一种面向多波段数字遥感影像的版权保护方案

付剑晶[1,2],王 珂[2],徐建军[3]
(1. 浙江传媒学院新媒体学院,浙江杭州 310018;2. 浙江大学遥感与信息技术应用研究所,浙江杭州 310058;
3. 浙江财经大学金融学院,浙江杭州 310018)

摘 要: 针对数字遥感影像大尺度、多波段、高保真的特性,提出了一种新颖的版权保护方案. 理论分析了第一奇异值向量方向的稳定性;通过比较某一参考向量分别与两个选定数据块的第一奇异值向量的夹角关系,建立单波段图像水印特征;然后为遥感影像的多波段特性提出了水印检测的快速策略与一般策略. 实验表明该方案对波段攻击与灰度攻击、组合攻击等保持图像内容的操作具有较强的鲁棒性.

关键词: 数字水印; 奇异值向量; 遥感影像; 波段攻击; 灰度攻击
中图分类号: TP391, TP79 **文献标识码:** A **文章编号:** 0372-2112 (2016)03-0732-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.03.035

A Copyright Protection Scheme for Multiband Digital Remote Sensing Imagery

FU Jian-jing[1,2], WANG Ke[2], XU Jian-jun[3]
(1. *College of New Media, Zhejiang University of Media and Communications, Hangzhou, Zhejiang* 310018, *China*;
2. *Institute of Remote Sensing and Information System, Zhejiang University, Hangzhou, Zhejiang* 310058, *China*;
3. *College of Finance, Zhejiang University of Finances and Economics, Hangzhou, Zhejiang* 310018, *China*)

Abstract: A novel copyright protection scheme is proposed for large scale, multi-band and high fidelity of digital remote sensing image. The stability of the first singular value vector direction is analyzed. In extracting watermarking feature for single band image, one bit feature is generated by comparing the angle size relationships that come from the first singular value vector of two selected data blocks and a reference vector. Next, the fast watermark detection strategy and general strategy are proposed especially for the multiband property of remote sensing imagery. The experimental results show that the proposed scheme is robust to band attack, gray attack, combination attacks and some other content-preserved operations.

Key words: digital watermarking; singular value vector; remote sensing imagery; band attack; gray attack

1 引言

数字遥感影像是通过传感设备对地物目标采集获取的数据信息,影像中的每个波段为一幅灰度图像. 通过对图像的分析与处理可以实现目标识别与信息提取. 随着遥感技术应用领域的拓展,在线发布与购买遥感影像变得越来越便利;与此同时耗资较大的遥感影像信息极易被恶意编辑、复制,导致影像所有者蒙受巨大经济损失,保护数字遥感影像的版权已成为一个迫切需求.

数字水印技术是对知识产权的一种有效保护方式,一般分为空间域方法和变换域方法,在变换域中,基于DCT和DWT的方法应用得较多. 与基于DCT的算法相比,DWT域的水印技术在觉质量与鲁棒性上的综合性能较好. 然而DWT的缺点是它不具有平移不变特性和方向选择特性,会影响到水印的性能. 由Do和Vetterli[1,2]提出的Contourlet变换也称为金字塔方向滤波器组(Pyramidal Directional Filter Bank, PDFB),它突破了小波变换有限地捕获方向信息的能力,允许不同尺度不同方向的逼近采样,可以更全面地表示图像本身的几何特性,而且它采用的迭代滤波器组使得计算更加高效. 所以近年来基于Contourlet的图像水印算法受到重视[3~5]. 文献[6~9]也表明,基于Contourlet域的水印技术能实现较好的视觉质量与鲁棒性,能抗击较低因子的JPEG压缩攻击.

收稿日期:2014-09-10;修回日期:2015-06-24;责任编辑:李勇锋
基金项目:浙江省科技厅公益技术项目(No. 2015C31110);国家新闻出版广电总局科研项目(No. 2014-42)

值得注意的是,普通图像只是满足视觉需求,而遥感影像中的图像更多地表现为其蕴含的数据价值,相应的水印算法必须确保数据的后续应用(如专题分析、数学分析、分类、边缘检测等)不受影响;所以一般图像水印算法在遥感领域的应用往往受到限制. 零水印技术[10~15]是根据图像数据本身的特征来产生水印,而不是嵌入水印数据,对原始数据是无损的,因而特别适用于遥感影像的版权保护. 与零水印技术最为密切的当为感知哈希,两者各有优势,并有一定的互补性. 感知哈希在检索应用领域更有优势,同时两者可以在媒体管理与认证方面发挥协同效用. 关于数字图像感知哈希的研究非常多,有兴趣的读者可以参阅相关文献[16~19]. 目前学术界也常称零水印为感知哈希,然而感知哈希起源最初与数字水印紧密相关,为了突出本研究对遥感影像数据的无损性,本文暂用数字水印的说法.

近年来陆续提出了一些关于数字遥感影像的水印算法,然而完全针对数字遥感影像主要特性(大尺度、多波段、数据高保真)的水印方案少见. 研究发现,绝大多数提出的算法对影像的遥感特性重视不够、针对性不强,具体表现为:(1)算法创新性不够,提出的算法大都是直接借用现有的普通图像水印算法或是稍加改进;(2)检测不便利,有些算法是非盲的,不便于应用;(3)抗水印攻击的范围偏小,很多算法只是考虑了滤波、噪声、JPEG 压缩等中的几项;(4)测试对象偏少,很多方案是在 1 ~2 个遥感影像上进行实验,实验数据可能缺乏代表性;(5)未考虑遥感影像的多波段特性,设计算法时将整个影像视作一幅灰度图像;(6)数据的保真性重视不够,很多算法未评价因水印的嵌入对原始数据造成的损伤程度以及对后续应用是否有影响.

本文为多波段数字遥感影像集的版权保护针对性地开展了水印方案研究,首先分析了第一奇异值向量方向的指向具有很好的稳定性,并基于此详细地阐述了所提出的水印方案,具体包括:(1)多波段水印提取算法,(2)单波段水印检测算法与虚警概率,(3)多波段遥感影像水印检测的快速策略与一般策略. 文中分析了方案的安全性、抗碰撞性及鲁棒性,实验表明提出的方案对波段攻击、普通单项攻击、灰度攻击、组合攻击表现很好的鲁棒性.

2　第 1 奇异值向量方向的稳定性

第 1 奇异值向量方向(First Singular Value Vector Direction,FSVVD)的稳定性是本文方案的基础,本节简要地介绍与之相关的奇异值分解(Singular Value Decomposition,SVD),并对 FSVVD 的稳定性进行数学分析.

一幅灰度数字图像 $\boldsymbol{I}$ 可以表示成 $m\times n$ 的矩阵 $\boldsymbol{I}=\{I_{ij}\}_{m\times n}$,而遥感影像中的每一波段都是一幅灰度图像. $\boldsymbol{I}$ 经 SVD 变换可表示为:

$$\boldsymbol{I}=\boldsymbol{USV}^{\mathrm{T}}=\sum_{i=1}^{r}\lambda_i\boldsymbol{U}_i\boldsymbol{V}_i^{\mathrm{T}}$$

其中 $\boldsymbol{U}$、$\boldsymbol{V}$ 分别为 $m\times m$ 和 $n\times n$ 的正交矩阵;$\boldsymbol{S}$ 是非负对角阵,$\boldsymbol{S}$ 中的 $\lambda_1,\lambda_2,\cdots,\lambda_r$ 称为矩阵 $\boldsymbol{I}$ 的奇异值,且满足 $\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_r$;$r$ 为矩阵 $\boldsymbol{I}$ 的秩. $\boldsymbol{U}_i$ 与 $\boldsymbol{V}_i$ 分别称为奇异值 λ_i 的左右奇异向量;$\boldsymbol{U},\boldsymbol{V}$ 的列分别是 $\boldsymbol{II}^{\mathrm{T}}$ 与 $\boldsymbol{I}^{\mathrm{T}}\boldsymbol{I}$ 的特征向量. 在本文,我们称 $\boldsymbol{U}_1(\boldsymbol{V}_1)$ 为矩阵 $\boldsymbol{I}$ 的第一奇异值向量,向量 $\boldsymbol{U}_1(\boldsymbol{V}_1)$ 在多维空间中的方向称为第一奇异值向量方向(First Singular Value Vector Direction,FSVVD).

关于 SVD 有很多重要的属性,有兴趣的读者可以参考文献[20]. 其中奇异值的稳定特性是常用的一个属性. 设 $\boldsymbol{A}$、$\boldsymbol{B}$ 为 $m\times n$ 的矩阵,二者的奇异值分别表示为 $\xi_1,\xi_2,\cdots,\xi_n$ 与 $\eta_1,\eta_2,\cdots,\eta_n$,则存在这样的关系:$|\xi_i-\eta_i|\leq\|\boldsymbol{A}-\boldsymbol{B}\|_2$. 这表明对矩阵 $\boldsymbol{A}$ 施加一个抖动 $\boldsymbol{\varepsilon}$(设 $\boldsymbol{\varepsilon}$ 为 $m\times n$ 的矩阵且 $\boldsymbol{B}=\boldsymbol{A}+\boldsymbol{\varepsilon}$),则 $\boldsymbol{A}$ 的奇异值具有稳定性,其中第一个奇异值 λ_1 抖动最小. 由此我们可以联想到 $\boldsymbol{A}$ 的第一奇异值向量在多维空间的指向上具有一定的稳定性,分析过程如下.

先对 $\boldsymbol{A},\boldsymbol{B}$ 执行 SVD 变换,表示为:$\boldsymbol{A}=\boldsymbol{USV}^{\mathrm{T}}=\sum_{i=1}^{r}\lambda_i\boldsymbol{U}_i\boldsymbol{V}_i^{\mathrm{T}}$,$\boldsymbol{B}=\hat{\boldsymbol{U}}\hat{\boldsymbol{S}}\hat{\boldsymbol{V}}^{\mathrm{T}}=\sum_{i=1}^{r}\xi_i\hat{\boldsymbol{U}}_i\hat{\boldsymbol{V}}_i^{\mathrm{T}}$,

其中 $\boldsymbol{B}=\boldsymbol{A}+\boldsymbol{\varepsilon}$,代表对 $\boldsymbol{A}$ 施加抖动 $\boldsymbol{\varepsilon}$ 后的矩阵. 向量 $\boldsymbol{U}_1$ 与 $\hat{\boldsymbol{U}}_1$ 的夹角 θ 定义为:

$$\cos(\theta)=(\boldsymbol{U}_1\cdot\hat{\boldsymbol{U}}_1)/(|\boldsymbol{U}_1||\hat{\boldsymbol{U}}_1|),$$

因 $|\boldsymbol{U}_1|=1,|\hat{\boldsymbol{U}}_1|=1$,故

$$\cos(\theta)=(\boldsymbol{U}_1\cdot\hat{\boldsymbol{U}}_1)=\boldsymbol{U}_1^{\mathrm{T}}\cdot\hat{\boldsymbol{U}}_1$$

同理,向量 $\boldsymbol{V}_1$ 与 $\hat{\boldsymbol{V}}_1$ 的夹角 $\hat{\theta}$ 可定义为:

$$\cos(\hat{\boldsymbol{\theta}})=(\boldsymbol{V}_1\cdot\hat{\boldsymbol{V}}_1)=\boldsymbol{V}_1^{\mathrm{T}}\cdot\hat{\boldsymbol{V}}$$

根据文献[20]中的定理 7,有

$$\|\boldsymbol{U}-\hat{\boldsymbol{U}}\|_F\leqslant M_1,\ \|\boldsymbol{V}-\hat{\boldsymbol{V}}\|_F\leqslant M_2,$$

其中

$$M_1=4\sqrt{2n}(\sqrt{2}+1)\|A\|_F\varepsilon_F/\lambda^2+o(\varepsilon_F^2),$$

$$\lambda^2=\min_{i\neq j}|\lambda_i^2-\lambda_j^2|$$

$$M_2=\begin{cases}2\|A^+\|_2\varepsilon_F+M_1,\mathrm{rank}(A)=n\\ 2\|A^+\|_2\sqrt{n}\varepsilon_2+4\sqrt{2n}(\sqrt{2}+1)\|A^+\|_2\cdot\\ \quad\|A\|_F\varepsilon_F/\lambda^2+o(\varepsilon_F^2),\mathrm{rank}(A)<n\end{cases}$$

根据范数不等式有

$$\|(\boldsymbol{U}_1-\hat{\boldsymbol{U}}_1,\boldsymbol{U}_2-\hat{\boldsymbol{U}}_2,\cdots,\boldsymbol{U}_m-\hat{\boldsymbol{U}}_m)\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}\|_2\leqslant\|\boldsymbol{U}-\hat{\boldsymbol{U}}\|_F$$

即

$$\| \boldsymbol{U}_1 - \hat{\boldsymbol{U}}_1 \|_2 \leqslant M_1$$

这又等价于

$$\| \boldsymbol{U}_1 - \hat{\boldsymbol{U}}_1 \|_2^2 = (\boldsymbol{U}_1 - \hat{\boldsymbol{U}}_1, \boldsymbol{U}_1 - \hat{\boldsymbol{U}}_1) \leqslant M_1^2$$

所以

$$(\boldsymbol{U}_1 - \hat{\boldsymbol{U}}_1, \boldsymbol{U}_1 - \hat{\boldsymbol{U}}_1) = 2 - 2\cos(\theta) \leqslant M_1^2,$$

即

$$\cos(\theta) \geqslant 1 - M_1^2/2, \tag{1}$$

同理可得

$$\cos(\hat{\theta}) \geqslant 1 - M_2^2/2 \tag{2}$$

由此可知，当 $\| \boldsymbol{\varepsilon} \| \to 0$，有 $M_1 \to 0, M_2 \to 0$，因而有 $\cos(\theta) \to 1, \cos(\hat{\theta}) \to 1$，即 $\theta \to 0, \hat{\theta} \to 0$. 由此证明向量 $\boldsymbol{U}_1(\boldsymbol{V}_1)$ 相对于抖动 $\boldsymbol{\varepsilon}$ 在空间的指向上具有稳定性.

3 多波段遥感影像水印方案

遥感影像集包含多个波段的图像，如 AVIRIS(Airbone Visible/Infrared Imaging Spectrometer)影像集包含 224 个波段. 设遥感影像集 RSI 中有 k 个波段图像，每个波段表示为 $I_j(j=1,2,\cdots,k,k+1)$，其中 I_{k+1} 表示 k 个波段的平均图像. 本节提出的零水印思想是对每个波段的图像 $I_j(j=1,2,\cdots,k,k+1)$ 提取特征水印；在检测时，对一个待验证的遥感影像集，若其平均图像含有水印，则检测结束，否则检测其中的每个波段是否含有水印，以此证明特定波段图像的版权.

3.1 多波段水印提取算法

本节阐述多波段遥感影像特征水印的提取算法. 算法先在每个波段图像的 2 级 CT 域的低频系数中选择一定数量的数据子块来抽取水印特征，并使所选择的数据子块尽可能均匀地分布在低频系数区的纹理当中. 接着要对遥感影像集 RSI 中的每个波段图像包括平均图像 I_j 分别提取特征水印. 然后对给定波段图像的两个选定的特征数据子块，根据各自的第一奇异值向量与事先设定的某一同维度参考向量夹角大小关系生成 1 比特特征水印信息. 图 1 给出了特征水印提取的块图，具体过程概括如下：

(1)根据密钥 K_1 选择 $2l$ 个数据子块用于抽取特征，并把数据子块的 $\boldsymbol{U}_l$ 向量及位置信息存放在数组 PosSel 中；从 PosSel 中逐个取出 $\boldsymbol{U}_l$ 向量，得到向量序列 $\boldsymbol{V}_i(i=1,2,\cdots,2l)$，其中 l 表示将要抽取的二进制序列的长度. 数据子块的尺寸设置为 4，并依照均匀度 E 值来判定合适的纹理块，其定义如下：

$$E = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{|B_k(i,j) - \bar{B}_k|}{\bar{B}_k} \tag{3}$$

其中 B_k，为任意给定的 $m \times n$ 的图像块，$B_k(i,j)$ 代表以 B_k 中以 (i,j) 为坐标的像素值，$\bar{B}_k$ 为 B_k 的像素平均值.

(2)根据密钥 K_2 随机置乱 $\boldsymbol{V}_i$ 的下标，输出新的向量序列 $\boldsymbol{V}_j'$，$(j=1,2,\cdots,2l)$，并由密钥 K_3 随机建立一个非零参考向量 $\boldsymbol{V}^r$，使 $\boldsymbol{V}^r$ 的维度与 $\boldsymbol{U}_1$ 向量相同.

(3)按照式(4)计算 $\boldsymbol{V}_j'$，$(j=1,2,\cdots,2l)$ 与 $\boldsymbol{V}^r$ 的向量夹角：

$$\cos(\theta_j) = (\boldsymbol{V}^r \cdot \boldsymbol{V}_j') / (|\boldsymbol{V}^r \| \boldsymbol{V}_j'|), \text{if} |\boldsymbol{V}_j'| \neq 0;$$
$$\theta_j = \text{null}, \text{if } |\boldsymbol{V}_j'| = = 0. \tag{4}$$

(4)由式(5)生成二进制特征水印序列 bi：

$$b_i = \begin{cases} 1, \text{if } \theta_i \geqslant \theta_{i+l} \text{ and } \theta_i \neq \text{null and } \theta_{i+l} \neq \text{null}; \\ 0, \text{if } \theta_i < \theta_{i+l} \text{and } \theta_i \neq \text{null and } \theta_{i+l} \neq \text{null}; \\ \text{null}, \text{if } \theta_i = = \text{null or } \theta_{i+l} = = \text{null}; \end{cases}$$
$$i = 1,2,\cdots,l. \tag{5}$$

(5)对事先准备好的二进制可视水印 $W(w_i, i=1,2,\cdots,s)$ 执行以 K_4 为密钥的 Arnold 置乱，设 $c_i = b_i(i=1,2,\cdots,l)$，如果 $l < s$，重复 c_i 序列直到与 w_i 序列长度相等. 再对 w_i、c_i 执行 XOR 运算，生成 W'.

(6)将波段图像 I_j 的注册信息 RegInf$[I_j]$ 提交到版权注册中心，其中 RegInf$[I_j]$ 包含密钥 $K_2 \sim K_4$，W'，坐标信息 PosSel$[i].(x,y)$，$i=1,2,\cdots,2l$.

上述过程用到了 4 个密钥 $K_1 \sim K_4$. 其中 K_1 用于水印提取位置的选择，所需存储空间小于 10 字节；$K_2 \sim K_4$ 需 3 字节存储空间，*PosSel* 中的 $2l$ 个坐标信息要占用 $4l$ 字节，其中 l 为待抽取的特征水印比特数；此外，用于生

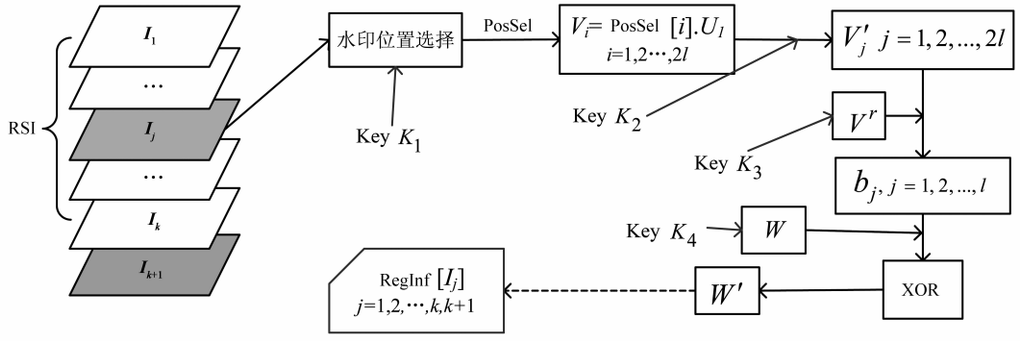


图1 特征水印提取块图

成提交到注册中心的 W' 需 s 比特存储空间. 因此单个波段未经压缩处理的注册信息 RegInf[I_j]小于$(4l+3)\times 8+s+10\times 8$ 比特. 如果不知道 K_1,水印攻击者就无法知道哪些数据子块被选来抽取水印信息,因而不能针对性地执行水印攻击. 若不知道这 $K_2\sim K_4$ 与 *PosSel* 中的坐标信息,私下建立的水印软件不能正确地提取影像版权所有者设置的水印信息. 因此所提出的算法可以公开,但每个波段的注册信息 RegInf[I_j]与 K_1 必须安全保存.

3.2　单波段水印检测与虚警概率

单波段图像的水印检测过程与特征生成过程基本一致. 设待检测的遥感影像集为 RSI′,并假设 RSI′中的一个波段图像 I_k 与水印注册信息 RegInf[I_m]相对应,具体检测过程如下:

(1)对 I_k 执行 2 级 CT,输出低频系数 LF2.

(2)从 RegInf[I_m]提取出以下信息:密钥 $K_2\sim K_4$,W',以及坐标信息 PosSel[i]. (x,y),$i=1,2,\cdots,2l$.

(3)根据获得的坐标系列(x_i,y_i),$i=1,2,\cdots,2l$,以及设定大小为 4 的行列尺寸,从 LF2 中截取数据子块 SubBk_i,并执行 SVD 变换提取 $\boldsymbol{U}_1$ 向量,从而得到向量序列 $\boldsymbol{V}_i(i=1,2,\cdots 2l)$.

(4)执行3.1 节算法过程中的(2)~(4)步,生成二进制序列 b_i',$i=1,2,\cdots,l$. 设 $c_i=b_i'$,如果 l 小于水印 W 的长度 s,重复 c_i 序列直到长度为 s. 对 c_i、$w_i'\in W'$ 执行 XOR 运算,生成 W''.

(5)对 W'' 执行以 K_4 为参数的 Arnold 反置乱,输出可视水印 $\hat{W}$.

(6)水印相关性检测. 根据式(6)定义的比特正确率(Bit Correction Rate,BCR)度量被提取的水印性能.

$$\mathrm{BCR}(W,\hat{W})=1-\left(\sum_{i=1}^{l} w_i\oplus\hat{w}_i\right)/l \tag{6}$$

其中⊕代表 XOR 操作,l 为抽取的二进制序列 b_i 的长度. 如果 I_j 的 BCR 值不小于检测阈值 $T(0<T<1)$,则证明 I_k 存在水印,否则 I_k 中不存在水印. 检测阈值 T 可以通过实验获得. 在检测过程中,对阈值 T 存在虚警错误,即对未嵌入水印的影像检测时判断存在水印. 虚警概率定义如下:

$$P_f=p(\mathrm{BCR}\geq T\mid \text{no watermark}) \tag{7}$$

由于二进制随机序列与提取的序列 $b_i(i=1,2,\cdots,l)$ 每比特匹配的概率为 0.5,则虚警概率定义为:

$$P_f=\sum_{m=\mathrm{int}(T\times l)}^{l}(0.5^m\times C_l^m) \tag{8}$$

其中,T 为检测阈值,m 为匹配的比特数量,C_l^m 为 l 与 m 形成的组合数,int()代表取整操作. 在后续实验中计算可得,当设置 $l=512$ 且 $T=0.615$ 时,$P_f=1.669\times 10^{-7}$(详见 4.1 节).

3.3　遥感影像集的水印检测

由于遥感影像集含有多个波段的图像,被检测的遥感影像集 RSI′中各波段除了会遭受图像处理攻击外,还可能遭到波段攻击,即波段增加、删除、交换或替换. 因此检测时先要解决被检测的波段图像与水印注册信息的对应关系,为此,我们的检测算法分两步进行,第一步执行快速检测策略;若第一步失败,执行第二步,一般检测,即对每个波段都进行检测. 检测方案如图 2 所示,检测过程是盲的,无需原始遥感影像集 RSI,具体过程如下:

第 1 步,快速检测. 首先从注册中心取出原始遥感影像集 RSI 中平均图像 I_{k+1} 对应的注册信息 RegInf[I_{k+1}];设被检测的遥感影像集包含 m 个波段,其平均图像表示为 I_{m+1},接着根据 RegInf[I_{k+1}] 与 I_{m+1} 执行单波段水印检测(3.2 节). 如果 I_{m+1} 被检测到水印,表明 RSI′中存在水印,否则继续执行第二步的检测. 注意,如果快速检测成功,只能说明 RSI′中部分波段存在水印,当然也可能每个波段都存在水印.

第 2 步,逐波段检测. 如果第一步未能检测到水印,RSI′中可能每个波段都不存在水印,也可能因经受波段攻击使部分波段存在水印. 因此,对 RSI′中的每个波段 $I_j(j=1,2,\cdots,m)$ 分别与水印注册信息集中的每

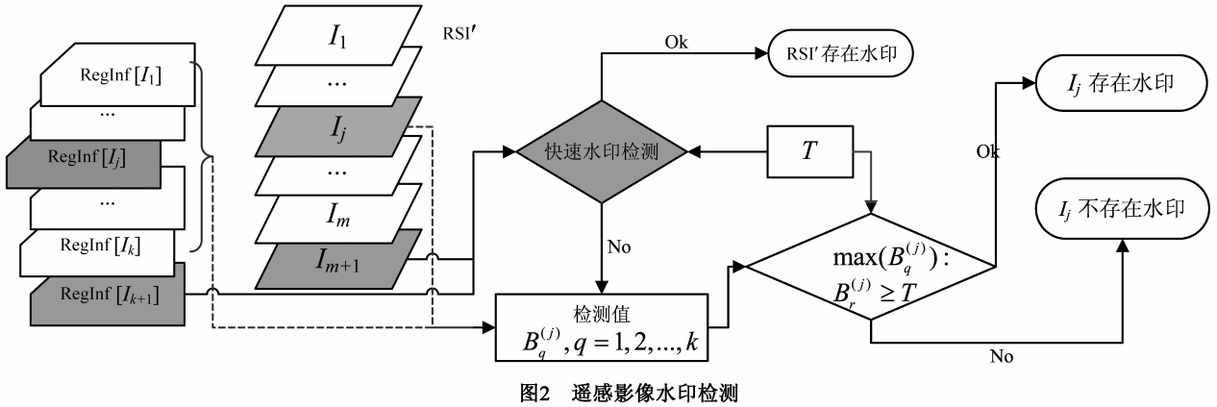


图2　遥感影像水印检测

个注册信息 RegInf[I_i]($i=1,2,\cdots,k$)执行 k 次单波段水印检测(3.2 节),按照式(6)生成检测值序列 $B_q^{(j)}$($q=1,2,\cdots,k$). 如果 $\max(B_q^{(j)})$ 为 $B_r^{(j)}$,且 $B_r^{(j)}\geq T$,则说明 RSI′中的波段 I_j存在水印. 值得注意的是,由于 $\boldsymbol{I}_j$可能被图像处理攻击过,$\boldsymbol{I}_j$在原始遥感影像集 RSI 中对应的波段未必是 r. 如果 $B_r^{(j)}<T$,则 RSI′中的波段 I_j不存在水印.

在原始遥感影像集 RSI 中,注册信息 RegInf[I_i]($i=1,2,\cdots,k$) 与波段图像 I_i是对应的. 由于 I_m与 I_i存在很大的相关性($m\neq i$),I_i可以看成 I_m经受某种图像攻击后的结果. 因此当用 RegInf[I_m]去检测波段 I_i,检测值可能大于或等于阈值 T. 依据此现象,在第 2 步的检测过程中,如果 $B_r^{(j)}\geq T$,则可能存在 $B_t^{(j)}\geq T(t\neq r)$.

3.4 鲁棒性分析

本节要对给定的图像攻击 $\boldsymbol{A}$,从理论上分析式(6)的数学期望,即 E(BCR). 由于 w_i、$\hat{w}_i$($i=1,2,\cdots,l$)各比特匹配事件是相互独立的,于是问题转化为 w_i、$\hat{w}_i$ 中任意一比特匹配的概率.

在波段图像 I_k的 2 级 CT 低频域 LF2 中,任意截取 2 个 4×4 的数据块,分别表示为 SubBk1、SubBk2;各自的 $\boldsymbol{U}_1$向量与参考向量 $\boldsymbol{V}'$的夹角分别用 θ_1、θ_2表示,并假定 θ_1、θ_2在区间[0,π]上服从随机均匀分布. 当波段图像 I_k经受图像攻击 A 扰动后,与 θ_1、θ_2对应的夹角分别用 β_1、β_2表示. 因此问题进一步转化为:如果 $\theta_1\geq\theta_2$,求 $\beta_1\geq\beta_2$的概率,即 $P(\beta_1\geq\beta_2)$;或者当 $\theta_1<\theta_2$,求 $P(\beta_1<\beta_2)$.

设波段图像 I_k因攻击 A 扰动后,SubBk1、SubBk2 各自的 $\boldsymbol{U}_1$向量波动角度平均值小于 γ($\gamma\geq0$) 的概率为 P_1. 则在 $\theta_1\geq\theta_2$条件下:1)如果 $\theta_1-\theta_2\geq2\gamma$,设 $P_1=P(\beta_1\geq\beta_2)$;2)如果 $\theta_1-\theta_2<2\gamma$,$\beta_1\geq\beta_2$的情况表现为随机,则有 $P(\beta_1\geq\beta_2)=0.5$;3) 此外 $P(\theta_1-\theta_2\geq2\gamma)=1-2\gamma/180$. 因而有:

$$P(\beta_1\geq\beta_2\mid\theta_1\geq\theta_2)=P(\beta_1\geq\beta_2)\times P(\theta_1-\theta_2\geq2\gamma)+P(\beta_1\geq\beta_2)\times P(\theta_1-\theta_2<2\gamma)$$
$$=P_1\times(1-2\gamma/180)+0.5\times(2\gamma/180).$$

同理,在 $\theta_1<\theta_2$的前提下也有相同的结果,即:

$$P(\beta_1<\beta_2\mid\theta_1<\theta_2)=P(\beta_2>\beta_1\mid\theta_2>\theta_1)$$
$$=P_1\times(1-2\gamma/180)+0.5\times(2\gamma/180)$$

归纳起来,波段图像 I_k针对攻击 A 的鲁棒性分析可表示为:

$$\mathrm{E(BCR)}=P_1\times(1-2\gamma/180)+0.5\times(2\gamma/180)$$

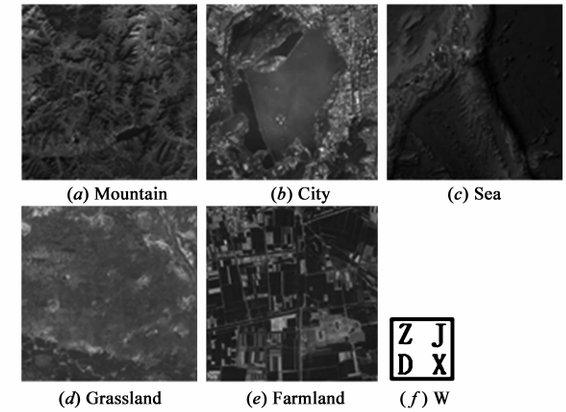
若攻击 A 为单项普通的图像处理(第 4 节表 1),并取 $\gamma=5°$时,根据实验测试有 $P_1=0.994$(受篇幅限制,测试数据被略),此时式(6)的数学期望 E(BCR)=0.9666.

表 1 用于仿真的图像攻击

编号	攻击	编号	攻击
1	绝对增亮(+30)	14	等比缩放(5×5)
2	相对增亮:[0,1]→[0.4,1]	15	变比缩放(0.8×1.8)
3	绝对变暗(-30)	16	均值滤波(5×5)
4	相对变暗([0,1]→[0,0.8])	17	中值滤波(5×5)
5	增加对比度([0.2,0.8]→[0,1])	18	维纳滤波(5×5)
6	降低对比度([0,1]→[0.2,0.8])	19	随机行列删除(5×10)
7	乘积性噪声(0.005)	20	周围剪切(25%)
8	高斯噪声(0.005)	21	抖动(dither)
9	椒盐噪声(0.005)	22	模糊(blurring, Gaussian,7×7,3)
10	旋转 30°(裁剪)	23	锐化(sharpen)
11	直方图均衡化(64)	24	随机剪切(25%)
12	JPEG(Q=30)	25	移除比特位(第5位置0)
13	等比缩放(0.5×0.5)		

4 实验结果

为了评价所提出方案的性能,我们做了一系列的实验测试. 实验在 Pentium(R) Dual-Core CPU E6600 3.06GHZ、MEM 2G;WinXp、Matlab2010 环境中进行. 从 Google Earth 中截取了 5 个不同场景 3 波段 SPOT 遥感影像集 $\mathrm{RSI}_1\sim\mathrm{RSI}_5$,每波段尺度为 800×800,如图 3($a$)~($e$)所示. 每个影像集 RSI_j($j=1,2,3,4,5$)的 3 个波段分别用 rRs_j、gRs_j、bRs_j表示,分别代表红色、绿色、蓝色波段;平均波段图用 aRs_j表示,因此参与实验测试的图片共 20 幅. 二进制水印图片 W 尺寸为 64×64,水印长度 $s=4096$,如图 3(f)所示. 对每个波段抽取的二进



(a) Mountain (b) City (c) Sea

(d) Grassland (e) Farmland (f) W

图3 用于测试的遥感影像(a)~(e):$\mathrm{RSI}_1\sim\mathrm{RSI}_5$,($f$) 水印标记

制序列长度 l 设定为 512. 此外设计了 25 种图像处理来仿真攻击,用于观察水印方案的稳健性,如表 1 所示. 其中$[n_1,n_2]\rightarrow[n_3,n_4]$($0\leqslant n_i\leqslant 1, i=1,2,3,4.$)表示对比度(亮度)值调整.

4.1　抗碰撞实验

从图 3 的遥影像集 $RSI_1 \sim RSI_5$ 中各抽取一个波段图像,按 3.1 节的方法获得各自的二进制序列,检测任意 2 个序列间的 BCR. 检测结果表明互不相同的序列间最大值 $BCR_1 = 0.573$. 此外,把随机生成 10000 个长度 $l=512$ 的 0 - 1 序列与从波段图像 rRs2 中抽取的二进制序列进行相关检测,BCR 最大值 $BCR_2 = 0.585$. 因此在当前实验参数环境下,水印检测阈值应满足条件:

$$T \geqslant \max(BCR_1, BCR_2) \tag{9}$$

依据式(9),本文设置 $T = 0.615$,由经式(8)编程计算,此时的虚警概率 $P_f = 1.669 \times 10^{-7}$.

4.2　抗攻击实验

我们执行了一系列图像处理攻击实验来检测本文方案的鲁棒性. 图 4、图 5 分别给出了来自表 1 的单项攻击与随机 3 项组合攻击的结果,其中(包括后续出现的相关图)平均 BCR 是指图 4 中共 20 个波段图像对同一攻击检测出的 BCR 平均值. 图 5 中第一项组合攻击"13 + 14 + 23"表示顺序执行表 1 中的攻击项:13 - 等比缩放(0.5 × 0.5)、14 - 等比缩放(5 × 5)、23 - 移除比特位. 图 6、图 7 分别给出了部分单项攻击与灰度攻击鲁棒性的详细测试结果. 波段攻击就是对遥感影像集进行增加、删除或置乱波段图像操作,实验表明本方案对波段攻击是鲁棒的,因篇幅所限在此省略相关实验数据及分析.

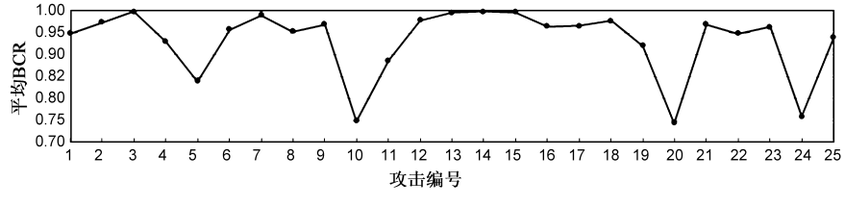


图4　单项攻击鲁棒性

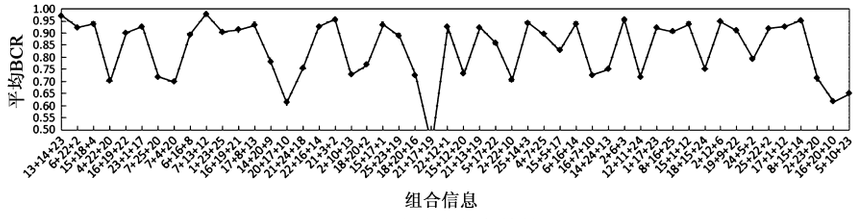


图5　组合攻击的鲁棒性

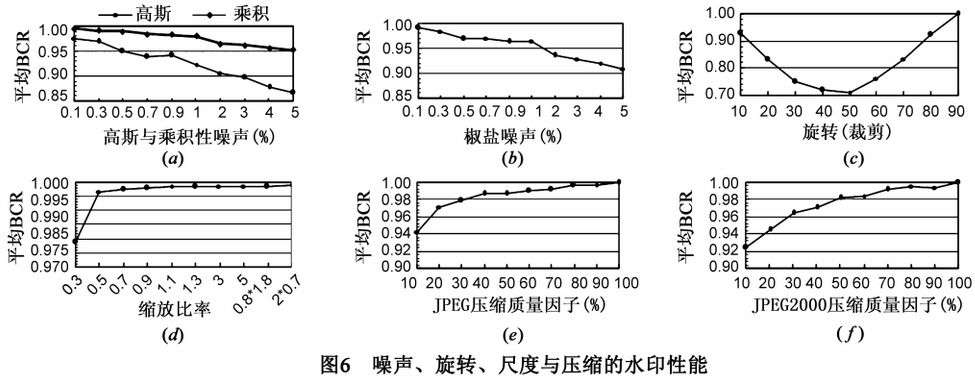


图6　噪声、旋转、尺度与压缩的水印性能

5　结论

多波段数字遥感影像是一种重要的空间信息资源,有着广泛的应用领域,其版权保护不容忽视. 针对近年来关于遥感影像水印算法存在的问题,本文提出了一种适应性强的水印方案,其特点概括如下. (1)提出了一种新的水印方案,包括基于第一奇异值向量方向稳定性的特征水印提取与检测,以及波段攻击与检测. (2)对遥感影像的大尺度、多波段、数据高保真特性针对性强,这些由方案的低计算复杂度、零水印嵌入、

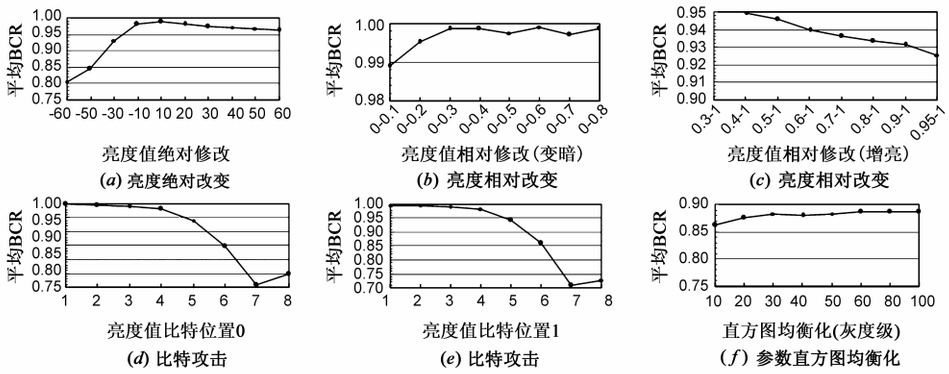


图7 灰度攻击的性能

多波段的快速检测与普通检测策略、盲性检测、抗灰度攻击与波段攻击的强鲁棒性来实现.(3)鲁棒性好,能抵制广泛的图像处理攻击;本方案能经受多种普通图像攻击、特殊攻击(灰度攻击)、三项组合攻击.(4)抗碰撞性能好,当水印抽取序列长度 $l=512$,检测阈值设定为 $T=0.615$ 时,虚警概率 $P_f=1.669\times10^{-7}$,随着 (l,T) 略微增加,P_f 将按指数级下降.

本文方案是面向多波段遥感影像集的一个比较全面的版权保护方案,也可应用于高光谱遥感影像的版权保护.由于普通图像可以看成是单波段的特殊遥感影像,方案经适当修改可用于普通图像的版权保护.

参考文献

[1] Do M, Vetterli M. Contourlets: a directional multiresolution image representation[A]. IEEE International Conference on Image Processing (ICIP'2002)[C]. Rochester: IEEE, 2002. 357 – 360.

[2] Do M, Vetterli M. The contourlet transform: an efficient directional multiresolution image representation[J]. IEEE Trans Image Process, 2005, 14 (12): 2091 – 2106.

[3] 李海峰,宋巍巍,王树勋. 基于 Contourlet 变换的稳健性图像水印算法[J]. 通信学报,2006,27 (4):287 – 294.
Li Hai-feng, Song Wei-wei, Wang Shu-xun. Robust image watermarking algorithm based on contourlet transform[J]. Journal on Communications, 2006, 27 (4): 287 – 294. (in Chinese)

[4] 楼偶俊,王相海,王钲旋. 基于 Contourlet 域重要系数特性的自适应图像水印算法[J]. 计算机科学,2009,6(3):237 – 240.
Lou Ou-jun, Wang Xiang-hai, Wang Zheng-xuan. Adaptive image watermarking algorithm based on the characteristics of important coefficients in Contourlet domain[J]. Computer Science, 2009, 6(3): 237 – 240. (in Chinese)

[5] 楼偶俊,王钲旋. 基于特征点模板的 Contourlet 域抗几何攻击水印算法研究[J]. 计算机学报,2009,32(2):308 – 317.
Lou Ou-jun, Wang Zheng-xuan. A Contourlet-domain watermarking algorithm against geometric attacks based on feature template[J]. Chinese Journal of Computers, 2009, 32(2): 308 – 317. (in Chinese)

[6] Niu P P, Wang X Y, Yang Y P, et al. A novel color image watermarking scheme in nonsampled contourlet-domain[J]. Expert Systems with Applications, 2011, 38(3): 2081 – 2098.

[7] Akhaee M A, Sahraeian S M E, Marvasti F. Contourlet-based image watermarking using optimum detector in a noisy environment[J]. IEEE Transactions on Image Processing, 2010, 19(4): 967 – 980.

[8] Wang X Y, Yang Y P, Yang H Y. A novel nonsampled contourlet-domain image watermarking using support vector regression[J]. Journal of Optics A-Pure and Applied Optics, 2009, 11(12): 327 – 334.

[9] Song H H, Yu S Y, Yang X K, et al. Contourlet-based image adaptive watermarking[J]. Signal Processing-Image Communication, 2008, 23(3): 162 – 178.

[10] Fridrich J, Goljan M, Du R. Lossless data embedding-new paradigm in digital watermarking[J]. EURASIP Journal on Applied Signal Processing, 2002, (2): 185 – 196.

[11] Vleeschouwer C D, Delaigle J F, Macq B. Circular interpretation of bijective transformations in lossless watermarking for media asset management[J]. IEEE Transactions on Multimedia, 2003, 5(1): 97 – 105.

[12] Chang C, Hwang K, Hwang M. A block based digital watermarks for copy protection of images[A]. 5th Asia-Pacific Conf Commun and 4th Optoelectron Commun Conf[C]. Beijing: China Institute of Communications, 1999. 977 – 980.

[13] 温泉,孙锬锋,王树勋. 零水印的概念与应用[J]. 电子学报,2003,31(2):1 – 3.
Wen Q, Sun T F, Wang S X. Concept and application of zero watermark[J]. Acta Electronica Sinica, 2003, 31

(2):1 – 3. (in Chinese)
[14] Tsai H H, Tseng H C, Lai Y S. Robust lossless image watermarking based on alpha-trimmed mean algorithm and support vector machine[J]. Journal of Systems and Software, 2010, 83(6): 1015 – 1028.
[15] Li J, Zhang Y D, Chen G Y. Zero-watermarking for copyright protection of remote sensing image[A]. 2008 9th International Conference on Signal Processing (ICSP 2008)[C]. Beijing, China: IEEE, 2008. 1083 – 1086.
[16] Monga V, Mhcak M K. Robust and secure image hashing via non-negative matrix factorizations[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 376 – 390.
[17] 牛夏牧,焦玉华. 感知哈希综述[J]. 电子学报,2008,36(7):1405 – 1411.
Niu Xia-mu, Jiao Yu-hua. An overview of perceptual hashing[J]. Acta Electronica Sinica, 2008, 36(7): 1405 – 1411. (in Chinese)
[18] Lv X D, Wang J. Perceptual image hashing based on shape contexts and local feature points[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(3): 1081 – 1093.
[19] Zhao Y, Wang S, Zhang X, et al. Robust hashing for image authentication using Zernike moments and local features[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 55 – 63.
[20] 李治林,黄开斌. 特征向量的几个扰动定理[J]. 高等学校计算数学学报,1990,(3):284 – 289.

作者简介

付剑晶　男,1976 年生于江西,副教授,博士,主要研究方向为数字图像水印、视频认证等. E-mail: fjjmsn@163.com

王　珂　男,1964 年生于浙江,教授、博士生导师,主要研究方向:信息安全、数据挖掘、遥感监测等.