Table 5 Feature vector of encryption image *B*1

表 5 加密图像 *B*1 的特征向量

Band	[0,15]	[16,31]	[32,63]	[64,127]	[128,255]
Band1	3 799 979	0	32 529 202	2 088 167	35 053
Band2	3 799 923	2 332	32 831 600	1 775 780	42 766
Band3	3 799 501	2 095 244	31 175 656	1 342 153	39 847
Band4	3 799 592	14 151 801	19 317 795	1 131 471	51 742
Band5	3 799 527	761 267	12 231 624	21 522 685	137 298
Band6	3 799 321	5 002 121	27 836 114	1 757 828	57 017
Band7	3 799 266	18 954 718	15 204 761	491 416	2 240
Band8	7 131 489	11 632 707	19 357 261	312 294	18 650
Band9	3 809 144	33 266 341	1 374 755	2 161	0
Band10	4 221 402	17 204	1 485 981	32 726 772	1 042
Band11	4 230 696	5 401	1 899 292	32 317 012	0

Table 6 Spend time of remote sensing image *B* in encryption/decryption

表 6 遥感图像 *B* 的加解密花费时间

Band	加密(s)	解密(s)	统计时间(s)
Band1	13.323 389	10.768 238	0.717 080
Band2	13.513 761	10.866 348	0.687 446
Band3	13.193 458	10.852 150	0.633 438
Band4	13.556 960	10.864 505	0.790 736
Band5	13.542 970	10.826 749	0.834 203
Band6	13.358 904	10.868 542	0.785 743
Band7	13.665 921	10.845 543	0.838 826
Band8	13.349 951	10.928 417	0.791 156
Band9	13.259 332	10.833 223	0.754 108
Band10	13.141 191	10.789 564	0.685 070
Band11	13.119 520	10.780 581	0.660 981

由图 7、图 8 可得:本文利用算法 1 对遥感图像的灰度值进行加密处理,加密后遥感图像的灰度值在原图像灰度值密集区域内处于均匀分布的状态,在灰度值稀疏区域,加密后的图像加入了背景噪声.掩盖了原遥感图像的直方图统计分布,攻击者很难从密文图像获取到正确的地物信息,从而在灰度值统计方面保证了原遥感图像的安全性.本方案的加密算法保证在无需建立索引的情况下支持密文的检索,且密文遥感图像的灰度值在统计区间范围内不受影响.根据密文图像数据量的大小,从多幅遥感图像中分别检索出目标遥感图像所要花费的时间如图 9 所示.本文密文匹配的检索算法适合在云服务器上完成,在保证遥感图像安全的同时缩短了检索所花销的时间.

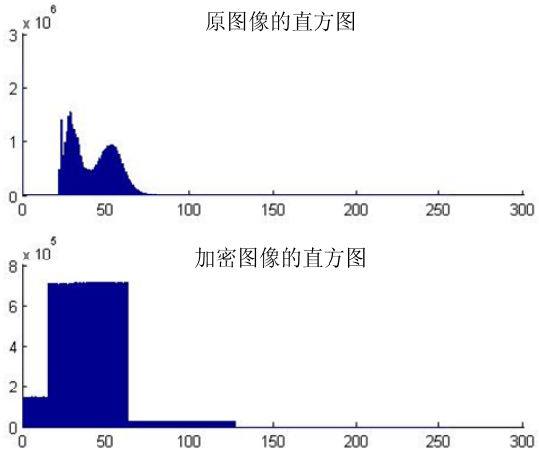


Fig.7 Histogram of original/encryption in remote sensing image *A*

图 7 遥感图像 *A* 加密前后的直方图

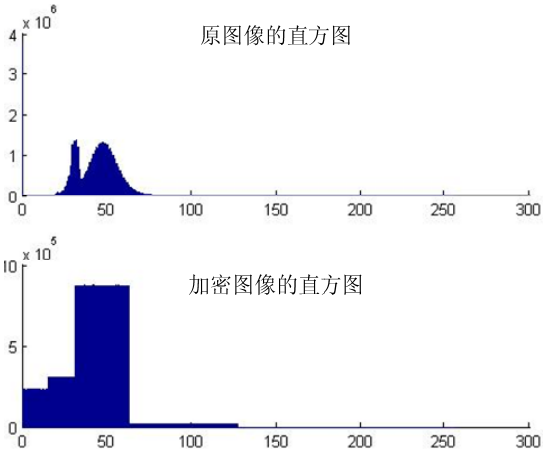


Fig.8 Histogram of original/encryption in remote sensing image *B*

图 8 遥感图像 *B* 加密前后的直方图

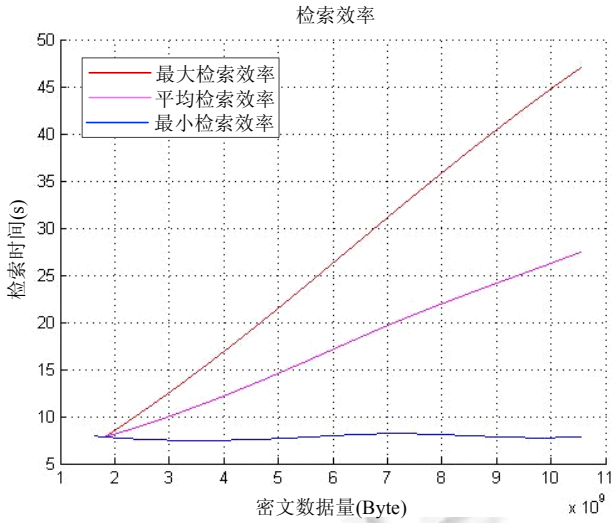


Fig.9 Query efficiency of ciphertext in remote sensing image

图 9 密文遥感图像的检索效率

5.2 安全性与性能分析

在设计加密算法时,需要在攻击模型下分析其安全性.改进的 Henon 映射加密算法是一种对称加密算法,因此可从密钥方面对其进行安全分析.在运用 Henon 映射进行加密时,密钥 a,b 是可以通过物理隔离的,因此,攻击的第三方很难从密钥 a,b 入手获取到遥感图像的信息.此外,根据上述实验的数据可知,一幅遥感图像的像素空间个数比较大,对于进行了频域加密的随机矩阵,攻击者是很难通过穷举法获得的.

改进的 Henon 映射加密算法涉及到随机数生成操作和异或运算,通过异或运算,隐藏原来遥感图像真实的像素值,保证遥感数据的安全性.同时,满足通过云服务器进行密文的检索匹配,用户本地运算量小、计算复杂度低、成本开销小,实现了在无需建立索引的基础上直接对加密的遥感图像的安全检索.

6 结束语

图像加密的原理是:改变原来图像的灰度信息,扰乱图像中像素的位置或灰度值,使一幅有意义的图像变得难以辨认.但是现有的加密算法一般不支持在密文上进行直接检索,因此,本文提出了一种改进的 Henon 映射加密方案,可以在无需建立索引的情况下直接对加密的遥感图像进行安全检索,既减少了磁盘存储容量,同时又不需要在解密的情况下实现对密文的直接检索,缩短了检索所消耗的时间,从而提高了密文遥感图像的可用性.下一步的工作是寻找优化方法,采用基于二叉树的搜索方法实现对密文空间数据的递归划分,以提高海量的遥感图像的加密与检索效率,减少运行时间.

References:

[1] Zhuang L, Zhuang YT, Wu JQ, Ye ZC, Wu F. Image retrieval approach based on sparse canonical correlation analysis. Ruan Jian Xue Bao/Journal of Software, 2012,23(5):1295−1304 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4032.htm [doi: 10.3724/SP.J.1001.2012.04032]

[2] Li W, Duan L, Xu D, Tsang IW. Text-Based image retrieval using progressive multi-instance learning. In: Proc. of the ICCV. 2011. 2049−2055. [doi: 10.1109/ICCV.2011.6126478]

[3] Flickner M, Sawhney H, Niblack W, Ashley J, Huang Q, Dom B, Gorkani M, Hafner J, Lee D, Petkovic D, Steele D, Yanker P. Query by image and video content: The QBIC system. IEEE Computer, 1995,28(9):23−32. [doi: 10.1109/2.410146]

© 中国科学院软件研究所 http://www.jos.org.cn

[4] Shi W, Zhu XF. Image retrieval based on contour reconstruction and feature point chord length. Ruan Jian Xue Bao/Journal of Software, 2014,25(7):1557−1569 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4443.htm [doi: 10.13328/j.cnki.jos.004443]

[5] Cao N, Yang Z, Wang C, Ren K, Lou W. Privacy-Preserving query over encrypted graph-structured data in cloud computing. In: Proc. of the Distributed Computing Systems (ICDCS). 2011. 393−402. [doi: 10.1109/ICDCS.2011.84]

[6] Cao N, Wang C, Li M, Ren K, Lou W. Privacy-Preserving multi-keyword ranked search over encrypted cloud data. In: Proc. of the IEEE INFOCOM. 2011. 393−402. [doi: 10.1109/ICDCS.2011.84]

[7] Zhu XD, Li H, Guo Z. Privacy-Preserving query over the encrypted image in cloud computing. Journal of Xidian University, 2014, 41(2):151−158 (in Chinese with English abstract). [doi: 10.3969/j.issn.1001-2400.2014.02.025]

[8] Liu Q, Wang GJ, Wu J. An efficient privacy preserving keyword search scheme in cloud computing. In: Proc. of the 12th IEEE Int'l Conf. on Computational Science and Engineering (CSE 2009). Vancouver, 2009. 715−720. [doi: 10.1109/CSE.2009.66]

[9] Chase M, Kamara S. Structured encryption and controlled disclosure. In: Proc. of the Advances in Cryptology (ASIACRYPT 2010). LNCS 6477, Berlin, Heidelberg: Springer-Verlag, 2010. 577−594. [doi: 10.1007/978-3-642-17373-8_33]

[10] Boneh D, Crescenzo GD, Ostrovsky R, Persiano G. Public key encryption with keyword search. In: Proc. of the Eurocrypt 2004. LNCS 3027, Berlin, Heidelberg: Springer-Verlag, 2004. 506−522.

[11] Song DX, Wagner P, Perrig P. Practical techniques for searches on encrypted data. In: Proc. of the 2000 IEEE Symp. on Security and Privacy. Berkeley, 2000. 44−55. [doi: 10.1109/SECPRI.2000.848445]

[12] Wang WC, Li ZW, Owens R, Bhargava B. Secure and efficient access to outsourced data. In: Proc. of the 2009 ACM Workshop on Cloud Computing Security. Chicago, 2009. 55−66. [doi: 10.1145/1655008.1655016]

[13] Huang RW, Gui XL, Yu S, Zhuang W. Privacy-Preserving computable encryption scheme of cloud computing. Chinese Journal of Computers, 2011,34(12):2391−2402 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.02391]

[14] Wang C, Cao N, Li J, Ren K, Lou W. Secure ranked keyword search over encrypted cloud data. In: Proc. of the ICDCS 2010. 2010. [doi: 10.1109/ICDCS.2010.34]

[15] Bellovin S, Cheswick W. Privacy-Enhanced searches using encrypted bloom filters. Technical Report, 2004/022, Cryptology ePrint Archive, 2004. http://eprint.iacr.org/2004/022/

[16] Cheon JH, Kim M, Kim M. Search-and-Compute on encrypted data. In: Proc. of the Financial Cryptography and Data Security-FC Int'l Workshop WAHC. LNCS 8976, Berlin, Heidelberg: Springer-Verlag, 2015. 142−159. [doi: 10.1007/978-3-662-48051-9_11]

[17] Zhang X, Peng P, Huang QL. Design and implementation of query over encrypted data. Journal of Yunnan University, 2010,32(6): 646−651 (in Chinese with English abstract).

[18] Prasad M, Sudha KL. Chaos image encryption using pixel shuffling. In: Proc. of the CCSEA (CS&IT 2002). 2011. 169−179. [doi: 10.5121/csit.2011.1217]

[19] Maniccam SS, Bourbakis NG. Image and video encryption using SCAN patterns. Pattern Recognition, 2004,37:725−737. [doi: 10.1016/j.patcog.2003.08.011]

[20] Zheng F, Tian XJ, Fan WH, Li XY, Gao B. Image encryption based on henon map. Journal of Beijing University of Posts and Telecommunications, 2008,31(1):66−70 (in Chinese with English abstract).

[21] Zhang H, Wang XF, Li ZH, Liu DH. A fast image encryption algorithm based on chaos system and henon map. Journal of Computer Research and Development, 2005,42(12):2137−2142 (in Chinese with English abstract). [doi: 10.1360/crad20051216]

附中文参考文献:

[1] 庄凌,庄越挺,吴江琴,叶振超,吴飞.一种基于稀疏典型性相关分析的图像检索方法.软件学报,2012,23(5):1295−1304. http://www.jos.org.cn/1000-9825/4032.htm [doi: 10.3724/SP.J.1001.2012.04032]

[4] 师文,朱学芳.基于轮廓重构和特征点弦长的图像检索.软件学报,2014,25(7):1557−1569. http://www.jos.org.cn/1000-9825/4443.htm [doi: 10.13328/j.cnki.jos.004443]

[7] 朱旭东,李晖,郭祯.云计算环境下加密图像检索.西安电子科技大学学报(自然科学版),2014,41(2):151−158. [doi: 10.3969/j.issn.1001-2400.2014.02.025]

© 中国科学院软件研究所 http://www.jos.org.cn

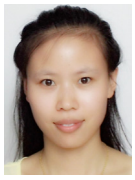
[13] 黄汝维,桂小林,余思,庄威.云环境中支持隐私保护的可计算加密方法.计算机学报,2011,34(12):2391−2402. [doi: 10.3724/SP.J.1016.2011.02391]

[17] 张璇,彭朋,黄勤龙.数据库密文检索技术的设计与实现.云南大学学报,2010,32(6):646−651.

[20] 郑凡,田小建,范文华,李雪研,高博.基于 Henon 映射的数字图像加密.北京邮电大学学报,2008,31(1):66−70.

[21] 张瀚,王秀峰,李朝晖,刘大海.一种基于混沌系统及 Henon 映射的快速图像加密算法.计算机研究与发展,2005,42(12):2137−2142. [doi: 10.1360/crad20051216]

黄冬梅(1964－),女,河南郑州人,教授,博士生导师,CCF 高级会员,主要研究领域为海洋数据管理,信息智能处理,辅助决策.



耿霞(1988－),女,硕士生,CCF 学生会员,主要研究领域为遥感信息安全.

魏立斐(1982－),男,博士,讲师,CCF 会员,主要研究领域为信息安全,密码学.

苏诚(1962－),男,教授级高工,主要研究领域为海洋灾害辅助决策系统建设,大型海洋信息化系统构建,海洋工程勘察与数值计算,海洋测绘,空间信息技术.

© 中国科学院软件研究所 http://www.jos.org.cn