BIBLIOGRAPHY

[1] about$_e$scape$_c$haracters. *https : //technet.microsoft.com/en − us/library/hh*847755.*aspx. Accessed* : 2022 − 09 − 20.

[2] M. T. Ahvanooey, H. D. Mazraeh, and S. H. Tabasi. An innovative technique for web text watermarking (aitw). *Information Security Journal: A Global Perspective*, 25:191–196, 12 2016. ISSN 1939-3555. doi: 10.1080/19393555.2016.1202356.

[3] M. T. Ahvanooey, Q. Li, J. Hou, H. D. Mazraeh, and J. Zhang. Aitsteg: An innovative text steganography technique for hidden transmission of text message via social media. *IEEE Access*, 6:65981–65995, 2018. ISSN 2169-3536. doi: 10.1109/ACCESS.2018.2866063.

[4] M. T. Ahvanooey, Q. Li, H. J. Shim, and Y. Huang. A comparative analysis of information hiding techniques for copyright protection of text documents. *Security and Communication Networks*, 2018:1–22, 2018. ISSN 1939-0114. doi: 10.1155/2018/5325040.

[5] M. T. Ahvanooey, Q. Li, J. Hou, A. R. Rajput, and C. Yini. Modern text hiding, text steganalysis, and applications: A comparative analysis. *Entropy*, 21:355, 4 2019. ISSN 1099-4300. doi: 10.3390/e21040355.

[6] M. T. Ahvanooey, Q. Li, X. Zhu, M. Alazab, and J. Zhang. Anitw: A novel intelligent text watermarking technique for forensic identification of spurious information on social media. *Computers Security*, 90:101702, 3 2020. ISSN 01674048. doi: 10.1016/j.cose.2019.101702.

[7] M. H. Alkawaz, G. Sulong, T. Saba, A. S. Almazyad, and A. Rehman. Concise analysis of current text automation and watermarking approaches. *Security and Communication Networks*, 9:6365–6378, 12 2016. ISSN 19390114. doi: 10.1002/sec.1738.

[8] M. Azeem, J. He, A. Ditta, and F. Akhtar. A novel approach to secret data concealment with high cover text capacity and security. *International Journal of Electronic Security and Digital Forensics*, 12:1, 2020. ISSN 1751-911X. doi: 10.1504/IJESDF.2020.10020454.

[9] H. M. Bashir, Q. Li, and J. Hou. A high capacity text steganography utilizing unicode zero-width characters. pages 668–675. IEEE, 11 2020. ISBN 978-1-7281-7647-5. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00116.

[10] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192:41–56, 7 2004. ISSN 08905401. doi: 10.1016/j.ic.2004.02.003.

[11] L. Chen, D. Moody, A. Regenscheid, and K. Randall. Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters (national institute of standards and technology, gaithersburg, md), draft nist special publication (sp) 800-186. *NIST Special Publication (SP)*, pages 800–186, 2019.

[12] J. C. Choon and J. H. Cheon. An identity-based signature from gap diffie-hellman groups, 2003.

[13] S. Deliri and M. Albanese. Security and privacy issues in social networks, 2015.

[14] S. Dixon. Number of social media users worldwide from 2018 to 2027, 7 2022.

[15] G. Gupta. What is birthday attack?? *February*, 2015.

[16] F. Hess. Efficient identity based signature schemes based on pairings, 2003.

[17] N. Hidayah. Laporan pemetaan hoaks edisi desember 2021, 2021.

[18] A. Hutchinson. Internal research from facebook shows that re-shares can significantly amplify misinformation, 5 2021.

[19] N. F. Johnson. Frank y. shih * digital watermarking and steganography: Fundamentals and techniques. crc/taylor amp; francis (2008). * isbn-13: 9781420047578. 46.99. 180 pp. hardcover. *The Computer Journal*, 53:616–617, 6 2010. ISSN 0010-4620. doi: 10.1093/comjnl/bxp057.

[20] D. M. Kar and I. Ray. Systematization of knowledge and implementation: Short identity-based signatures, 2019. URL `https://arxiv.org/abs/1908.05366`.

[21] E. Kiltz and G. Neven. Identity-based signatures. 2009.

[22] S. Kingslin. Evaluative approach towards text steganographic techniques. *Indian Journal of Science and Technology*, 8:1–8, 1 2015. ISSN 09746846. doi: 10.17485/ijst/2015/v8i29/84415.

[23] R. Kumar, S. Chand, and S. Singh. An efficient text steganography sheme using unicode space characters. *The International Journal of Forensic Computer Science*, 10:8–14, 12 2015. ISSN 18099807. doi: 10.5769/J201501001.

[24] S. Lee and J. Kim. Warningbird: A near real-time detection system for suspicious urls in twitter stream. *IEEE Transactions on Dependable and Secure Computing*, 10:183–195, 5 2013. ISSN 1545-5971. doi: 10.1109/TDSC.2013.3.

[25] S. Midorikawa. ecpy. `https://github.com/elliptic-shiho/ecpy`, 2013.

[26] S. Mishra, R. Yaduvanshi, K. Dubey, and P. Rajpoot. Ess-ibaa: Efficient, short, and secure id-based authentication algorithm for wireless sensor network. *International Journal of Communication Systems*, 34, 5 2021. ISSN 1074-5351. doi: 10.1002/dac.4764.

[27] N. Naqvi, A. T. Abbasi, R. Hussain, M. A. Khan, and B. Ahmad. Multilayer partially homomorphic encryption text steganography (mlphe-ts): A zero steganography approach. *Wireless Personal Communications*, 103:1563–1585, 11 2018. ISSN 0929-6212. doi: 10.1007/s11277-018-5868-1.

[28] K. G. Paterson and J. C. N. Schuldt. Efficient identity-based signatures secure in the standard model, 2006.

[29] R. Petrovic, B. Tehranchi, and J. M. Winograd. Security of copy-control watermarks. pages 117–126. IEEE, 9 2007. ISBN 978-1-4244-1467-3. doi: 10.1109/TELSKS.2007.4375954.

[30] L. Y. Por, K. Wong, and K. O. Chee. Unispach: A text-based data hiding method using unicode space characters. *Journal of Systems and Software*, 85:1075–1082, 5 2012. ISSN 01641212. doi: 10.1016/j.jss.2011.12.023.

[31] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park. Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421:43–69, 12 2017. ISSN 00200255. doi: 10.1016/j.ins.2017.08.063.

[32] R. SAKAI. Cryptosystems based on pairing. *Proc. of SCIS2000, Jan.*, 2000. URL `https://cir.nii.ac.jp/crid/1570291225722108672.bib?lang=en`.

[33] D. R. I. M. Setiadi. Psnr vs ssim: imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications*, 80(6):8423–8444, 2021.

[34] A. Shamir. Identity-based cryptosystems and signature schemes.

[35] P. Singh and R. Chadha. A survey of digital watermarking techniques, applications and attacks. 2 2013.

[36] Y. Wang and P. Moulin. Perfectly secure steganography: Capacity, error exponents, and code constructions. *IEEE Transactions on Information Theory*, 54:2706–2722, 6 2008. ISSN 0018-9448. doi: 10.1109/TIT.2008.921684.

[37] Z. Wang, E. P. Simoncelli, and A. C. Bovik. Multiscale structural similarity for image quality assessment. In *The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, 2003*, volume 2, pages 1398–1402. Ieee, 2003.

[38] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli. Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, 13 (4):600–612, 2004.

[39] R. Yaduvanshi and S. Mishra. An efficient and secure pairing free short id-based signature scheme over elliptic curve. *SSRN Electronic Journal*, 2019. ISSN 1556-5068. doi: 10.2139/ssrn.3351027.

[40] X. Yi. An identity-based signature scheme from the weil pairing. *IEEE Communications Letters*, 7:76–78, 2 2003. ISSN 1089-7798. doi: 10.1109/LCOMM.2002.808397.

[41] X. Zhou, Z. Wang, W. Zhao, and J. Yu. Attack model of text watermarking based on communications. pages 283–286. IEEE, 2009. ISBN 978-0-7695-3876-1. doi: 10.1109/ICIII.2009.529.