一种加密遥感图像的安全外包搜索方案

黄冬梅[1]，吴国健[1]，魏立斐[1*]，魏泉苗[2]，戴亮[1]

[1]上海海洋大学信息学院，上海 201306；

[2]国家海洋局东海分局，上海 200136

摘要 遥感图像具有多时相、多语义、多波段等特点，鉴于敏感遥感图像涉及国家机密信息及传统图像搜索效率低下的原因，利用云平台进行遥感图像安全外包搜索已是大势所趋。因此提出了一种加密遥感图像的安全外包搜索方案，对存储在云平台的遥感图像进行扫描模式加密，再通过异或(XOR)运算和 Johnson-Lindenstrauss (JL)转换得到一份双密文，JL 转换的遥感图像用于在云平台进行搜索，XOR 运算后的遥感图像用于图像解密。实验结果表明，本文方案可以有效保证云平台上遥感图像的安全性，同时，加密图像搜索的准确率高，搜索效率较同态加密提升 98.37%，且计算复杂度低，通信成本低，适合于云计算平台部署应用。

关键词 图像处理；密文图像搜索；遥感图像；Johnson-Lindenstrauss 转换；扫描模式加密；安全外包；云平台

中图分类号 TP751.1 **文献标识码** A **doi**：10.3788/LOP56.031001

A Secure Outsourcing Search Scheme for Encrypted Remote Sensing Images

Huang Dongmei[1], Wu Guojian[1], Wei Lifei[1*], Wei Quanmiao[2], Dai Liang[1]

[1] *College of Information Technology, Shanghai Ocean University, Shanghai* 201306, *China*;

[2] *East China Sea Branch, State Oceanic Administration, Shanghai* 200136, *China*

Abstract The remote sensing images have the multi-temporal, multi-semantics and multi-spectral characteristics. In view of the sensitive remote sensing images involving state secret information with low searching efficiency, it is a general trend to conduct a secure outsourcing search for remote sensing images based on a cloud platform. Thus, a scheme of secure outsourcing search for encrypted remote sensing images is proposed. The remote sensing image stored on the cloud platform is first encrypted by the scan mode, and then a double ciphertext is obtained through the exclusive or operation and the Johnson-Lindenstrauss (JL) transformation. The JL-transformed remote sensing images are used to search on the cloud platform, while the exclusive or encrypted remote sensing images are used to decrypt image. The experimental results show that this scheme can effectively guarantee the security of remote sensing images on the cloud platform. Meanwhile, the search accuracy of encrypted images is high and the search efficiency is 98.37% higher than that by homomorphic encryption. Moreover, the computational complexity and communication cost are low, and it is suitable for the deployment on the cloud computing platforms.

Key words image processing; encrypted image search; remote sensing images; Johnson-Lindenstrauss transformation; scan mode encryption; secure outsourcing; cloud platforms

OCIS codes 100.3008; 110.2970; 110.2960; 280.4750

1 引 言

当前图像搜索技术主要分为基于文本的图像搜索和基于内容的图像搜索，基于文本的图像搜索采用对图像附加关键词信息从而实现图像搜索，该方法存在输入工作量大，描述信息存在多义性；对于海

收稿日期：2018-06-05；**修回日期**：2018-07-26；**录用日期**：2018-08-11

基金项目：国家自然科学基金(61402282，61672339，41671431)、上海市自然科学基金(18ZR1417300)、上海市科委地方高校能力建设项目(15590501900，17050501900)、上海海洋大学科技发展专项项目

* **E-mail**：Lfwei@shou.edu.cn

量数据而言，手工注释费时费力。基于内容的图像搜索是从图像中提取特征，如低层次图像的形状、纹理、颜色、轮廓等表层的特征[1]。但是，图像搜索技术涉及到特征向量、欧氏距离等计算密集型过程，需要硬件设备具有较高的计算能力，大量的图像本地存储会造成服务器压力巨大[2]。针对图像的计算[3]和存储这两个问题，借助云计算庞大的计算能力和存储的资源池已是未来的发展趋势。

然而，由于遥感图像和普通图像不同，遥感图像具有 16 位深灰度值、波段数量大等特点，且遥感信息是关系国家安全与国民经济建设的重要战略资源，卫星遥感图像一般包含湖泊、森林等地面物体，属于国家的重要机密信息，如果直接将遥感图像外包给云平台进行搜索将会泄露隐私信息，同时在传输过程中也可能会受到非法攻击，因此，利用云平台进行图像搜索同时保证遥感图像内容的安全是亟待解决的问题[4]。

目前，在云环境下已经出现了大量的密文计算及搜索方案[5-8]。然而，针对图像外包密文搜索的研究刚刚起步，张春艳等[9]提出了基于离散小波变换和感知哈希的加密医学图像检索算法；陈帆[10]提出了量化 SIFT 和同态加密的隐私保护图像检索方法；秦姣华等[11]提出了融合多特征的图像检索算法；韩威等[12]提出了一种云环境下 JPEG 图像的安全检索方法；但是，目前的大多数加密体制并不适合在加密遥感图像直接搜索，目前黄冬梅等[13]提出了基于 Henon 映射的加密遥感图像的安全检索方案和耿霞[14]提出的支持密文搜索和运算的遥感图像加密研究，沈志荣等[15]提出了可搜索加密机制研究与进展，Demir 等[16]提出了基于哈希的大型档案馆可扩展遥感图像搜索与检索，Lu 等[17]提出了通过特征保护来保护图像检索，但搜索效率及安全性仍有不足。

因此，本文针对遥感图像的特殊性提出了一种加密遥感图像的搜索方案，将遥感图像进行波段拆分，对单波段遥感图像进行扫描模式加密，再将遥感图像进行异或（XOR）运算和 Johnson-Lindenstrauss (JL)转换[18-19]生成双密文，上传到云平台，计算多幅加密遥感图像的欧氏距离，获取满足条件的遥感图像。本文方案利用云平台强大的计算能力，将运算量大的操作如距离计算等放在云端进行，在客户端仅完成数据的加密上传，在云端进行遥感图像的搜索，很好地解决了搜索效率和安全性问题。

2 问题的描述与定义

2.1 系统模型

系统将单波段遥感图像进行存储，通过单波段的命名规则从云端下载对应其他波段的遥感图像。由于遥感图像在本地搜索速度太慢，则利用云平台的优势进行遥感图像搜索，为了保证遥感图像在云端处理的安全性，需要在本地对遥感图像进行加密处理，再对加密图像进行 JL 转换，将转换后的加密图像上传到云端，计算欧氏距离匹配相应的遥感图像。本文系统模型如图 1 所示，主要分为 4 类角色：1）图像持有者，通过安全信道将遥感图像传输至终端；2）第三方平台，存储加密遥感图像，为授权搜索者提供搜索服务，匹配图像并发送结果图像给搜索者；3）授权搜索者，通过搜索者与终端之间的安全信道传递索引图像和私钥，获得匹配到的加密遥感图像，通过私钥进行解密，从而获取明文遥感图像；4）终端，将遥感图像加密上传至云端进行搜索。

上述模型中终端与图像持有者及授权搜索者两者之间都存在一个安全信道可以传输遥感图像及私钥。

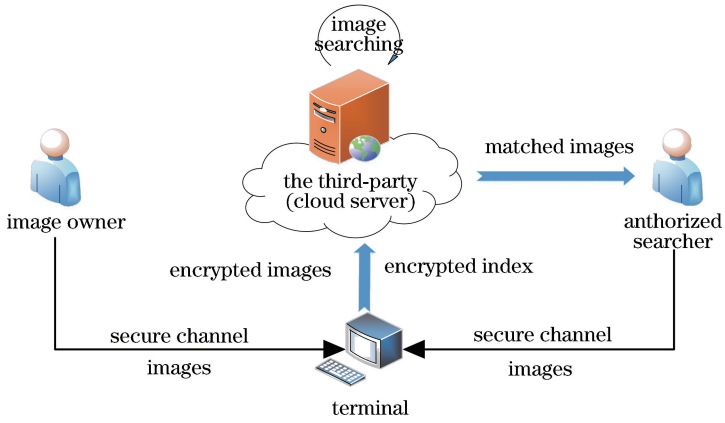

图 1 加密遥感图像的安全外包搜索方案系统模型

Fig. 1 System model for secure outsourcing search for encrypted remote sensing images

2.2 威胁模型

本文算法在保护遥感图像隐私信息的情况下进行搜索操作，但执行算法过程中会遭遇到各种攻击，导致图像信息的泄露，主要关注以下 4 种威胁：

1）信道截取者，在图像传输过程中，攻击者通过某种手段破坏安全信道并截取隐私信息。

2）半诚实第三方，第三方即是执行遥感图像的搜索操作，但在计算过程中可能会通过统计、穷举法等推断遥感图像的信息。

3）恶意攻击者，通过二值化攻击算法可以对加密遥感图像进行攻击，获取图像的大致轮廓。

4）统计分析中相邻像元的相关度，该值可以反映图像的扩散程度。原始图像中相邻像元之间的相关度通常很大，一种好的图像置乱加密算法应该让加密后的图像相邻像元之间的相关度趋近于零。

2.3 设计目标

设计目标为：1）安全性，图像搜索技术可以抵抗上述四种威胁。2）准确性，加密遥感图像搜索技术达到的效果接近于明文图像搜索算法效果。3）高效性，本文所用的加密算法对加密图像搜索耗时在可接受范围内。

2.4 算法描述

如图 2 所示，图像持有者对给定的遥感图像进行波段拆分，得到图像中一个波段，将该单波段图像进行 XOR 运算和 JL 转换，得到两份密文分别记为 $\boldsymbol{E}_A$ 和 $\boldsymbol{E}_B$，并上传至云端。

表 1 为算法 1，即系统模型中 Encrypted image 和 Encrypted index 的算法描述。

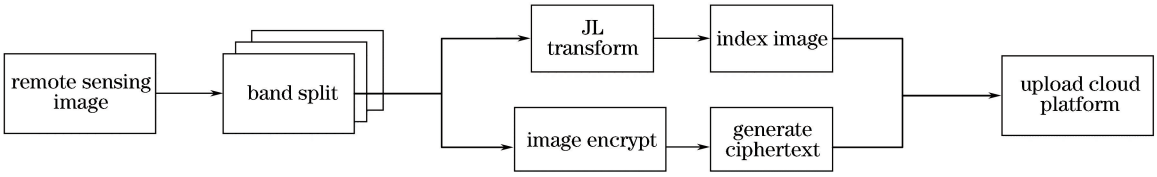

图 2 图像持有者上传图像流程图

Fig. 2 Flow chart of uploading image by image owner

表 1 算法 1 遥感图像加密算法

Table 1 Algorithm 1 of encryption algorithm for remote sensing images

Input	Split an index remote sensing image band into a single-band image $\boldsymbol{Y}(i,j)$; Height and width of remote sensing image are H and W; Randomly generate a matrix $\boldsymbol{Q}$ of Gaussian distribution $h^2\times k$ obeying an average of 0 and a variance of $1/k$; Randomly generate a matrix $\boldsymbol{R}$ of $H\times W$; Randomly generate a matrix $\boldsymbol{\Delta}$ of $h^2\times k$;
Ouput	XOR encrypted remote sensing image $\boldsymbol{E}_A$; JL transformation encrypted remote sensing image $\boldsymbol{E}_B$; Double ciphertext $\boldsymbol{E}_B=\{\boldsymbol{E}_A,\boldsymbol{E}_B\}$

Algorithmic process	1. for image $\boldsymbol{Y}$ $i=1$ to H {
	2. for image $\boldsymbol{Y}$ $j=1$ to W {
	3. $\boldsymbol{E}_A(i,j)=\boldsymbol{Y}(i,j)\oplus\boldsymbol{R}(i,j)$
	4. }
	5. }
	6. for image $\boldsymbol{Y}$ $i=1$ to h^2 {
	7. for image $\boldsymbol{Y}$ $j=1$ to h^2 {
	8. for matrix $\boldsymbol{Q}$ $m=1$ to h^2 {
	9. for matrix $\boldsymbol{Q}$ $n=1$ to k {
	10. $\boldsymbol{E}_B(m,n)=\boldsymbol{Y}(i,j)\times\boldsymbol{Q}(m,n)+\boldsymbol{\Delta}(m,n)$
	11. }
	12. }
	13. }
	14. }
	15. return upload index $\boldsymbol{E}_I=\{\boldsymbol{E}_A,\boldsymbol{E}_B\}$

如图 3 所示，将索引遥感图像进行波段拆分，进行扫描模式加密，再进行 JL 转换得到索引 JL 转换图像，通过计算索引 JL 转换图像和云端存储遥感图像的欧氏距离进行匹配，将满足匹配条件的遥感图像下载到本地进行解密，然后将所有该图像的波段重新组合，得到结果遥感图像。

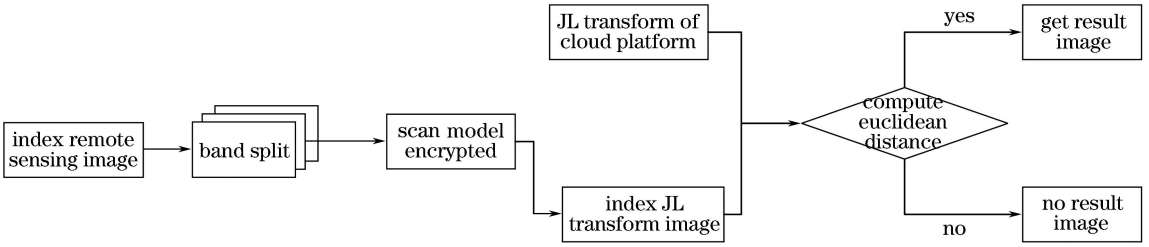

图 3 加密遥感图像的搜索方案基本流程图

Fig. 3 Basic flow chart for search of encrypted remote sensing images

表 2 为算法 2，即系统模型中 Image searching 的算法描述。

表 2 算法 2 遥感图像间欧氏距离计算算法

Table 2 Algorithm 2 of algorithm for calculation of Euclidean distance between remote sensing images

Input	Height and width of remote sensing image $\boldsymbol{E}_B$ by JL transformation are H and W; Remote sensing image $\boldsymbol{S}$ stored in cloud platform;
Ouput	Distance of two remote sensing images is d;

Algorithmic process	1. for image $\boldsymbol{E}_B$ $i=1$ to H {
	2. for image $\boldsymbol{E}_B$ $j=1$ to W {
	3. sum$+=(\boldsymbol{E}_B(i,j)-\boldsymbol{S}(i,j))^2$
	4. }
	5. }
	6. $d=\sqrt{\left\|\frac{\text{sum}-2\times k\times\xi^2}{h^2}\right\|}$
	7. return distance d

3 加密遥感图像安全搜索方案

将 JL 转换和图像加密结合，提出一种基于双密文的加密遥感图像安全搜索方案，并针对基本方案中安全性和效率的不足问题，在基本方案上加入了随机置换和比值匹配策略，提出了改进方案。

3.1 基本方案

3.1.1 遥感图像异或加密过程

授权搜索者通过 ENVI 将 7 波段遥感图像进行波段拆分，以 Band3 单波段遥感图像为例，图像的长记为 H，宽记为 W，波段数记为 N。

授权搜索者将 Band3 单波段图像的像素值存入矩阵 $\boldsymbol{E}^{\mathrm{O}}$，随机生成一个行数为 H，列数为 W 的矩阵 $\boldsymbol{E}^{\mathrm{RD}}$，将矩阵 $\boldsymbol{E}^{\mathrm{O}}$ 与矩阵 $\boldsymbol{E}^{\mathrm{RD}}$ 进行异或运算，得到一份密文 $\boldsymbol{E}^{\mathrm{EO}}$。

$$\boldsymbol{E}^{\mathrm{EO}}_{m,n}=\boldsymbol{E}^{\mathrm{O}}_{m,n}\oplus\boldsymbol{E}^{\mathrm{RD}}_{m,n}。\tag{1}$$

图像加密流程图如图 4 所示。

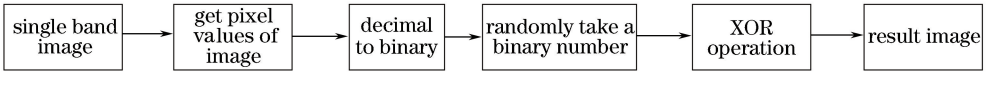

图 4 图像 XOR 加密流程图

Fig. 4 Flow chart of XOR encryption of images

3.1.2 遥感图像 JL 转换过程

随机生成一个置换表，如图 5 所示，将进行遥感图像拆分得到的结果进行 JL 转换（根据 JL 转换的特性，可以保持像素间的距离），JL 转换流程图如图 6 所示，其中块置换即二维转一维，行置换即根据置换表将每一行像素值整体置换。

授权搜索者随机生成一个 $h^2\times k$ 的矩阵 $\boldsymbol{Q}$，其元素服从均值为 0，方差为 $1/k$ 的高斯分布，将所有像素点经过块置换后形成一个 $h^2\times h^2$ 矩阵 $\boldsymbol{A}$，然后矩阵 $\boldsymbol{A}$ 右乘矩阵 $\boldsymbol{Q}$ 得到一个矩阵 $\boldsymbol{B}$，再随机生成一

1	2	3	4	5	6	7	8	9
↓	↓	↓	↓	↓	↓	↓	↓	↓
6	3	9	2	7	4	1	5	8

图 5 置换表

Fig. 5 Permutation table

个 $h^2\times k$ 的矩阵 $\boldsymbol{\Delta}$，其元素服从均值为 0，方差为 s^2 的高斯分布，最后将矩阵 $\boldsymbol{B}$ 加上随机矩阵 $\boldsymbol{\Delta}$ 得到矩阵 $\boldsymbol{C}$。JL 转换公式为

$$\boldsymbol{C}_{h^2\times k}=\boldsymbol{A}_{h^2\times h^2}\cdot\boldsymbol{Q}_{h^2\times k}+\boldsymbol{\Delta}_{h^2\times k}。\tag{2}$$

3.1.3 遥感图像间距离的计算过程

授权搜索者将 JL 转换图像上传至云端，进行欧氏距离计算，将索引图像矩阵记为 $\boldsymbol{V}$，云端库中图像矩阵记为 $\boldsymbol{U}$，根据下式计算欧氏距离，结果存于矩阵 $\boldsymbol{d}$，即

$$\boldsymbol{d}_{m,n}=\sqrt{\left|\frac{\|\boldsymbol{V}_{m,n}-\boldsymbol{U}_{m,n}\|_2^2-2k\xi^2}{h^2}\right|},\tag{3}$$

根据(3)式将矩阵 $\boldsymbol{d}$ 所有点求其数学期望，获取最佳值，即

$$\bar{d}=\frac{\sum_{m=0,n=0}^{H-1,W-1}\boldsymbol{d}_{\mathrm{m,n}}}{\mathrm{H}\times\mathrm{W}}。\tag{4}$$

3.1.4 遥感图像解密过程

授权搜索者将云端匹配的遥感图像下载至本地，用随机矩阵 $\boldsymbol{E}^{\mathrm{RD}}$ 对本地图像进行恢复，得到一个二维矩阵 $\boldsymbol{E}^{\mathrm{DE}}$，即明文单波段图像，表达式为

$$\boldsymbol{E}_{m,n}^{\mathrm{DE}}=\boldsymbol{E}_{m,n}^{\mathrm{EN}}\oplus\boldsymbol{E}_{m,n}^{\mathrm{RD}},\tag{5}$$

授权搜索者将明文单波段图像进行重新组合，得到结果遥感图像。

3.2 改进方案

3.2.1 安全性提升

根据 JL 转换的特性，遥感图像 I_{JL} 保存了明文图像中的相邻像素的位置信息，虽然无法准确获取遥感图像的灰度值，但通过二值化攻击可以基本获得图像的大致轮廓，对图像进行二值化攻击，效果图如图 7 所示。

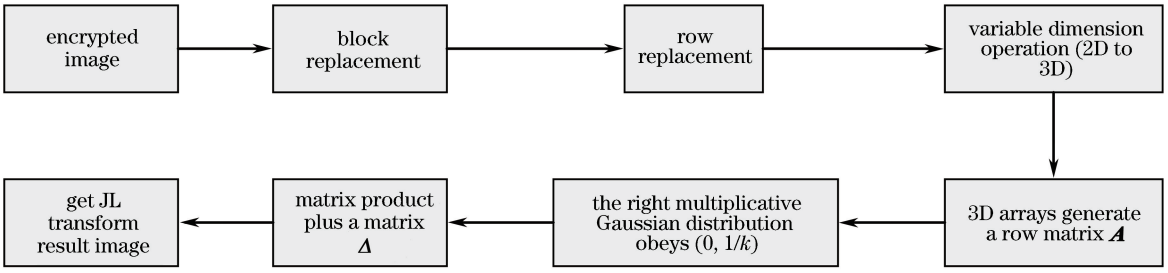

图 6 JL 转换流程图

Fig. 6 Flow chart of JL transformation

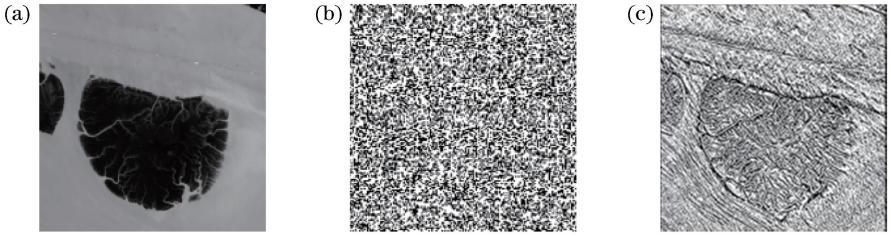

图 7 二值化攻击效果图。(a)原图；(b)密文图像；(c)二值化攻击结果图像

Fig. 7 Binary attack effect. (a) Original image; (b) encrypted image; (c) binary attack result

为了保证隐私不被泄露，本文必须要消除图像像素点及其周围点之间的强关联性。因此改进方案采用扫描模式加密[20]，在遥感图像加密操作和 JL 转换前都先对图像的像素点位置进行扰乱。

扫描算法代表基于形式语言的二维空间扫描的一整套方法[21]，可表示和生成大量的变化广泛的扫描路径。其基本思想是重排图像像素，是用一类由加密专用的扫描语言生成的扫描模式完成的。扫描语言用语法表示为 $G=(\Gamma,\Sigma,A,\Pi)$，其中，$\Gamma=\{A,S,P,U,V,T\}$ 是非结尾符号，$\Sigma=\{c,d,o,s,r,a,e,m,y,w,b,z,x,B,Z,X,(,),\mathrm{space},0,1,2,3,4,5,6,7\}$ 是结尾符号；A 是起始符号；Π 是乘积规则，由下式给出，即

$$A\rightarrow S\mid P,\tag{6}$$

$$S \rightarrow UT, \tag{7}$$

$$P \rightarrow VT(AAAA), \tag{8}$$

$$U \rightarrow c \mid d \mid o \mid s \mid r \mid a \mid e \mid m \mid y \mid w \mid b \mid z \mid x, \tag{9}$$

$$V \rightarrow B \mid Z \mid X, \tag{10}$$

$$T \rightarrow 0 \mid 1 \mid 2 \mid 3 \mid 4 \mid 5 \mid 6 \mid 7, \tag{11}$$

对上述加密专用扫描语言的语义说明如下：

1)(6)式表示处理扫描 S 或分划 P。

2)(7)式的意义是用扫描模式 U 和变换 T 扫描区域。

3)(8)式表示用分划模式 V 和变化 T 扫描区域。

4)(9)式表示用光栅 r、连续光栅 c、直角 a、向外螺旋 s、水平对称 m、对角线平行 e、对角线对称 y、第二对角线 w、z 型 z、块型 b 或 x 型 x 等方式扫描，参见图 8。

5)(10)式的意义是分别用 B 类、Z 类或 X 类模式进行分划，参见图 9。

6)(11)式表示用 8 种变换中的一种进行扫描或分划。

对于分划，这些变换由图 9 表示，对于扫描，这些变换定义为对所有的扫描模式，0 表示图 9 中的恒等变换，2 表示顺时针旋转 90°。对扫描模式 c、o、s、a、e、m、y、w、b 和 x，4 表示顺时针旋转 180°，而 6 表示顺时针旋转 270°。对于扫描模式 r 和 z，4 表示垂直反射，而 6 表示顺时针旋转 90°后进行垂直反射，对于扫描模式 d，4 表示水平反射后顺时针旋转 90°，而 6 表示垂直反射后顺时针旋转 180°。对所有扫描模式，1、3、5 和 7 分别是扫描路径 0、2、4 的相反过程。

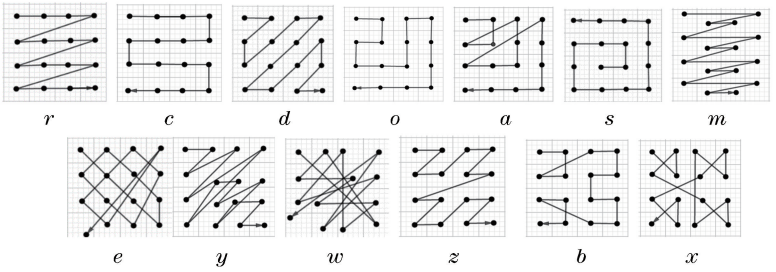

图 8 基本扫描模式

Fig. 8 Basic scan modes

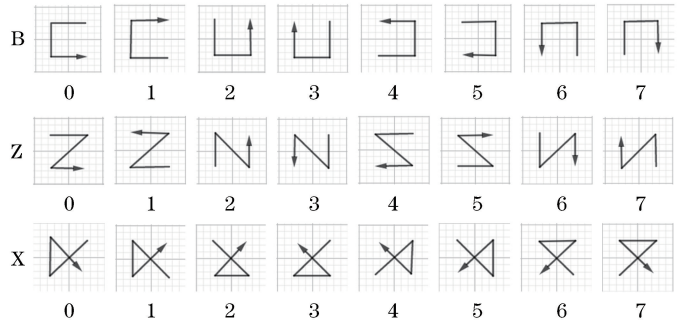

图 9 分划模式和变换

Fig. 9 Mode division and transformation

对于 16 pixel×16 pixel 的图像扫描密钥 B5(s2 Z0(c5 b0 o0 s5) c4 d1)，相应于这个密钥的扫描路径如图 10 所示。

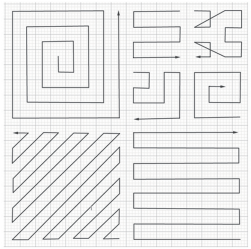

图 10 扫描密钥 B5(s2 Z0(c5 b0 o0 s5) c4 d1)路径示意图

Fig. 10 Path schematic for scanning of key B5(s2 Z0(c5 b0 o0 s5) c4 d1)

3.2.2 搜索效率提高

基于特征匹配的尺度不变特征变换算法以其改进算法[22-24]中提到的邻近距离比值匹配策略方法，采用最邻近距离和次邻近距离的比值作为两个特征向量是否为匹配特征点的判断标准。本文方案通过同幅遥感图像 I 中的不同位置像素值的比值作为索引，通过索引初步去除大量不匹配的遥感图像，来提

高图像的搜索效率，通过取多个点比值的均值来提高精度。去除条件：对阈值 T_1、T_2 取值如表 1 所示，输出满足 $T_1 \leqslant g_{I_1}/g_{I_2} \leqslant T_2$ 条件的图像，比值计算为

$$g_{I_i} = \sum_{i,j=0,m,n=x}^{H-x-1,H-1} \frac{I_{m,n}}{I_{i,j}}。\tag{12}$$

表 3 最优阈值分析表

Table 3 Optimal threshold analysis

(T_1,T_2)	Actual number of similar images	Number of images searched	Number of correct images	Number of error images	Number of images not searched
(0.7,0.8)	56	0	0	0	56
(0.8,0.9)	56	0	0	0	56
(0.9,1.0)	56	4	4	0	52
(1.0,1.1)	56	12	12	0	44
(1.1,1.2)	56	52	32	20	24
(1.2,1.3)	56	56	0	56	56
(0.8,1.0)	56	4	4	0	52
(0.9,1.1)	56	20	20	0	36
(1.0,1.2)	56	64	44	20	12
(0.8,1.1)	56	20	20	0	36
(0.9,1.2)	56	72	52	20	4

由表 3 搜索出的正确图像数和未搜索出的图像数可知，T_1、T_2 取值为 0.9、1.2 时，搜索效果最优，改进方案减少了不相关遥感图像的搜索时间，提高了图像搜索速度及效率。同时，本节结合的一种双密文方法较单密文有以下优势：1）双密文是将两份单密文进行融合成独立的密文，遥感图像搜索过程中，单密文采取串行搜索的方式，第一幅图像搜索完成后进行解密再搜索第二幅图像，而双密文将采取并行搜索方式，第一幅图像搜索完成后直接搜索第二幅图像，同时解密第一幅图像，图库中图像数量较多时将节省大量处理时间，提高搜索效率；2）遥感图像搜索过程中使用的 JL 转换加密图像的密文具有不可逆的特性[18]，而异或加密密文只应用于图像解密，不参与图像搜索，因此，攻击者在图像搜索过程中无法获取图像信息，提升了图像搜索的安全性。

4 实验仿真与性能分析

实验平台采用两台 PC 机，一台模拟客户端，一台模拟第三方，其中作为第三方的 PC 配置为 Intel (R) Core(TM) i5-6500 CPU @3.2 Hz 3.19 GHz，内存为 12 G，Win10 64 位操作系统，算法通过 opencv 平台和 python 语言实现，实验数据集采用从地理空间数据云网站获取的 Landsat8 卫星遥感图像的数据进行实验。

4.1 搜索精度分析

本实验从中抽取了 400 张 512 pixel×512 pixel 的遥感图像组成图库，为增加实际效果，并给图像加上不同大小的高斯噪声来模拟实际图像，实验过程中各参数取值如表 4 所示。

表 4 参数取值表

Table 4 Parameter value

Parameter	Instructions	Value
H	Height of remote sensing image	512
W	Width of remote sensing image	512
N	Band number of remote sensing image	200
h	Height of JL transformation	5
k	Variance parameter of Gaussian distribution $\boldsymbol{Q}$	18
s	Variance parameter of Gaussian distribution $\boldsymbol{\Delta}$	0.5
T	Threshold	550

实验随机选取一幅遥感图像作为索引图像，搜索结果如图 11 所示，图 11(a)为图 O 地区的图像，图 11(b)为图 O 地区的不同时相的图像，图 11(c)为图 O 地区含$(0,384^2)$高斯分布噪声的遥感图像，用来模拟实际噪声图像，图 11(d)为光线暗沉的遥感图像。图 11(e)～(g)则搜索不到，图 11(e)为发生形变的遥感图像，图 11(f)为上海周边某个岛屿的遥感图像，图 11(g)为一块陆地的遥感图像。

搜索结果的全面与否，需要通过查全率来表现，而结果的准确性，则需要通过查准率来反映，查准率和查全率数据如表 5 和 6 所示。其对应的查准率和查全率对比图如图 12 和 13 所示。

从图 12 和 13 可以看出，将基本方案、改进方案和Lowe方案[25]三者进行对比，三个方案的查全率

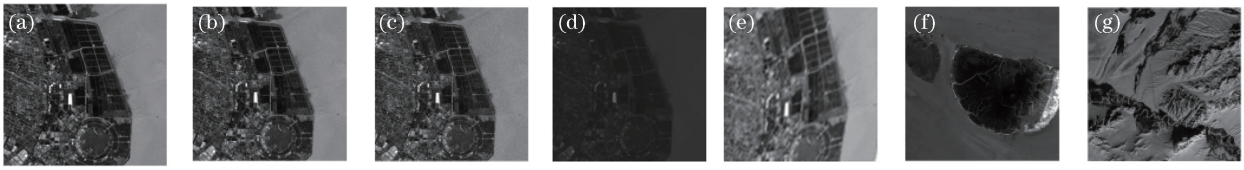

图 11 遥感图像搜索结果。(a)图像 O;(b)不同时相的图像;(c)含高斯分布噪声的遥感图像;(d)光线暗沉的遥感图像;(e)发生形变的遥感图像;(f)岛屿的遥感图像;(g)陆地的遥感图像

Fig. 11 Search results of remote sensing images. (a) Image O; (b) image with different phases; (c) remote sensing image with Gaussian noise; (d) remote sensing image under dimmed light; (e) remote sensing image with deformation; (f) remote sensing image of island; (g) remote sensing image of land

表 5 查准率

Table 5 Precision rate

Scheme category	Number of images							
	50	100	150	200	250	300	350	400
Lowe's scheme[25]	0.135	0.229	0.378	0.446	0.568	0.608	0.676	0.729
Basic scheme	0.059	0.101	0.166	0.196	0.25	0.268	0.304	0.333
Improved scheme	0.139	0.222	0.375	0.431	0.556	0.597	0.667	0.722

表 6 查全率

Table 6 Recall rate

Scheme category	Number of images							
	50	100	150	200	250	300	350	400
Lowe's scheme[25]	0.179	0.304	0.500	0.589	0.750	0.804	0.893	0.964
Basic scheme	0.179	0.304	0.500	0.589	0.750	0.804	0.911	1
Improved scheme	0.179	0.286	0.482	0.554	0.714	0.768	0.857	0.929

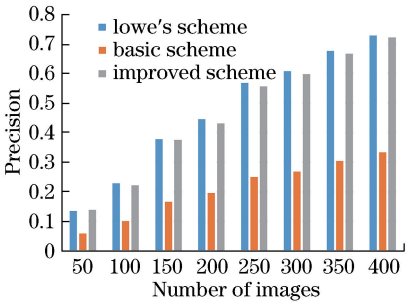

图 12 查准率对比图

Fig. 12 Comparison of precision rates

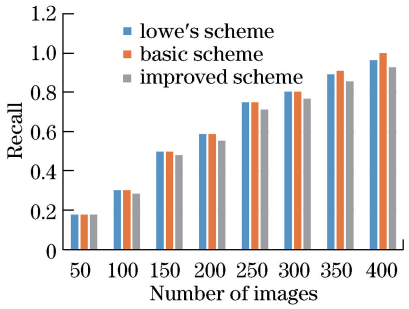

图 13 查全率对比图

Fig. 13 Comparison of recall rates

均接近 100%,改进方案和 Lowe 方案[25]搜索效果接近,较基本方案显著提高了遥感图像查准率。

4.2 搜索效率分析

文献[10]中证实文献[10]方案的搜索效果接近于 Lowe 方案[25],因此,本文改进方案的搜索效果接近于文献[10]方案。除了查准率和查全率的比较分析,还在速度方面进行了对比分析,文献[10]使用 Paillier 同态加密搜索 100 幅遥感图像需 11.95 h,在基本方案中搜索 100 幅遥感图像需 50 min,在改进方案中只需 11.7 min,基本方案搜索效率较文献[10]方案提高了 93.03%,改进方案较基本方案又提高了 76.6%,因此,本文方案不仅提高了查准率,搜索效率也有大幅的提升,提高了 98.37%。本文两者方案搜索图像的时间对比如图 14 所示。

4.3 安全性分析

本文方案针对 2.2 节的 4 种威胁模型进行抵御分析如下:

1) 抗信道截取者的能力

这种威胁是较弱的一种模型,通过对遥感图像进行加密传输,就可以抵御这种威胁。

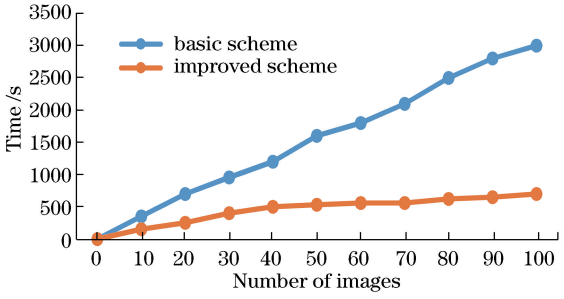

图 14 搜索时间对比

Fig. 14 Comparison of search time

2) 抗穷举法的能力

首先,将图像的像素值进行异或运算,如攻击者不能得到进行异或运算随机矩阵,则不可能恢复原有图像的像素值,对于 JL 转换的图像加密技术安全性,攻击者假若没有图像持有者私钥,需尝试所有可能性的排列以获得图像信息,但是,对于有 n 个像素值图像排列的可能性是 $n!$,因此,对于一个 512 pixel×512 pixel 的遥感图像,攻击者要想正确猜测出排列情况的可能性是 $10^{-1306595}$,所以,任何攻击者要想恢复商用价值的图像代价太高。

3)抗二值化攻击的能力

在改进方案中增加了随机置换,有效干扰了图像像素点之间的位置关系,对于一个 512 pixel×512 pixel 的遥感图像,扫描模式加密将图像所有位置进行重排,每个像素点位置都有 262144 种可能性,恢复原图像的可能性是 $10^{-1306595}$,攻击者若想用二值化攻击也将无法获得图像的大致轮廓,保证了该方案的安全性。实验测试结果如图 15 所示。

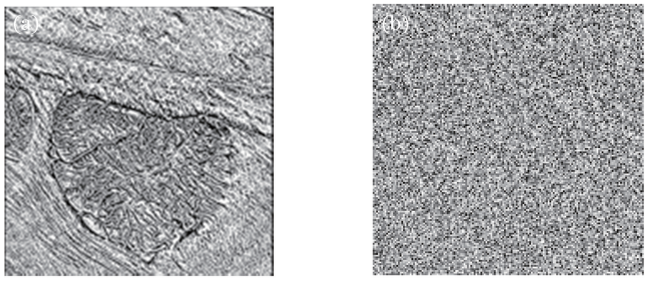

图 15 二值化攻击效果图。(a)基本方案;(b)改进方案

Fig. 15 Binary attack effect. (a) Basic scheme; (b) improved scheme

4) 抗统计分析图像相邻像元相关度的能力

如图 16 和 17 所示分别为原始图像和加密图像中相邻像元间的相关关系,由图 16 和 17 可知,横坐标表示图像的像素点,纵坐标表示对应横坐标像素值位置的下方位置,图 16 中纵坐标随着横坐标的增大而增大,因此原始图像相邻像元间呈正相关关系,加密处理后的图像散点均匀分布 0~170 之间,且纵坐标不随着横坐标的变化而变化,因此加密图像相邻像元间呈不相关关系,表达式为

$$r=\frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2\cdot\sum_{i=1}^{n}(y_i-\bar{y})^2}}。\tag{13}$$

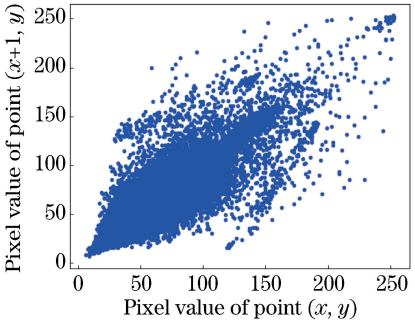

图 16 原始图像中相邻像元间的相关关系

Fig. 16 Correlation among adjacent pixels in original image

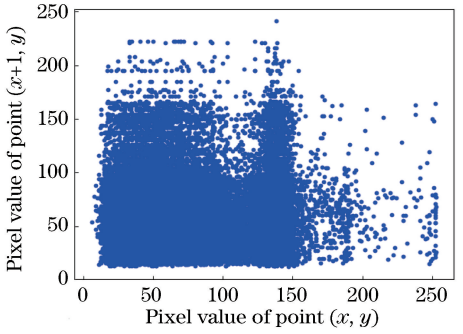

图 17 加密图像中相邻像元间的相关关系

Fig. 17 Correlation among adjacent pixels in encrypted image

由于实验数据过多,实验部分数据如表 7 所示,通过(13)式计算实验数据可得:原始图像邻像元间的相关系数 $r_1=0.938205538143$,加密图像相邻像元间的相关系数 $r_2=-0.00326092783623$,r_2 趋于 0,说明达到一种很好的置换效果。

表 7 原始图像与加密图像的相邻像素点数据表

Table 7 Adjacent pixel point data in original and encrypted images

Original image	Pixel value of point(x, y)	156	139	143	138	139	147	153	156	157	146
	Pixel value of point ($x+1$, y)	77	57	71	56	48	49	61	78	81	91
Encrypted image	Pixel value of point(x,y)	156	139	143	138	139	147	153	156	151	156
	Pixel value of point ($x+1$, y)	33	111	19	63	47	114	24	88	37	32

根据密文搜索的方式,本文方案与其他密文比较方案进行对比,如表 8 所示。

表 8 密文搜索方案分析表

Table 8 Analysis of related schemes for ciphertext search

Ciphertext search scheme	Suitable for cloud computing	Support image search	Security	Accuracy	Search efficiency
Ref. [26]	Yes	False	Low	Low	Low
Ref. [27]	False	False	High	High	Low
Ref. [28]	False	Yes	Low	High	Low
Ref. [13]	Yes	Yes	Higher	High	Higher
Proposed scheme	Yes	Yes	High	High	High

5 结 论

为了保护云数据的安全与隐私,安全外包技术已逐步应用到云存储与计算中。本文提出了一种加密遥感图像的安全外包搜索方案,通过扫描模式加密及双密文方案进行遥感图像单波段特征匹配,很好地解决了遥感图像加密存储与搜索的安全问题。相比于文献[10]中方案的安全性和搜索效率有显著提高,改进方案的搜索效率提高了 98.37%,该方案的优点是速度快、效率高,且计算复杂度低,可提高加密遥感图像的可用性。鉴于遥感图像的文件大、数量多等特点,搜索时间较长,下一步工作就是在实际云平台上部署实现遥感图像的安全外包搜索。

参 考 文 献

[1] Asiyan H , Abudurexiti H . Comparative research of image retrieval based on text and content[J]. Journal of Capital Normal University (Natural Science Edition), 2012, 33(4): 6-9.
阿斯艳·哈米提, 阿不都热西提·哈米提. 基于文本的图像检索与基于内容的图像检索技术的比较研究[J]. 首都师范大学学报(自然科学版), 2012, 33(4): 6-9.

[2] Hou P, Chen L, Cheng G. A new method of multi-temporal remote sensing images storage management [J]. Ordnance Industry Automation, 2010, 29(3): 63-67.
侯平, 陈荦, 程果. 一种多时相遥感影像存储管理的新方法[J]. 兵工自动化, 2010, 29(3): 63-67.

[3] Wu Y Q, Wang Z L. Infrared andvisible image fusion based on target extraction and guided filtering enhancement[J]. Acta Optica Sinica, 2017, 37(8): 0810001.
吴一全, 王志来. 基于目标提取与引导滤波增强的红外与可见光图像融合[J]. 光学学报, 2017, 37(8): 0810001.

[4] Zhang Y Q, Wang X F, Liu X F, *et al*. Survey on cloud computing security[J]. Journal of Software, 2016, 27(6): 1328-1348.
张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述[J]. 软件学报, 2016, 27(6): 1328-1348.

[5] Yao L S, Zhu Z Y, Cheng J X. Colorimage encryption algorithm based on DNA sequence operation and fractional order Chen hyper-chaotic system[J]. Laser & Optoelectronics Progress, 2016, 53(9): 091003.
姚丽莎, 朱珍元, 程家兴. DNA 序列和分数阶 Chen 超混沌系统彩色图像加密[J]. 激光与光电子学进展, 2016, 53(9): 091003.

[6] Bai Y B H, Lü X D, Li G Q, *et al*. Optical interference double gray image encryption system based on compressive sensing [J]. Laser & Optoelectronics Progress, 2016, 53(4): 041002.
白音布和, 吕晓东, 李根全, 等. 基于压缩感知的光学干涉双灰度图像加密系统[J]. 激光与光电子学进展, 2016, 53(4): 041002.

[7] Xiang F, Liu C Y, Fang B X, *et al*. Research on ciphertext search for the cloud environment [J]. Journal on Communications, 2013, 34(7): 143-153.
项菲, 刘川意, 方滨兴, 等. 云计算环境下密文搜索算法的研究[J]. 通信学报, 2013, 34(7): 143-153.

[8] Zhu B P, Zhang J K. Scheme ofciphertext retrieval in

cloud based on ontology semantic expansion [J]. Journal of Nanjing University of Science and Technology (Nature Science), 2015, 39(4): 392-397.
朱保平, 张金康. 云环境中基于本体语义扩展的密文检索方案[J]. 南京理工大学学报(自然科学版), 2015, 39(4): 392-397.

[9] Zhang C Y, Li J B, Wang S S. Encrypted image retrieval algorithm based on discrete wavelet transform and perceptual hash [J]. Journal of Computer Applications, 2018, 38(2): 539-544,572.
张春艳, 李京兵, 王双双. 基于离散小波变换和感知哈希的加密医学图像检索算法[J]. 计算机应用, 2018, 38(2): 539-544,572.

[10] Chen F. Privacy preserving image retrieval method based on binary SIFT and homomorphic encryption [J]. Transducer and Microsystem Technologies, 2017, 36(5): 83-87.
陈帆. 量化 SIFT 和同态加密的隐私保护图像检索方法[J]. 传感器与微系统, 2017, 36(5): 83-87.

[11] Qin J H, Xie B, Xiang X Y, *et al*. An image retrieval algorithm based on multi-feature fusion [J]. Telecommunication Engineering, 2017, 57(9): 1023-1029.
秦姣华, 谢备, 向旭宇, 等. 融合多特征的图像检索算法[J]. 电讯技术, 2017, 57(9): 1023-1029.

[12] Han W, Shen M, Xu Y Y, *et al*. Secure JPEG image retrieval method under cloud environment [J]. Application Research of Computers, 2017, 34(4): 1239-1243.
韩威, 申铭, 徐彦彦, 等. 一种云环境下 JPEG 图像的安全检索方法[J]. 计算机应用研究, 2017, 34(4): 1239-1243.

[13] Huang D M, Geng X, Wei L F, *et al*. A secure query scheme on encrypted remote sensing images based on henon mapping [J]. Journal of Software, 2016, 27(7): 1729-1740.
黄冬梅, 耿霞, 魏立斐, 等. 基于 Henon 映射的加密遥感图像的安全检索方案[J]. 软件学报, 2016, 27(7): 1729-1740.

[14] Geng X. Remote sensing image encryption supporting ciphertext search and computation [D]. Shanghai: Shanghai Ocean University, 2017.
耿霞. 支持密文搜索和运算的遥感图像加密研究[D]. 上海: 上海海洋大学, 2017.

[15] Shen Z R, Xue W, Shu J W. Survey on the research and development of searchable encryption schemes [J]. Journal of Software, 2014, 25(4): 880-895.
沈志荣, 薛巍, 舒继武. 可搜索加密机制研究与进展[J]. 软件学报, 2014, 25(4): 880-895.

[16] Demir B, Bruzzone L. Hashing-based scalable remote sensing image search and retrieval in large archives [J]. IEEE Transactions on Geoscience and Remote Sensing, 2016, 54(2): 892-904.

[17] Lu W J, Varna A L, Swaminathan A, *et al*. Secure image retrieval through feature protection[C] // 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, 2009: 1533-1536.

[18] Ailon N, Chazelle B. Approximate nearest neighbors and the fast Johnson-Lindenstrauss transform [C] // Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing-STOC′06, the Thirty-Eighth Annual ACM Symposium, 2006.

[19] Indyk P, Motwani R. Approximate nearest neighbors [C] // Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing - STOC′98, the Thirtieth Annual ACM Symposium, 1998.

[20] Sun X H. Image encryption algorithms and practices [M]. Beijing: Science Press, 2013: 64-74.
孙燮华. 图像加密算法与实践[M]. 北京: 科学出版社, 2013: 64-74.

[21] Maniccam S S, Bourbakis N G. Image and video encryption using SCAN patterns [J]. Pattern Recognition, 2004, 37(4): 725-737.

[22] Wang F, You H J, Fu X Y. Adapted anisotropic Gaussian SIFT matching strategy for SAR registration [J]. IEEE Geoscience and Remote Sensing Letters, 2015, 12(1): 160-164.

[23] Dellinger F, Delon J, Gousseau Y, *et al*. SAR-SIFT: a SIFT-like algorithm for SAR images [J]. IEEE Transactions on Geoscience and Remote Sensing, 2015, 53(1): 453-466.

[24] Wang B S, Zhang J X, Lu L J, *et al*. A uniform SIFT-like algorithm for SAR image registration [J]. IEEE Geoscience and Remote Sensing Letters, 2015, 12(7): 1426-1430.

[25] Lowe D G. Distinctiveimage features from scale-invariant keypoints [J]. International Journal of Computer Vision, 2004, 60(2): 91-110.

[26] Wang C, Cao N, Li J, *et al*. Secure ranked keyword search over encrypted cloud data [C] // IEEE 30th International Conference on Distributed Computing Systems, 2010: 253-262.

[27] Cheon J H, Kim M, Kim M. Search-and-compute on encrypted data [M] // Heidelberg: Springer, 2015: 142-159.

[28] Zhang X, Peng P, Huang Q L. Design and implementation of query over encrypted data [J]. Journal of Yunnan University (Natural Sciences Edition), 2010, 32(6): 646-651, 656.
张璇, 彭朋, 黄勤龙. 数据库密文检索技术的设计与实现[J]. 云南大学学报(自然科学版), 2010, 32(6): 646-651,656.