软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(7):1729−1740 [doi: 10.13328/j.cnki.jos.005039]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于 Henon 映射的加密遥感图像的安全检索方案*

黄冬梅[1], 耿 霞[1], 魏立斐[1], 苏 诚[1,2]

[1](上海海洋大学 信息学院,上海 201306)

[2](国家海洋局 东海分局预报中心,上海 200137)

通讯作者: 魏立斐, E-mail: lfwei@shou.edu.cn

摘 要: 遥感图像具有多时相、多语义、多波段等特点,鉴于遥感图像在商业行业及国防军事中的重要性,海量遥感图像密文检索的效率和精度直接影响了遥感大数据使用的广泛性和实时性.对密文存储的遥感大数据的安全检索,是其可用性最重要的标志之一.提出了一种基于 Henon 映射的遥感图像可搜索加密方案,根据遥感图像的成像原理及多波段特征,采用改进的 Henon 映射对每个波段的灰度值进行加密处理.同时,根据遥感图像的“大数据”特征,通过统计灰度值的区间信息来构造遥感图像的特征向量,并根据相似度匹配算法来检索目标图像.通过对 Landsat 8 遥感图像进行加密与检索进行实验,结果表明,该方案有效地提高了检索密文遥感图像的安全性及准确性,且计算复杂度低、通信成本开销小.

关键词: 遥感图像;遥感大数据;密文检索;Henon 映射;特征向量

中图法分类号: TP391

中文引用格式: 黄冬梅,耿霞,魏立斐,苏诚.基于 Henon 映射的加密遥感图像的安全检索方案.软件学报,2016,27(7): 1729−1740. http://www.jos.org.cn/1000-9825/5039.htm

英文引用格式: Huang DM, Geng X, Wei LF, Su C. A secure query scheme on encrypted remote sensing images based on Henon mapping. Ruan Jian Xue Bao/Journal of Software, 2016,27(7):1729−1740 (in Chinese). http://www.jos.org.cn/1000-9825/5039.htm

A Secure Query Scheme on Encrypted Remote Sensing Images Based on Henon Mapping

HUANG Dong-Mei[1], GENG Xia[1], WEI Li-Fei[1], SU Cheng[1,2]

[1](College of Information and Technology, Shanghai Ocean University, Shanghai 201306, China)

[2](East China Sea Branch of State Oceanic Administration People’s Republic of China, Shanghai 200137, China)

Abstract: Remote sensing image has the characteristics of multi-temporal, multi-semantic and multi-spectral, and it plays an important role in different industries and military. It is a significant issue that the efficiency and accuracy of ciphertext query on the huge amounts of remote sensing image have direct impact on the remote sensing big data in its general applicability and real-time performance. For ciphertext, secure-retrieval on remote sensing big data is one of the important standards on the usability of remote sensing image. This paper first proposes an encryption/query scheme on remote sensing image including encryption algorithm and query algorithm, and then constructs an image query scheme on the encrypted remote sensing image based on the improved Henon mapping. Based on the imaging principle and multi-band remote sensing image characteristics, the paper takes the improved Henon mapping technique to encrypt the gray value of remote sensing image for each band. According to the characteristics of “remote sensing big data”, the process extracts the feature vector by the statistical gray values for each band, and then queries the target remote image based on matching algorithm. Finally,

* 基金项目: 国家重点基础研究发展计划(973)(2012CB316206); 国家自然科学基金(61272098, 61402282); 上海市科学技术委员会科研计划(15590501900, 14YF1404200)

Foundation item: National Basic Research Program of China (973) (2012CB316206); National Nature and Science Foundation of China (61272098, 61402282); Project of Science and Technogoly Commission of Shanghai Municipality (15590501900, 14YF1404200)

收稿时间: 2015-10-10; 修改时间: 2016-01-12; 采用时间: 2016-02-22; jos 在线出版时间: 2016-03-22;

CNKI 网络优先出版: 2016-03-22 13:23:34, http://www.cnki.net/kcms/detail/11.2560.TP.20160322.1323.007.html

© 中国科学院软件研究所 http://www.jos.org.cn

experiments are carried out on encrypting and processing the big data of Landsat 8 remote sensing satellites, the experimental results show that the presented algorithms effectively improve the security and accuracy on the usage of remote sensing image. Meanwhile, the scheme has a low computational complexity and communication cost.

Key words: remote sensing image; remote sensing big data; ciphertext query; Henon mapping; feature vector

在信息全球化的背景下,遥感图像以其可视化、全球化、网络化以及智能化的特点在各行各业中显示出了令人瞩目的优势与潜力,尤其在信息获取与数据分析处理方面展示了其独特的魅力.随着“空天地底”海洋立体观测遥感技术的飞速发展,催生了高精度、高频度、大覆盖的遥感数据呈几何级数爆炸式增长.海洋遥感数据以 TB 级/天的规模增加,目前已达到 EB 级,成为公认的“大数据”.海洋遥感大数据已成为海洋灾害动态监测、实时追踪、快速预警和辅助决策的重要数据来源.如何提高遥感数据的可用性,使数据使用者能够安全地从多时相、多语义、多波段中快速检索出目标图像,已经成为一个重要的研究课题.随着遥感数据的多元化和海量化,遥感数据已经呈现出明显的“大数据”特征,传统的数据分析方法已经难以处理.遥感图像作为一种重要的时空数据,已经在环境监测、灾害预报、国防安全等重大领域发挥着不可或缺的作用.同时,作为国家重要的战略性、基础性信息资源,在军事领域具有重要的决策地位.为了防止遥感图像在传输、存储、共享过程中受到恶意的截取或破坏,亟需可靠的技术手段对其进行加密保护.

大数据环境下,相似图像搜索原理已变得越来越受关注,为了提高数据的可用性,“以图搜图”的新型搜索模式应运而生.“以图搜图”是在原图像的基础上,搜索与之相似或相关的图片信息.相似图像搜索的原理主要有:(1) 基于内容特征的提取;(2) 基于图像信息的编码;(3) 相似度匹配算法.随着互联网上的各类图像资源增长速度惊人,需要在海量的图像数据中快速地检索出目标图像,其中,影响大数据检索效率最本质的原因可以归结为:(1) 建立索引,减少读取的数据;(2) 数据本地化;(3) 更多的服务器;(4) 更优化的检索算法.

遥感图像加密和检索的效率和精度,直接影响了遥感图像数据的运用.基于遥感图像在国防安全中的特殊性,我们需要在海量的加密数据中快速、安全地检索出目标文件.由于目前的大多数加密体制并不适合在加密的遥感图像上进行直接检索,因此,本文根据遥感图像的成像原理及多波段特征,采用改进的 Henon 映射对每个波段的灰度值进行加密处理.同时,并根据遥感图像的“大数据“特征,通过统计灰度值的区间信息来构造遥感图像的特征向量,并根据相似度匹配算法来检索目标图像.本文提出的加密检索方法可以直接构建明文与密文之间的映射关系,该方案的优点是无需预先构造描述加密图像的索引,且计算复杂度低,可提高密文遥感图像的可用性.

本文第 1 节介绍相关工作.第 2 节是预备知识.第 3 节提出基于改进的 Henon 映射的遥感图像加密算法.第 4 节提出加密遥感图像的检索算法.第 5 节通过实验数据与安全分析,表明方案的高效性与安全性.最后总结全文.

1 相关工作

云计算时代,数据隐私保护的需求极大地推动了密文检索技术的发展,尤其是在大数据分析方法蓬勃兴起的今天,又为密文检索技术的发展带来新的动力.早期的图像检索是基于文本的图像检索(TBIR),利用文本描述的方式对图像的特征进行描述.庄凌等人[1]提出了一种通过研究文本与图像两种模态之间关系来构建反映两者间潜在语义关联的有效模型,该模型通过自然语言形式来表达检索意图,并最终检索到相关图像.但是对海量的图像进行文本描述是一项浩大的工程,且极易出现错误,给检索工作带来难度.Wen 等人[2]利用 TBIR 对网页图像进行分类和学习,但是得到的文本信息表达精度不高,无法用于含有丰富信息的遥感图像方面.为弥补上述不足,基于内容的图像检索应运而生,通过利用图像本身的纹理、形状等特征,从海量的图像中检测出目标图像,目的是为了能够高效率地检索出满足要求的图像信息.IBM 公司开发的最早的商业化 QBIC 系统[3]就是一款经典的基于图像内容的检索系统,用户可以通过选定颜色、形状、纹理和草图去检索图库.师文等人[4]通过分析目标轮廓的能量保持率来对其进行降维重构处理,并把提取的目标轮廓作为重要的形状信息和特征点信息.鉴于遥感图像在军事领域的重要意义,我们需要对其进行相应的加密处理.图像加密的实质是对图像的灰度矩阵进

© 中国科学院软件研究所 http://www.jos.org.cn

行初等变换,从而打乱像素之间的内在关系,使一张有意义的数字图像变得杂乱无章,从而掩盖图像的重要信息.加密后的遥感图像无法直接获得正确的纹理、形状等基本特征,因此需要通过建立索引的方法对密文进行检索[5−7].但是建立索引也有其局限性,尤其是在信息量达到一定数量时,如何在大量的数据中找到最相关的文档具有一定的难度.目前,直接对遥感图像进行加密检索的方案比较罕见.

可计算加密技术在保证数据安全的同时支持对密文的计算,目前的可计算加密技术分为两类:支持检索的加密技术和支持运算的加密技术.Liu 等人[8]提出了一种支持密文检索的对称加密方法,通过关键词,可以高效率地在云客户端上搜索,既保证数据隐私又保证其查询隐私.Chase 和 Kamara[9]提出了一种可搜索的对称加密方法,通过对结构化的数据加密并进行搜索.文献[10−12]提出了基于非对称加密的密文检索方案.文献[13]中设计了一种支持矩阵和向量运算的可计算加密方案 CESVMC,实现了支持对加密字符串的模糊检索和对加密数值数据的四则运算.上述加密方案在用户进行数据外包之前往往需要进行大量的运算操作,这对于遥感大数据来说,在效率方面无疑要大打折扣.针对上述问题,我们设计的加密方案是基于非线性映射与异或运算,支持对加密的遥感图像进行快速的检索匹配.

现有的密文检索方法按照密码构造方案可分为如下 6 种.

(1) 安全索引搜索方法:通过建立密文与关键词之间的关联性来对密文进行搜索,同时支持远程服务器上的密文检索.该方法存在的问题是:算法不支持对文档进行多关键词查询,造成检索效率及准确性较低;攻击者可以从关键词入手获取密文的关键信息,安全性能比较低.同时,对文档进行删除或修改操作会对索引的更新带来问题;

(2) 基于关键词的公钥加密方法:该方法主要是把身份的加密和关键词搜索结合起来,在一定程度上保证了算法的安全性及准确性.缺点是应用范围小,不适合大数据的密文检索;

(3) 保护隐私的排序搜索方法:该方法首先对关键字进行加密保护,然后把整个文档进行加密上传到服务器,通过计算,检索出含有关键词密文的加密文档并对其排序,评价高的返回给用户.该方案的缺点是不适合含有多个关键字的文档进行检索;

(4) 基于全同态加密的检索方法:通过电路元技术能够实现密文的检索和计算.同时,该加密方法能够支持整个密文数据库的检索.但是该方案具有很大的计算成本;

(5) 基于 Hash 函数的密文检索方法:利用对称加密方法和 Hash 技术实现了对数据库的加密和密文的检索.该算法的缺点是:需要额外的存储空间来存储用于检索的校验码,攻击者已从校验码入手进行密文数据库的攻击;

(6) 本文方案加密检索的对象是 GB 级的遥感图像:首先,通过 Henon 映射对遥感图像的位置信息进行置乱;其次,用改进的Henon算法进行灰度值加密,使加密后的密文遥感影像在无需建立索引的情况下支持密文检索;且本地只需要进行一次加解密,其余所有的计算量通过云服务器完成.在提高检索效率的同时以减少本地的运算成本.

相关的方案比较见表 1.

Table 1 Analysis of ciphertext query

表 1 密文检索方法的分析

密文检索方法	适合云计算	支持图像检索	安全性	准确性	检索效率
安全索引搜索方法 Secure ranked keyword search over encrypted cloud data[14]	是	否	低	低	低
基于关键词的公钥加密方法 Public-Key encryption with keyword search[10]	否	否	高	高	低
保护隐私的排序搜索方法 Privacy-Enhanced searches using encrypted bloom filters[15]	否	否	高	低	低
基于同态加密的检索方法 Search-and-Compute on encrypted data[16]	否	否	高	高	低
基于 Hash 函数的密文检索方法 数据库密文检索技术的设计与实现[17]	否	是	低	高	较高
我们的方案	是	是	较高	高	高

© 中国科学院软件研究所 http://www.jos.org.cn

2 预备知识

本文采用的 Henon 映射[18]是一个基于排序的二维非线性系统,其方程如公式(1)所示.

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{1}$$

文献[19]中研究了参数 a,b 对映射的影响,当 $0.54<a<2,0<|b|<1$ 时,系统属于超混沌状态.对一般的 RGB 图像来说,按红绿蓝 3 种不同颜色波段生成的序列的长度是原图像大小的 3 倍;但对于遥感图像而言,正好利用了这一特性对每个波段进行加密运算,从而可以方便地提出每个波段的特征向量.文献[18]中,Prasad,Sudha 提出了运用 Henon 映射对 RGB 图像进行置乱加密,但是加密使用的混沌序列是待加密图像大小的 3 倍,这在一定程度上消耗了存储空间.文献[20,21]中,利用 Henon 映射对图像的灰度值进行加密处理,结合 Henon 映射的优点——设计简单、运算快速、解密准确、安全性高等特点.本文采用的 Henon 映射主要是对遥感图像的像素位置进行多轮迭代置乱,同时结合遥感图像自身的特点——遥感图像的波段性特性(Landsat 8 遥感图像共有 11 个波段)及每幅遥感图像数据量大等特征,使攻击者很难正确地获取到原遥感图像的像素位置信息;其次,在 Henon 映射的基础上,利用改进的算法对遥感图像的灰度值进行加密处理,使得密文图像的灰度值在统计区间满足均匀分布,保证了遥感图像的安全.加密后的密文遥感影像在无需建立索引的情况下支持密文检索,且本地的运算量为一次加解密时间,检索匹配所需要消耗的计算量通过云服务器来完成,在提高检索效率的同时减少了运算成本.

3 基于 Henon 映射的加密算法的改进

本文采用 Henon 映射[18]的核心思想是:通过可逆二维非线性 Henon 映射对图像进行空间范围的置乱,然后通过随机矩阵在一定范围内对遥感图像进行频域加密.该改进的加密算法 $Enc()$的最大优点是:使用的是一种基于排序变换方法及实现快速的异或运算,能够保证密文遥感图像的灰度值在一定的统计区间分布上满足均匀分布,防止了敏感数据泄露.鉴于遥感图像在地物识别技术上对灰度值的要求较高,通过对灰度值进行混淆加密后,很难对原有地物进行分类识别.设 $A(x,y)_{M\times N}$ 为遥感图像,其中,x,y 表示像元的坐标位置,M,N 分别表示遥感图像的长和宽,(x_n,y_n)是遥感图像在第 n 次置换后的空间位置坐标,$DN(x_n,y_n)$为相对应空间位置上的灰度值(digital number,简称 DN,表示遥感图像像元的灰度值),(x_{n+1},y_{n+1})为改变后的像素值位置.由于像素的位置必须为整数,因此 a,b 必须选取整数值.同时,为了最大化地减小相邻像素间的相关性,在空域上进行 r 轮的重复迭代,设置控制秘钥 a,b 和 r 的值,则对遥感图像进行空间位置变换的方程如下:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \bmod M \\ y_{n+1} = bx_n \bmod N \end{cases} \tag{2}$$

为了能够对加密的遥感图像进行方便的检索匹配,需要对随机矩阵进行相应的处理变换,使随机矩阵与遥感图像进行频域加密之后还能保持原有的特征向量.

本文采用的 Henon 混沌映射的核心算法是

$$data(x_{n+1},y_{n+1})=[DN(x_n,y_n)\oplus randint(x_n,y_n)] \bmod G \tag{3}$$

其中,$data(x_{n+1},y_{n+1})$为加密后遥感图像的灰度值矩阵,$randint(x_n,y_n)$为与遥感图像大小相等的随机矩阵,G 表示遥感图像的灰度区间最大值.该取模运算不仅利用其不可逆性增强了加密算法的安全性,同时也抑制了图像噪声的生成,使加密处理后的灰度值仍在有效的灰度值区间内.对于 8bit 的 Landsat8 遥感图像,可取 G=256.基于时间序列的同一地理位置的遥感图像在成像上具有很大的相似性,但又不会完全相同.基于 Hash 函数的抗冲突特性构造的可搜索加密方案,无法找到两个相似的遥感图像满足检索要求.利用取模运算的优势在于:可以根据空间向量的相关度检索出在时间序列上相近的遥感图像,从而做出相应的判断与决策,在密文图像检索过程中满足抗干扰性,提高了密文数据的可用性.

为了能够对加密的遥感图像进行检索,需对随机矩阵 $randint(x_n,y_n)$进行处理变换,加密算法如下.

算法 1. 频域加密的随机矩阵.

输入:遥感图像 A;

© 中国科学院软件研究所 http://www.jos.org.cn

遥感图像的长 M 和宽 N,其空间位置像素值 $A(i,j)$;

采样参数与遥感图像大小相等且随机数波动范围比较大的矩阵 R_1;

输出:可异或的随机矩阵 $randint(x_n,y_n)$.

算法过程:

```
for RS image abscissa i=1 to M {
  RS image ordinate j=1 to N {
    if A(i,j)≥0 && A(i,j)≤15
      R2(i,j)=R1(i,j) mod 16
    else
      if A(i,j)≥16 && A(i,j)≤31
        R2(i,j)=R1(i,j) mod 16
    else
      if A(i,j)≥32 && A(i,j)≤63
        R2(i,j)=R1(i,j) mod 32
        else
          if A(i,j)≥64 && A(i,j)≤127
            R2(i,j)=R1(i,j) mod 64
          else
            if A(i,j)≥128 && A(i,j)≤255
              R2(i,j)=R1(i,j) mod 128
  }
}
Return randint(xn,yn)=R2(i,j)
```

由上述频域加密的算法可知:首先,把遥感图像的灰度值转换成二进制表示;然后,自定义密文图像的搜索区间(即,灰度值的比特位长度),在密文的搜索区间范围内对灰度值进行加密处理.其中,取模运算的优势在于,不仅使灰度值在一定范围的区间内满足均匀分布,保证其灰度值不受统计分布的影响,而且支持该算法的不可逆性,攻击者很难由密文恢复出明文信息,在支持密文遥感图像检索的同时保证了遥感图像的安全.

由加密算法中公式(2)和公式(3)可知,其解密算法 $Dec()$ 为

$$\begin{cases} x_n = (y_{n+1}/b) \bmod M \\ y_n = ((x_{n+1} + ay_{n+1}^2 - 1)/b) \bmod N \\ DN(x_n, y_n) = [data(x_{n+1}, y_{n+1}) \oplus randint(x_n, y_n)] \bmod G \end{cases} \tag{4}$$

根据上述加解密算法,可得到如图 1 所示的加解密流程图.

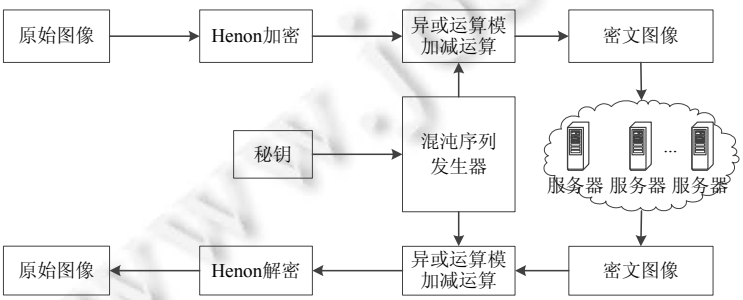


Fig.1 Flow of encryption/decryption algorithm based on improved Henon mapping

图 1 改进的 Henon 映射的加解密流程图

© 中国科学院软件研究所 http://www.jos.org.cn

该算法的优点主要体现在:(1) 通过结合异或运算和模加/减运算,使得破解者无法有效地获取混沌序列,这相对于只运用异或运算对图像进行加密的方法来说,安全性更高,被破解的可能性更低;(2) 对密文的检索无需建立在索引的基础之上,与传统的密文检索相比,更具有安全性,准确性更高.

4 加密遥感图像的检索算法

4.1 遥感图像特征向量的提取

遥感图像的原始数据都是由 DN 值构成的,经过辐射定标转换成具有实际物理意义的反射率值.DN 值的范围是由传感器的量化级别来确定的,如果是 $n$bit 的量化,则 DN 值的范围是 $0\sim(2^n-1)$,那么整个遥感图像的灰度空间共有$(2^n-1)^m$ 种颜色,其中,m 表示遥感图像的波段数,因此具有较大的灰度空间值.

本文采用Landsat 8卫星的遥感数据,下载数据为经典的TIFF格式,根据地物在不同波段表现出来的反射率值可以很容易地判断地物特征,根据加密算法 $Enc()$,密文遥感图像在搜索范围内的灰度值处于均匀分布状态,攻击者很难根据直方图统计判断出具体的地物信息.如图 2 所示,是遥感图像 A 特征向量提取的流程图,为了方便加密过程中的频域加密处理,首先将遥感图像进行灰度值量化预处理;其次判断灰度值区间,得到遥感图像的特征向量Γ,该算法可描述为 $F(A)=\Gamma$.遥感图像特征向量提取的过程主要是在云服务器上执行,在一定程度上不仅提高了检索效率,而且减少了本地的计算量,尤其是对隐私性要求较高的数据,亦可在不可信的云环境中进行存储及检索.

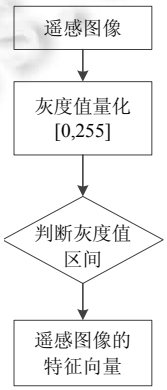


Fig.2 Extraction of feature vector in remote sensing image

图 2 遥感图像的特征向量提取

4.2 遥感图像的相似性匹配

根据遥感图像的特征向量提取方法,可以得到加密之前的遥感图像 A 的特征向量 $F(A)=\Gamma 1$,同理可以得到加密之后的遥感图像其对应的特征向量为 $F(Enc(A))=\Gamma 2$.如图 3 所示,可以通过云服务器快速地匹配原遥感图像的特征向量与加密后的特征向量,对任意的$\varepsilon>0$,满足$|\Gamma 1-\Gamma 2|<\varepsilon$,在无需解密的情况下,快速地查找到所需要的目标图像.

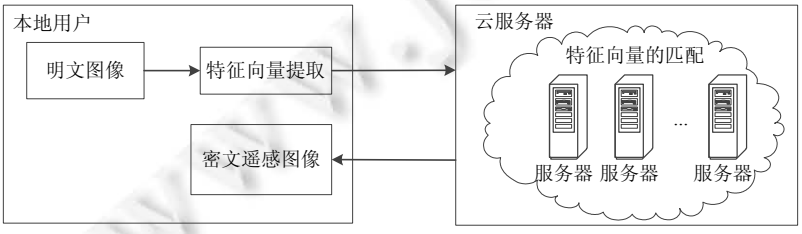


Fig.3 Flow of secure retrieve in remote sensing image

图 3 遥感图像的安全检索流程图

© 中国科学院软件研究所 http://www.jos.org.cn

5 实验数据与安全性分析

5.1 实验数据分析

实验采用的是 Landsat 8 卫星的遥感数据,下载的原始数据是 16bit 的灰度值.首先需要对图像进行预处理,将每个图层的灰度值量化为 8bit,目的是展示加密过程中的频域加密处理,同时提高加密遥感图像的检索匹配效率.如图 4 所示,为对于我国某领海域范围内的遥感图像进行量化的结果图.

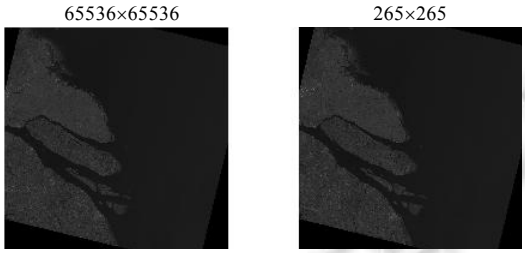


Fig.4 Quantity image of remote sensing image

图 4 遥感图像的量化图

为了能够拥有较高的匹配概率,我们选取以下 5 个阈值范围,分别是[0,15],[16,31],[32,63],[64,127],[128,255],把灰度值划分为 5×11 个组空间,在此基础上,可以统计每幅遥感图像的特征向量.利用改进的 Henon 映射对遥感图像进行加密检索,如图 5 所示.利用 Matlab 2013,我们对遥感图像 *A*(文件大小共计 1.70GB)的每个波段进行部分截取,截取的图像像素大小为 6200×6200,并对其截取的部分进行加密及解密运算,见表 2,分别显示出每个波段加密与解密的时间及其每个波段获得特征向量的时间.显然,统计加密图像 *A*1 的特征向量所花费的总时间为 7.463 793s.在遥感图像的检索过程中,加密与解密本地只需要进行一次,在很大程度上减少了本地的计算量.由表 3 和表 4 可以看出,遥感图像 *A* 在加密前后的特征向量保持不变.

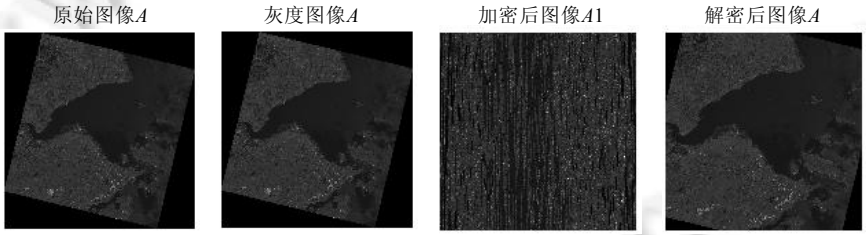


Fig.5 Effects of encryption/decryption in remote sensing image *A*

图 5 遥感图像 *A* 的加解密效果图

Table 2 Spend time of remote sensing image *A* in encryption/decryption

表 2 遥感图像 *A* 的加解密花费时间

Band	加密(s)	解密(s)	统计时间(s)
Band1	13.155 237	10.975 810	0.638 484
Band2	13.208 316	11.190 299	0.634 848
Band3	13.153 874	11.054 541	0.631 276
Band4	13.119 191	11.043 555	0.662 142
Band5	13.590 150	11.035 426	0.799 354
Band6	13.369 588	10.971 619	0.781 883
Band7	13.281 387	11.162 737	0.766 021
Band8	13.357 785	10.862 895	0.647 117
Band9	13.011 818	10.711 478	0.590 834
Band10	13.316 250	10.879 944	0.665 623
Band11	13.315 733	10.925 348	0.646 211

© 中国科学院软件研究所 http://www.jos.org.cn

Table 3 Feature vector of remote sensing image *A*

表 3 遥感图像 *A* 的特征向量

Band	[0,15]	[16,31]	[32,63]	[64,127]	[128,255]
Band1	2 372 960	0	35 447 366	600 842	31 233
Band2	2 372 934	0	35 607 628	435 664	36 175
Band3	2 372 413	270	35 723 747	322 859	33 112
Band4	2 372 533	1 835 785	33 911 356	290 351	42 376
Band5	2 372 475	1 211 652	23 109 203	11 665 973	93 098
Band6	2 372 131	11 285 788	22 725 185	2 011 798	57 499
Band7	2 372 094	16 979 923	18 396 842	688 497	15 045
Band8	8 430 045	0	29 960 296	61 791	269
Band9	2 376 374	35 978 294	97 733	0	0
Band10	2 773 158	0	123 202	35 544 052	11 989
Band11	2 762 804	0	201 554	35 488 043	0

Table 4 Feature vector of encryption image *A*1

表 4 加密图像 *A*1 的特征向量

Band	[0,15]	[16,31]	[32,63]	[64,127]	[128,255]
Band1	2 372 960	0	35 447 366	600 842	31 233
Band2	2 372 934	0	35 607 628	435 664	36 175
Band3	2 372 413	270	35 723 747	322 859	33 112
Band4	2 372 533	1 835 785	33 911 356	290 351	42 376
Band5	2 372 475	1 211 652	23 109 203	11 665 973	93 098
Band6	2 372 131	11 285 788	22 725 185	2 011 798	57 499
Band7	2 372 094	16 979 923	18 396 842	688 497	15 045
Band8	8 430 045	0	29 960 296	61 791	269
Band9	2 376 374	35 978 294	97 733	0	0
Band10	2 773 158	0	123 202	35 544 052	11 989
Band11	2 762 804	0	201 554	35 488 043	0

同时,我们对遥感图像 *B* 的第 6 波段进行部分截取,并对截取的部分进行加密及解密运算,如图 6 所示.得到遥感图像 *B*(文件大小共计 1.57GB)及其加密图像 *B*1 的特征向量(见表 5),并进行比较可以发现,遥感图像 *A* 与遥感图像 *B* 的特征向量存在显著的差异性.如表 6 所示,显示了遥感图像 *B* 每个波段加密与解密的时间及其每个波段获得特征向量的时间.显然,统计加密图像的特征向量所花费的总时间为 8.178 787s.

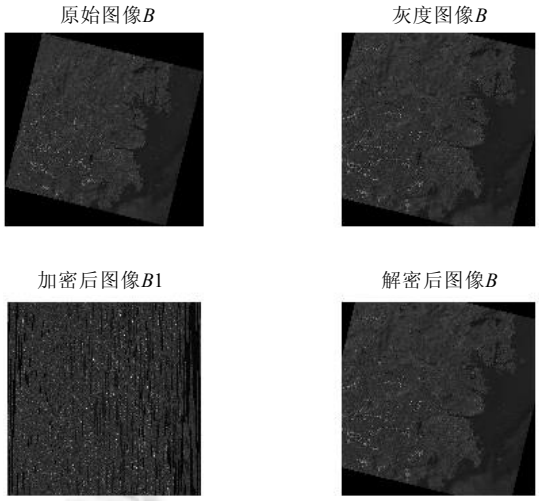


Fig.6 Effects of encryption/decryption in remote sensing image *B*

图 6 遥感图像 *B* 的加解密效果图

© 中国科学院软件研究所 http://www.jos.org.cn

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.

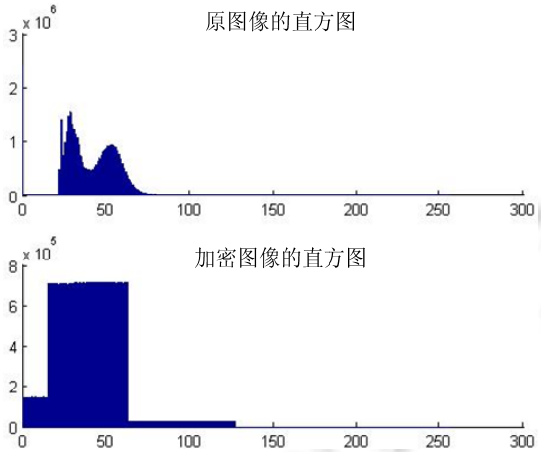


Fig.7 Histogram of original/encryption in remote sensing image *A*

图 7 遥感图像 *A* 加密前后的直方图

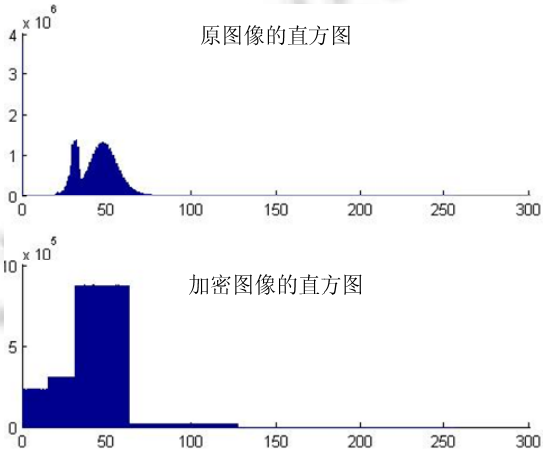


Fig.8 Histogram of original/encryption in remote sensing image *B*

图 8 遥感图像 *B* 加密前后的直方图

© 中国科学院软件研究所 http://www.jos.org.cn

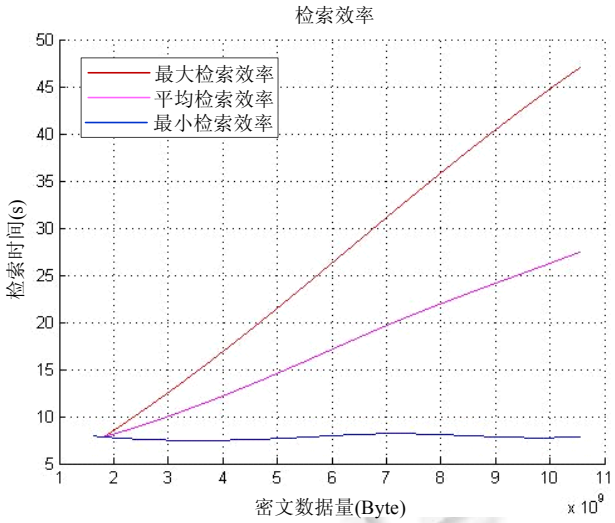


Fig.9 Query efficiency of ciphertext in remote sensing image

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]

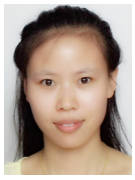
[17] 张璇,彭朋,黄勤龙.数据库密文检索技术的设计与实现.云南大学学报,2010,32(6):646−651.

[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.

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.



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.

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.

www.jos.org.cn