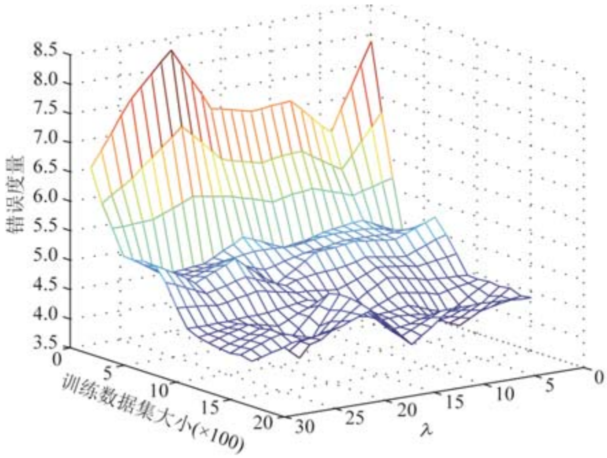
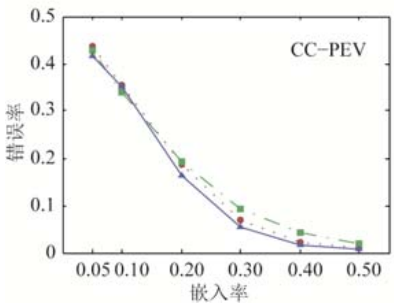
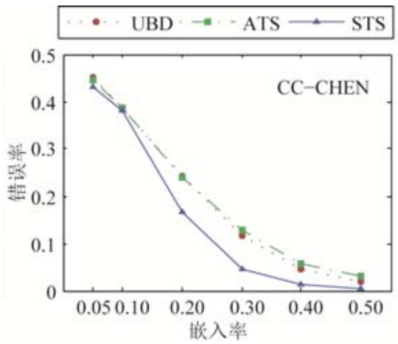


Fig.9 The relationship between the experimental parameters and the average error rate

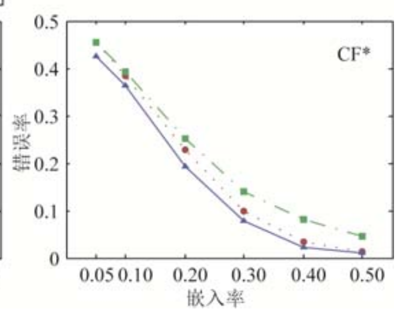
图 9 实验参数与平均错误率关系示意图



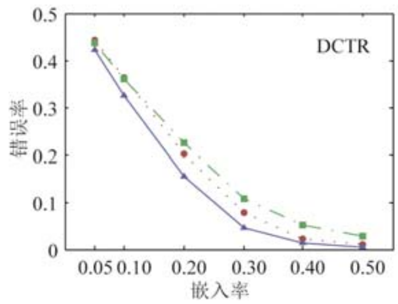
(a) CC-PEV 特征对比实验结果



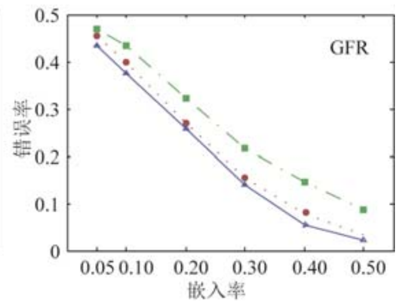
(b) CC-CHEN 特征对比实验结果



(c) CF*特征对比实验结果



(d) DCTR 特征对比实验结果



(e) GFR 特征对比实验结果

Fig.10 The comparison of experimental results between our method and other methods

图 10 本文方法与其他方法对比结果图

Table 1 The comparison of experimental results between our method and other methods

表 1 本文方法与其他方法对比结果表

隐写分析特征	分析框架	不同嵌入率(bpac)下检测错误率(%)					
		0.05	0.1	0.2	0.3	0.4	0.5
CC-PEV	UBD	43.71	35.14	18.57	6.99	2.33	1.02
	ATS	42.73	**34.03**	19.40	9.25	4.30	1.90
	STSS	**41.47**	35.12	**16.39**	**5.57**	**1.51**	**0.80**
CC-CHEN	UBD	45.05	38.62	24.13	11.71	4.57	1.84
	ATS	44.45	38.60	23.85	12.88	5.73	3.00
	STSS	**43.14**	**38.13**	**16.56**	**4.68**	**1.34**	**0.50**

Table 1 The comparison of experimental results between our method and other methods (Continued)

表 1 本文方法与其他方法对比结果表(续)

隐写分析特征	分析框架	不同嵌入率(bpac)下检测错误率(%)					
		0.05	0.1	0.2	0.3	0.4	0.5
CF*	UBD	45.42	38.31	22.74	9.77	3.41	1.44
	ATS	45.40	39.13	25.15	14.00	8.00	4.55
	STSS	**42.63**	**36.29**	**19.25**	**7.67**	**2.24**	**1.03**
DCTR	UBD	44.38	36.47	20.02	7.80	2.34	0.93
	ATS	43.60	35.95	22.60	10.85	5.08	2.80
	STSS	**42.25**	**32.50**	**15.31**	**4.53**	**1.20**	**0.43**
GFR	UBD	45.52	39.86	26.98	15.49	7.77	3.47
	ATS	46.85	43.45	32.30	21.53	14.48	8.68
	STSS	**43.39**	**37.59**	**25.71**	**13.93**	**5.46**	**2.08**

6 结 论

隐写操作在对数字图像进行修改的同时也改变了图像在特征空间中的位置,不同图像的特征在隐写作用下运动模式也会不同.以往的隐写分析工作没有充分挖掘训练数据与测试样本之间的关系,也没有充分利用测试样本本身的信息来进行分析.本文提出了“特定测试样本隐写分析(STSS)框架”,研究了影响隐写分析的两个重要因素——“特征距离”与“特征运动模式”相似度,基于这两个因素,在训练数据库中针对每个测试样本选择专用的训练集训练分类器,很大程度上解决了隐写分析中的 CSM 问题.实验结果表明,本文方法进一步挖掘了训练数据库的分析潜力,有效利用了测试样本的信息,在特定测试样本的隐写分析场景中表现出的性能优于其他方法.

当拥有大数据训练资源时,我们就有条件对特定测试样本筛选更匹配的训练集,所以,STSS 框架适用于设计大数据环境下的精准隐写分析系统.但本文对 STSS 框架仅进行了初步探索,未来还有许多问题需要进一步研究.

(1) 本文假设隐写算法与嵌入率已知,下一步可以尝试对常见隐写修改模式,如“LSB 替换”和“加减 1”进行未知嵌入率的隐写分析;

(2) 本文目前只对经典的非自适应隐写算法 nsF5 作了分析,设计了两种训练集筛选特征,取得了初步实验效果.对于使用 STC 框架的自适应隐写算法,未来可以考虑融合其他特征(如纹理特征)进行深入研究,设计更好的训练集筛选方法,以进一步拓宽 STSS 框架的应用范围,完善其性能.

References:

[1] Chen, K. Information hiding, digital watermarking and steganography. In: Encyclopedia of Multimedia Technology & Networking. 2005. 382–389. [doi: 10.4018/978-1-59140-561-0.ch055]

[2] Li B, He J, Huang J, Shi YQ. A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 2011,2(2):142–172.

[3] Wang SZ, Zhang XP, Zhang KW. Digital Steganography and Steganalysis: Information Warfare Technology in the Internet Age. Beijing: Tsinghua University Press Co., Ltd, 2005 (in Chinese).

[4] Bender W, Gruhl D, Morimoto N, Lu A. Techniques for data hiding. IBM Systems Journal, 1996,35(3.4):313–336.

[5] Sharp T. An implementation of key-based digital signal steganography. In: Information Hiding. Berlin, Heidelberg: Springer-Verlag, 2001. 13–26. [doi: 10.1007/3-540-45496-9_2]

[6] Mielikainen J. LSB matching revisited. IEEE Signal Processing Letters, 2006,13(5):285–287. [doi: 10.1109/LSP.2006.870357]

[7] Pevný T, Filler T, Bas P. Using high-dimensional image models to perform highly undetectable steganography. In: Proc. of the Int’l Workshop on Information Hiding. Berlin, Heidelberg: Springer-Verlag, 2010. 161–177. [doi: 10.1007/978-3-642-16435-4_13]

[8] Holub V, Fridrich J. Designing steganographic distortion using directional filters. In: Proc. of the 2012 IEEE Int’l Workshop on Information Forensics and Security (WIFS). IEEE, 2012. 234–239. [doi: 10.1109/WIFS.2012.6412655]

[9] Holub V, Fridrich J. Digital image steganography using universal distortion. In: Proc. of the 1st ACM Workshop on Information Hiding and Multimedia Security. ACM, 2013. 59–68. [doi: 10.1145/2482513.2482514]

[10] Fridrich JJ, Kodovský J. Multivariate gaussian model for designing additive distortion for steganography. In: Proc. of the ICASSP. 2013. 2949–2953. [doi: 10.1109/ICASSP.2013.6638198]

[11] Sedighi V, Fridrich JJ, Cogranne R. Content-Adaptive pentary steganography using the multivariate generalized Gaussian cover model. In: Media Watermarking, Security, and Forensics. 2015. 94090H. [doi: 10.1117/12.2080272]

[12] Sedighi V, Cogranne R, Fridrich J. Content-Adaptive steganography by minimizing statistical detectability. IEEE Trans. on Information Forensics and Security, 2016,11(2):221–234. [doi: 10.1109/TIFS.2015.2486744]

[13] Westfeld A. F5-A steganographic algorithm: High capacity despite better steganalysis. In: Proc. of the 4th Information Hiding Workshop. 2001,2137:289–302. https://link.springer.com/chapter/10.1007/3-540-45496-9_21

[14] Fridrich J, Pevný T, Kodovský J. Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities. In: Proc. of the 9th Workshop on Multimedia & Security. ACM, 2007. 3–14. [doi: 10.1145/1288869.1288872]

[15] Provos N. Defending against statistical steganalysis. In: Proc. of the Usenix Security Symp, Vol. 10. 2001. 323–336.

[16] Sallee P. Model-Based steganography. In: Proc. of the IWDW. 2003,2939:154–167. [doi: 10.1007/978-3-540-24624-4_12]

[17] Sallee P. Model-Based methods for steganography and steganalysis. Int'l Journal of Image and Graphics, 2005,5(1):167–189. [doi: 10.1142/S0219467805001719]

[18] Fridrich J, Goljan M, Soukal D. Perturbed quantization steganography. Multimedia Systems, 2005,11(2):98–107. [doi: 10.1007/s00530-005-0194-3]

[19] Kim Y, Duric Z, Richards D. Modified matrix encoding technique for minimal distortion steganography. In: Information Hiding. 2006,4437:314–327. [doi: 10.1007/978-3-540-74124-4_21]

[20] Solanki K, Sarkar A, Manjunath BS. YASS: Yet another steganographic scheme that resists blind steganalysis. In: Proc. of the Int'l Workshop on Information Hiding. Berlin, Heidelberg: Springer-Verlag, 2007. 16–31. [doi: 10.1007/978-3-540-77370-2_2]

[21] Guo L, Ni J, Shi YQ. Uniform embedding for efficient JPEG steganography. IEEE Trans. on Information Forensics and Security, 2014,9(5):814–825. [doi: 10.1109/TIFS.2014.2312817]

[22] Guo L, Ni J, Su W, Tang C, Shi YQ. Using statistical image model for JPEG steganography: Uniform embedding revisited. IEEE Trans. on Information Forensics and Security, 2015,10(12):2669–2680. [doi: 10.1109/TIFS.2015.2473815]

[23] Wang SZ, Zhang XP, Zhang WM. Recent advances in image-based steganalysis research. Chinese Journal of Computers, 2009, 32(7):1247–1263 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.01247]

[24] Kodovsky J, Fridrich J, Holub V. Ensemble classifiers for steganalysis of digital media. IEEE Trans. on Information Forensics and Security, 2012,7(2):432–444. [doi: 10.1109/TIFS.2011.2175919]

[25] Shi YQ, Chen C, Chen W. A Markov process based approach to effective attacking JPEG steganography. In: Proc. of the Int'l Workshop on Information Hiding. Berlin, Heidelberg: Springer-Verlag, 2006. 249–264. [doi: 10.1007/978-3-540-74124-4_17]

[26] Haralick RM, Shanmugam K, Dinstein IH. Textural features for image classification. IEEE Trans. on Systems Man & Cybernetics, 1973,3(6):610–621. [doi: 10.1109/TSMC.1973.4309314]

[27] Holotyak T, Fridrich J, Voloshynovskiy S. Blind statistical steganalysis of additive steganography using wavelet higher order statistics. In: Proc. of the IFIP TC-6 TC-11 Int'l Conf. on Communications and Multimedia Security. Springer-Verlag, 2005. 273–274. [doi: 10.1007/11552055_31]

[28] Pevny T, Fridrich J. Merging Markov and DCT features for multi-class JPEG steganalysis. In: Proc. of the Int'l Society for Optics and Photonics on Electronic Imaging. 2007. 650503-13. [doi: 10.1117/12.696774]

[29] Chen C, Shi YQ. JPEG image steganalysis utilizing both intrablock and interblock correlations. In: Proc. of the IEEE Int'l Symp. on Circuits and Systems. IEEE, 2008. 3029–3032. [doi: 10.1109/ISCAS.2008.4542096]

[30] Kodovský J, Fridrich J. Calibration revisited. In: Proc. of the 11th ACM Workshop on Multimedia and Security. ACM, 2009. 63–74. [doi: 10.1145/1597817.1597830]

[31] Pevny T, Bas P, Fridrich J. Steganalysis by subtractive pixel adjacency matrix. IEEE Trans. on Information Forensics and Security, 2010,5(2):215–224. [doi: 10.1109/TIFS.2010.2045842]

[32] Kodovský J, Fridrich JJ. Steganalysis of JPEG images using rich models. Media Watermarking, Security, and Forensics, 2012, 8303:0A–1.

[33] Fridrich J, Kodovsky J. Rich models for steganalysis of digital images. IEEE Trans. on Information Forensics and Security, 2012, 7(3):868–882. [doi: 10.1109/TIFS.2012.2190402]

[34] Huang W, Zhao XF, Feng DG, Sheng RN. JPEG steganalysis based on feature fusion by principal component analysis. Ruan Jian Xue Bao/Journal of Software, 2012,23(7):1869–1879 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4107.htm [doi: 10.3724/SP.J.1001.2012.04107]

[35] Li F, Zhang X, Chen B, Feng G. JPEG steganalysis with high-dimensional features and Bayesian ensemble classifier. IEEE Signal Processing Letters, 2013,20(3):233–236. [doi: 10.1109/LSP.2013.2240385]

[36] Denemark T, Fridrich JJ, Holub V. Further study on the security of S-UNIWARD. In: Media Watermarking, Security, and Forensics. 2014. 902805. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9028/902805/Further-study-on-the-security-of-S-UNIWARD/10.1117/12.2044803.full?SSO=1

[37] Holub V, Fridrich JJ. Phase-Aware projection model for steganalysis of JPEG images. In: Media Watermarking, Security, and Forensics. 2015. 94090T. [doi: 10.1117/12.2075239]

[38] Holub V, Fridrich J. Low-Complexity features for JPEG steganalysis using undecimated DCT. IEEE Trans. on Information Forensics and Security, 2015,10(2):219–228. [doi: 10.1109/TIFS.2014.2364918]

[39] Song X, Liu F, Yang C, Luo X, Zhang Y. Steganalysis of adaptive JPEG steganography using 2D Gabor filters. In: Proc. of the 3rd ACM Workshop on Information Hiding and Multimedia Security. ACM, 2015. 15–23. [doi: 10.1145/2756601.2756608]

[40] Zheng GH, Feng GR, Yu J, Cheng H, Zhang XP. JPEG steganalysis based on LSB detection and enhanced features. Journal of Applied Sciences, 2016,34(6):670–676 (in Chinese with English abstract).

[41] Tang W, Li H, Luo W, Huang J. Adaptive steganalysis against WOW embedding algorithm. In: Proc. of the 2nd ACM Workshop on Information Hiding and Multimedia Security. ACM, 2014. 91–96. [doi: 10.1145/2600918.2600935]

[42] Denemark TD, Boroumand M, Fridrich J. Steganalysis features for content-adaptive JPEG steganography. IEEE Trans. on Information Forensics and Security, 2016,11(8):1736–1746. [doi: 10.1109/TIFS.2016.2555281]

[43] Denemark T, Sedighi V, Holub V, Cogranne R, Fridrich J. Selection-Channel-Aware rich model for steganalysis of digital images. In: Proc. of the 2014 IEEE Int'l Workshop on Information Forensics and Security (WIFS). IEEE, 2014. 48–53. [doi: 10.1109/WIFS.2014.7084302]

[44] Zhang Y, Liu F, Yang C, Luo XY, Song XF, Lu J. Steganalysis of content-adaptive JPEG steganography based on Gauss partial derivative filter bank. Journal of Electronic Imaging, 2017,26(1):013011. [doi: 10.1117/1.JEI.26.1.013011]

[45] Qian Y, Dong J, Wang W, Tan T. Deep learning for steganalysis via convolutional neural networks. Media Watermarking, Security, and Forensics, 2015,9409:94090J. [doi: 10.1117/12.2083479]

[46] Lubenko I, Ker AD. Going from small to large data in steganalysis. Media Watermarking, Security, and Forensics, 2012,8303: 0M01–0M10. [doi: 10.1117/12.910214]

[47] Kodovský J, Sedighi V, Fridrich JJ. Study of cover source mismatch in steganalysis and ways to mitigate its impact. In: Media Watermarking, Security, and Forensics. 2014. 90280J. [doi: 10.1117/12.2039693]

[48] Lerch-Hostalot D, Megías D. Unsupervised steganalysis based on artificial training sets. Engineering Applications of Artificial Intelligence, 2016,50:45–59. [doi: 10.1016/j.engappai.2015.12.013]

[49] Ker AD, Pevný T. A mishmash of methods for mitigating the model mismatch mess. In: Media Watermarking, Security, and Forensics. 2014. 90280I. [doi: 10.1117/12.2038908]

附中文参考文献:

[3] 王朔中,张新鹏,张开文.数字密写和密写分析:互联网时代的信息战技术.北京:清华大学出版社有限公司,2005.

[23] 王朔中,张新鹏,张卫明.以数字图像为载体的隐写分析研究进展.计算机学报,2009,32(7):1247–1263. [doi: 10.3724/SP.J.1016.2009.01247]

[34] 黄炜,赵险峰,冯登国,盛任农.基于主成分分析进行特征融合的 JPEG 隐写分析.软件学报,2012,23(7):1869–1879. http://www.jos.org.cn/1000-9825/4107.htm [doi: 10.3724/SP.J.1001.2012.04107]

[40] 郑国华,冯国瑞,余江,程航,张新鹏.基于 LSB 检测的 JPEG 隐写分析特征增强方法.应用科学学报,2016,34(6):670–676.

张逸为(1991－),男,吉林省吉林市人,学士,主要研究领域为信息隐藏,人工智能.

俞能海(1964－),男,博士,教授,博士生导师,CCF 专业会员,主要研究领域为多媒体数据处理与分析、检索,互联网信息检索(社区,标注),数字内容安全(云计算与云计算安全).

张卫明(1976－),男,博士,教授,博士生导师,CCF 专业会员,主要研究领域为信息隐藏,密文域计算.