. Nikolaev, "Optimizing pooling function for pooled steganalysis," in *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2015.

[143] L. Guo, J. Ni, W. Su, C. Tang, and Y.-Q. Shi, "Using statistical image model for JPEG steganography: uniform embedding revisited," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2669–2680, 2015.

[144] A. Wilson and A. D. Ker, "Avoiding detection on twitter: embedding strategies for linguistic steganography," *Electronic Imaging*, vol. 28, pp. 1–9, 2016.

[145] T. Denemark, J. Fridrich, and P. Comesaña-Alfaro, "Improving selection-channel-aware steganalysis features," *Electronic Imaging*, vol. 28, pp. 1–8, 2016.

[146] T. Denemark, M. Boroumand, and J. Fridrich, "Steganalysis features for content-adaptive JPEG steganography," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1736–1746, 2016.

[147] M. Boroumand and J. Fridrich, "Boosting steganalysis with explicit feature maps," in *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, 2016.

[148] P. Bas, "Steganography via cover-source switching," in *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2016.

[149] P. Bas, "Natural steganography: cover-source switching for better steganography," *arXiv preprint arXiv:1607.07824*, 2016.

[150] A. D. Ker, "The square root law of steganography: bringing theory closer to practice," in *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, 2017.

[151] T. Denemark and J. Fridrich, "Model based steganography with precover," *Electronic Imaging*, vol. 29, pp. 56–66, 2017.

[152] M. Boroumand and J. Fridrich, "Applications of explicit non-linear feature maps in steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 823–833, 2017.

[153] M. Boroumand and J. Fridrich, "Nonlinear feature normalization in steganalysis," in *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, 2017.

[154] T. Denemark and J. Fridrich, "Steganography with two JPEGs of the same scene," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017.

[155] T. Denemark and J. Fridrich, "Steganography with multiple JPEG images of the same scene," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2308–2319, 2017.

[156] P. Bas, "An embedding mechanism for natural steganography after down-sampling," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017.

[157] R. Cogranne, V. Sedighi, and J. Fridrich, "Practical strategies for content-adaptive batch steganography and pooled steganalysis," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017.

[158] W. Zhou, W. Zhang, and N. Yu, "A new rule for cost reassignment in adaptive steganography," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2654–2667, 2017.

[159] C. Kin-Cleaves and A. D. Ker, "Adaptive steganography in the noisy channel with dual-syndrome trellis codes," in *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2018.

[160] A. D. Ker, "On the relationship between embedding costs and steganographic capacity," in *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, 2018.

[161] T. Pevný and A. D. Ker, "Exploring non-additive distortion in steganography," in *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, 2018.

[162] M. Chen, M. Boroumand, and J. Fridrich, "Deep learning regressors for quantitative steganalysis," *Electronic Imaging*, vol. 30, pp. 1–7, 2018.

[163] M. Boroumand, M. Chen, and J. Fridrich, "Deep residual network for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1181–1193, 2018.

[164] T. Denemark, P. Bas, and J. Fridrich, "Natural steganography in JPEG compressed images," in *Electronic Imaging*, 2018.

[165] Q. Giboulot, R. Cogranne, and P. Bas, "Steganalysis into the wild: how to define a source?" in *IS&T Electronic Imaging, Media Watermarking, Security, and Forensics 2018*, 2018.

[166] Z. Qian, K.-K. R. Choo, R. Cogranne, and X. Zhang, "Multimedia security: novel steganography and privacy preserving," *Security and Communication Networks*, vol. 2018, pp. 1–2, 2018.

[167] M. Chen, M. Boroumand, and J. Fridrich, "Reference channels for steganalysis of images with convolutional neural networks," in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, 2019.

[168] Y. Yousfi, J. Butora, J. Fridrich, and Q. Giboulot, "Breaking ALASKA: color separation for steganalysis in JPEG domain," in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, pp. 138–149, 2019.

[169] E. Giboulot and J. Fridrich, "Payload scaling for adaptive steganography: an empirical study," *IEEE Signal Processing Letters*, vol. 26, no. 9, pp. 1339–1343, 2019.

[170] J. Butora and J. Fridrich, "Effect of JPEG quality on steganographic security," in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, 2019.

[171] T. Taburet, P. Bas, W. Sawaya, and J. Fridrich, "A natural steganography embedding scheme dedicated to color sensors in the JPEG domain," *Electronic Imaging*, vol. 31, pp. 1–11, 2019.

[172] T. Taburet, P. Bas, J. Fridrich, and W. Sawaya, "Computing dependencies between DCT coefficients for natural steganography in JPEG domain," in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, pp. 57–62, 2019.

[173] R. Cogranne, Q. Giboulot, and P. Bas, "The ALASKA steganalysis challenge: a first step towards steganalysis," in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, 2019.

[174] A. Zakaria, M. Chaumont, and G. Subsol, "Pooled steganalysis in JPEG: how to deal with the spreading strategy?" in *2019 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2019.

[175] S. Bernard, T. Pevný, P. Bas, and J. Klein, "Exploiting adversarial embeddings for better steganography," in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, pp. 216–221, 2019.

[176] Y. Yousfi and J. Fridrich, "JPEG steganalysis detectors scalable with respect to compression quality," *Electronic Imaging*, vol. 32, pp. 1–11, 2020.

[177] J. Butora and J. Fridrich, "Minimum perturbation cost modulation for side-informed steganography," *Electronic Imaging*, vol. 32, pp. 1–8, 2020.

[178] M. Boroumand and J. Fridrich, "Synchronizing embedding changes in side-informed steganography," *Electronic Imaging*, vol. 32, pp. 1–12, 2020.

[179] J. Butora and J. Fridrich, "Steganography and its detection in JPEG images obtained with the trunc quantizer," in *ICASSP 2020 – 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2020.

[180] J. Butora, Y. Yousfi, and J. Fridrich, "Turning cost-based steganography into model-based," in *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*, 2020.

[181] E. Giboulot, P. Bas, and R. Cogranne, "Synchronization minimizing statistical detectability for side-informed JPEG steganography," in *2020 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2020.

[182] S. Bernard, P. Bas, J. Klein, and T. Pevný, "Explicit optimization of min max steganographic game," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 812–823, 2020.

[183] T. Taburet, P. Bas, W. Sawaya, and J. Fridrich, "Natural steganography in JPEG domain with a linear development pipeline," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 173–186, 2020.

[184] R. Cogranne, E. Giboulot, and P. Bas, "ALASKA#2: challenging academic research on steganalysis with realistic images," in *2020 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2020.

[185] Q. Giboulot, R. Cogranne, D. Borghys, and P. Bas, "Effects and solutions of cover-source mismatch in image steganalysis," *Signal Processing: Image Communication*, vol. 86, pp. 115888, 2020.

[186] E. Giboulot, R. Cogranne, and P. Bas, "JPEG steganography with side information from the processing pipeline," in *ICASSP 2020 – 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2020.

[187] R. Cogranne, "Selection-channel-aware reverse JPEG compatibility for highly reliable steganalysis of JPEG images," in *ICASSP 2020 – 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2020.

[188] R. Cogranne, Q. Giboulot, and P. Bas, "Steganography by minimizing statistical detectability: the cases of JPEG and color images," in *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*, 2020.

[189] W. Su, J. Ni, X. Hu, and J. Fridrich, "Image steganography with symmetric embedding using Gaussian Markov random field model," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 3, pp. 1001–1015, 2020.

[190] X. Liao, J. Yin, M. Chen, and Z. Qin, "Adaptive payload distribution in multiple images steganography based on image texture features," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 897–911, 2020.

[191] T. Itzhaki, Y. Yousfi, and J. Fridrich, "Data augmentation for JPEG steganalysis," in *2021 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2021.

[192] J. Butora, Y. Yousfi, and J. Fridrich, "How to pretrain for steganalysis," in *Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security*, 2021.

[193] R. Cogranne, E. Giboulot, and P. Bas, "Efficient steganography in JPEG images by minimizing performance of optimal detector," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1328–1343, 2021.

[194] E. Giboulot, R. Cogranne, and P. Bas, "Detectability-based JPEG steganography modeling the processing pipeline: the noise-content trade-off," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2202–2217, 2021.

[195] M. Liu, W. Luo, P. Zheng, and J. Huang, "A new adversarial embedding method for enhancing image steganography," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4621–4634, 2021.

[196] J. Butora and J. Fridrich, "Revisiting perturbed quantization," in *Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security*, 2021.

[197] A. D. Ker, "Capacity laws for steganography in a crowd," in *Proceedings of the 2022 ACM Workshop on Information Hiding and Multimedia Security*, 2022.

[198] Y. Yousfi, E. Dworetzky, and J. Fridrich, "Detector-informed batch steganography and pooled steganalysis," in *Proceedings of the 2022 ACM Workshop on Information Hiding and Multimedia Security*, 2022.

[199] Q. Giboulot, P. Bas, R. Cogranne, and D. Borghys, "The cover source mismatch problem in deep-learning steganalysis," in *2022 30th European Signal Processing Conference (EUSIPCO)*, pp. 1032–1036, 2022.

[200] V. Leask, R. Cogranne, D. Borghys, and H. Bruyninckx, "UNCOVER: development of an efficient steganalysis framework for uncovering hidden data in digital media," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–8, 2022.

[201] E. Dworetzky and J. Fridrich, "Explaining the bag gain in batch steganography," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3031–3043, 2023.

[202] E. Kaziakhmedov, E. Dworetzky, and J. Fridrich, "Limits of data driven steganography detectors," in *Proceedings of the 2023 ACM Workshop on Information Hiding and Multimedia Security*, 2023.

[203] J. Butora and P. Bas, "Side-informed steganography for JPEG images by modeling decompressed images," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2683–2695, 2023.

[204] M. Beneš, B. Lorch, and R. Böhme, "JPEG steganalysis using leaked cover thumbnails," in *2023 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2023.

[205] S. Craver and N. Rosbrook, "Applying a zero-knowledge watermarking protocol to secure elections," in *Proceedings of the 2023 ACM Workshop on Information Hiding and Multimedia Security*, 2023.

[206] E. Giboulot, T. Pevný, and A. D. Ker, "The non-zero-sum game of steganography in heterogeneous environments," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 4436–4448, 2023.

[207] X. Mo, S. Tan, W. Tang, B. Li, and J. Huang, "ReLOAD: using reinforcement learning to optimize asymmetric distortion for additive steganography," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1524–1538, 2023.

[208] D. Huang, W. Luo, M. Liu, W. Tang, and J. Huang, "Steganography embedding cost learning with generative multi-adversarial network," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 15–29, 2023.

[209] E. Dworetzky and J. Fridrich, "How to form bags in batch steganography," in *2024 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2024.

[210] E. Kaziakhmedov, E. Dworetzky, and J. Fridrich, "Analyzing quantitative detectors for content-adaptive steganography," *Electronic Imaging*, vol. 36, no. 4, 2024.

[211] E. Dworetzky, E. Kaziakhmedov, and J. Fridrich, "Improving steganographic security with source biasing," in *Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security*, 2024.

[212] J. Butora and P. Bas, "Size-independent reliable CNN for RJCA steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4420–4431, 2024.

[213] M. Beneš and R. Böhme, "Kerckhoffs in prison: a study of the steganalyst's knowledge," in *2024 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2024.

[214] B. Lorch and R. Böhme, "Steganalysis in directional JPEG images," in *2024 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2024.

[215] M. Beneš and R. Böhme, "Exploring diffusion-inspired pixel predictors for WS steganalysis," in *Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security*, 2024.

[216] A. Mallet, M. Beneš, and R. Cogranne, "Cover-source mismatch in steganalysis: systematic review," *EURASIP Journal on Information Security*, vol. 2024, no. 1, pp. 26, 2024.

[217] A. Mallet, R. Cogranne, and P. Bas, "Linking intrinsic difficulty and regret to properties of multivariate gaussians in image steganalysis," in *Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security*, 2024.

[218] E. Dworetzky, E. Kaziakhmedov, and J. Fridrich, "Secure payload scaling for source adaptive payload allocation," *Electronic Imaging*, vol. 36, pp. 1–11, 2024.

[219] Q. Liu, W. Su, J. Ni, X. Hu, and J. Huang, "An efficient distortion cost function design for image steganography in spatial domain using quaternion representation," *Signal Processing*, vol. 219, pp. 109370, 2024.

[220] Y. Pan, J. Ni, Q. Liu, W. Su, and J. Huang, "Efficient JPEG image steganography using pairwise conditional random field model," *Signal Processing*, vol. 221, pp. 109493, 2024.

[221] E. Kaziakhmedov, J. Fridrich, and P. Bas, "Effect of acquisition noise outliers on steganalysis," in *Proceedings of the 2025 ACM Workshop on Information Hiding and Multimedia Security*, 2025.

[222] E. Kaziakhmedov and J. Fridrich, "Transformers for pooled steganalysis," *Electronic Imaging*, vol. 37, pp. 1–10, 2025.

[223] E. Dworetzky and J. Fridrich, "Secure payload scaling in detector-informed batch steganography: the mismatched detectors case," in *Proceedings of the 2025 ACM Workshop on Information Hiding and Multimedia Security*, 2025.

[224] J. Butora and P. Bas, "MODE: loss function for deep steganalysis at low false positive rate," in *2025 33rd European Signal Processing Conference (EUSIPCO)*, 2025.

[225] Y. Zhang, Y. Ma, Q. Zhang, Y. Pei, and X. Luo, "An image robust batch steganography framework with minimum embedding signs," *IEEE Transactions on Information Forensics and Security*, 2025.

[226] B. Li, N. Li, J. Yang, et al., "Image steganalysis using active learning and hyperparameter optimization," *Scientific Reports*, vol. 15, no. 1, pp. 7340, 2025.

[227] H. Y. El-Arsh, A. Abdelaziz, A. Elliethy, H. A. Aly, and T. A. Gulliver, "Information-theoretic bounds for steganography in visual multimedia," *Journal of Information Security and Applications*, vol. 89, pp. 103966, 2025.

[228] E. Levecque, A. Noirault, T. Pevný, J. Butora, P. Bas, and R. Cogranne, "Targeted pooled latent-space steganalysis applied to generative steganography, with a fix," in *ICASSP 2026 – 2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 13452–13456, 2026.