Proceedings on Privacy Enhancing Technologies, 3. Rochester NY, United States: Privacy Enhancing Technologies Board: 212–225[DOI:10.1515/popets-2016-0024]

Kaptchuk G, Jois T M, Green M and Rubin A D. 2021. Meteor: Cryptographically secure steganography for realistic distributions//In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, United States: ACM: 1529-1548[DOI: 10.1145/3460120.3484550]

Kerckhoffs A. 1883. La cryptographie militaire. J. Sci. Militaires, 9(4)[DOI:10.4000/bibnum.555]

Kohls K, Holz T, Kolossa D and Pöpper C. 2016. SkypeLine: Robust hidden data transmission for VoIP//In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. New York, NY, United States: ACM: 877-888[DOI: 10.1145/2897845.2897913]

Peng J, Jiang Y, Tang S and Meziane F. 2019. Security of streaming media communications with logistic map and self-adaptive detection-based steganography//IEEE Transactions on Dependable and Secure Computing, 18(4):1962-1973[DOI: 10.1109/TDSC.2019.2946138]

Reimers N and Gurevych I. 2019. Sentence-bert: Sentence embeddings using siamese bert-networks[EB/OL]. [2019-8-27]. https://doi.org/10.48550/arXiv.1908.10084

Ren Y, Ruan Y, Tan X, Qin T, Zhao S, Zhao Z and Liu T Y. 2019. Fastspeech: Fast, robust and controllable text to speech// Advances in neural information processing systems, 32. San Diego, CA, USA: NIPS[DOI:10.5555/3454287.3454572]

Rosen M B, Parker J and Malozemoff A J. 2021. Balboa: Bobbing and weaving around network censorship//In 30th USENIX Security Symposium. CA, USA: USENIX Association: 3399-3413[DOI:10.48550/arXiv.2104.05871]

Saenger J, Mazurczyk W, Keller J and Caviglione L. 2020. Vo IP network covert channels to enhance privacy and inform ation sharing. Future Generation Computer Systems, 111. The Netherlands: Elsevier: 96-106[DOI:10.1016/j.future.202 0.04.032]

Salton G and Buckley C. 1988. Term-weighting approaches in automatic text retrieval. Information processing & manage ment, 24(5). The Netherlands: Elsevier: 513-523[DOI:10.10 16/0306-4573(88)90021-0]

Tian J, Xiong G, Li Z and Gou G. 2020. A survey of key technologies for constructing network covert channel. Security and Communication Networks, 2020. Egypt: Hindawi: 1-20[DOI: 10.1155/2020/8892896]

Vaswani A, Shazeer N, Parmar N, Uszkoreit J, Jones L, Gomez A N, Kaiser Ł and Polosukhin I. 2017. Attention is all you need//Advances in neural information processing systems, 30. San Diego, CA, USA: NIPS[DOI:10.48550/arXiv.1706.03762]

Wang Y, Skerry-Ryan R J, Stanton D, Wu Y, Weiss R J, Jaitl y N, Yang, Z, Xiao Y, Chen Z, Bengio S and Le Q. 201 7. Tacotron: Towards end-to-end speech synthesis[EB/OL]. [2017-05-29].https://doi.org/10.48550/arXiv.1703.10135

Yujian L and Bo L. 2007. A normalized Levenshtein distance metric. IEEE transactions on pattern analysis and machine intelligence, 29(6): 1091-1095[DOI:10.1109/TPAMI.2007.1078]

Zhang W M, Wang H X, Li B, Ren Y Z, Yang Z L, Chen K J, Li W X, Zhang X P, Yu N H . 2022. Overview of steganography on multimedia. Journal of Image and Graphics, 27(6): 1918-1943. (张卫明, 王宏霞, 李斌, 任延珍, 杨忠良, 陈可江, 李伟祥, 张新鹏, 俞能海. 2022. 多媒体隐写研究进展. 中国图象图形学报, 27(6): 1918-1943.) [DOI: 10.11834/jig.211272]

作者简介

张晏铭，男, 硕士生, 研究方向为隐蔽通信。E-mail：azesinter@mail.ustc.edu.cn

陈可江，通信作者，男，研究员，研究方向为信息隐藏，可证明安全隐写，人工智能安全，隐私保护。E-mail：chenkj@ustc.edu.cn

丁锦扬，男，硕士生，主要研究方向为信息隐藏，人工智能安全，隐私保护。E-mail：source@mail.ustc.edu.cn

张卫明，男，教授，主要研究方向为信息隐藏，数字水印，对抗样本，深度伪造与检测。E-mail：zhangwm@ustc.edu.cn

俞能海，男，教授，主要研究方向为图像处理，信息隐藏，数据安全。E-mail：ynh@ustc.edu.cn