

## 一种新的遥感图像机密信息隐藏算法

岳 芹<sup>1</sup>, 陈 晨<sup>2</sup>

(1. 皖西学院 数理系, 安徽 六安 237000; 2. 福建富士通信息软件有限公司, 福州 350013)

(yqer@163.com)

**摘 要:** 为了防止遥感图像包含的机密信息被泄露, 将基于样本的图像修补方法用于遥感图像机密信息隐藏。该方法从遥感图像中选择与机密信息图像块最大相似区域, 覆盖机密信息块, 从而达到机密信息隐藏的目的。该方法不仅具有很强的不觉察性, 而且对于遥感图像的使用价值影响较小。结合数字水印技术, 实现了根据用户权限来决定用户能否看到隐藏的机密信息, 从而方便了遥感图像的使用。仿真实验结果表明, 该方法是可行的, 能够提高遥感图像使用的安全性。

**关键词:** 图像修补; 遥感图像; 信息隐藏; 数字水印

**中图分类号:** TP309 **文献标志码:** A

## New secrete information hiding method for remote sensing images

YUE Qin<sup>1</sup>, CHEN chen<sup>2</sup>

(1. Department of Mathematics and Physics, West Anhui University, Lu'an Anhui 237000, China;

2. Fujian Fujitsu Communication Software Company Limited, Fuzhou Fujian 3500013, China)

**Abstract:** To prevent the leak of secrete information hidden in remote sensing image, a sample-based method for image inpainting was used in hiding secrete information in remote sensing image. The method selected the maximum region similar to secrete information image, and covered the secrete information block, thus hiding the secrete information. The method had not only strong invisibility, but also little influence on the use of remote sensing image. With reference to digital watermarking, whether users can see secrete information or not according to their authority status was realized, which facilitated the use of remote sensing image. Experimental results show that the method is feasible, and it improves the application security of remote sensing image.

**Key words:** image inpainting; remote sensing image; information hiding; digital watermarking

随着互联网的发展, 数字产品的广泛传播使得遥感图像本身包含的机密信息被泄露的可能性大大增加<sup>[1]</sup>。如果简单地对图像局部加密或者掩盖, 无疑对外宣告该处含有值得“注意”的信息。因此, 本文尝试利用基于样本的图像修补方法隐藏该类机密信息<sup>[2]</sup>, 该方法有很强的隐蔽性, 不易引起他人的特别留意, 而且对遥感图像使用的影响较小。仿真实验结果证明了该方法是可行的。

### 1 一种基于样本的图像修补方法

目前数字图像修补技术的应用范围越来越广, 成为当前计算机图形学和计算机视觉中的一个研究热点, 而对于大区域修补常用的技术是基于样本的纹理合成图像修补技术, 即从图像的源区域复制像素点填充进目标区域中, 包含了已有的纹理和结构信息, 而区域之间的结构信息则通过改变像素点的填充顺序可以得到。这样算法既解决了同时生成纹理和结构信息的问题, 也保持了原有纹理合成算法高效的优点<sup>[3-5]</sup>。本文正是基于样本的图像修补算法, 首先移除遥感图像中的机密信息, 再对其修复, 并结合数字水印技术, 实现了遥感图像机密信息的隐藏。文献[4-5]都具体介绍了该方法的主要实现过程, 本文简单介绍如下。

设有图像  $I$ , 待填充的目标区域为  $\Omega$ , 轮廓线为  $\delta_\Omega$ ,  $p$  是轮廓线上一点, 源区域为  $\Phi$  ( $\Phi = I - \Omega$ ), 如图 1 所示。

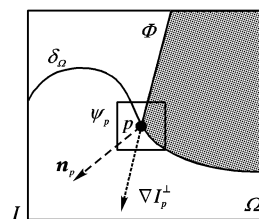


图 1 修补区域示意图

目标区域内沿轮廓线的方形模板  $\psi_p$ , 大小可取为  $3 \times 3$ ,  $9 \times 9$ , 实际应用中应设为比最大的可鉴别的纹元略大。中心点  $\psi_p$  在轮廓线  $\delta_\Omega$  上, 模板  $\psi_p$  应包含了一部分已合成的像素。在算法设计中, 模板内的每个像素点都有一个颜色值和置信值 (表示该点的填充情况, 为 1 表示已填充, 为 0 表示还未填充)。初始化完成后, 循环执行下面的 3 个步骤, 直到填充全部完成。

#### 1.1 计算优先级

优先级的大小取决于两部分因素: 一部分是该模板的数据值, 它反映了模板的结构信息强弱, 从而保证线性结构部分的优先合成; 另一部分是模板的置信度值, 要求优先填充那些含已填充像素较多部分的模板, 因为填充这样的模板可以依赖更多的已知像素。二者相互制约, 共同构成优先级。这里的优先级计算用下面的公式<sup>[4]</sup>:

收稿日期: 2009-05-25; 修回日期: 2009-07-15。 基金项目: 安徽省高校青年教师资助项目 (2008jq1153)。

作者简介: 岳芹 (1978-), 女, 安徽宿州人, 讲师, 硕士, 主要研究方向: 模糊数学; 陈晨 (1982-), 男, 安徽宿州人, 硕士, 主要研究方向: 信息隐藏、图像处理。

$$P(p) = C(p)D(p) \quad (1)$$

$$C(p) = \frac{\sum_{q \in \psi_p \cap \Omega} C(q)}{|\psi_p|}$$

$$D(p) = \frac{|\nabla I_p^\perp \cdot \mathbf{n}_p|}{\alpha}$$

其中:  $C(p)$  表示模板的置信度值;  $D(p)$  表示模板的数据值;  $C(q)$  表示模板内像素点的置信值, 初始化时, 位于目标区域中的每个点的值设为 0, 源区域中的每个点的值设为 1。即:

$$C(q) = \begin{cases} 0, & \forall q \in \Omega \\ 1, & \forall q \in I - \Omega \end{cases} \quad (2)$$

$|\psi_p|$  是模板  $\psi_p$  的面积;  $\alpha$  是一个标准化参数, 对于一般的灰度图来说,  $\alpha = 255$ ;  $\mathbf{n}_p$  是轮廓线在  $p$  点的单位法向量;  $\nabla I_p^\perp$  是在  $p$  点的光谱透线的强度和方向。

对于每一个模板, 根据计算得到的优先级决定合成顺序。根据公式, 一方面, 包含了较多的已填充像素的模板, 置信度值较大, 在目标区域中形成转角和卷须的模板将被优先填充, 结构明显、包含线段突出的模板, 数据值较大, 像断线部分就可以优先顺利地连接; 另一方面, 数据值大的模板会使优先级倾向线段突出的部分, 而置信度值大的模板则会抑止那些线段的突出, 在这种情况下两者会取得一定的平衡。

### 1.2 寻找最匹配模板拷贝样本块

一旦优先级计算完毕, 则从源区域取样, 寻找和该模板已合成像素最匹配的模板, 并填充该模板。

### 1.3 更新置信值

随着模板内剩余像素的填充完毕, 重新更新该模板内像素的置信值:

$$C(q) = C(\hat{p}); \forall q \in \psi_p \cap \Omega$$

算法流程如图 3 所示。

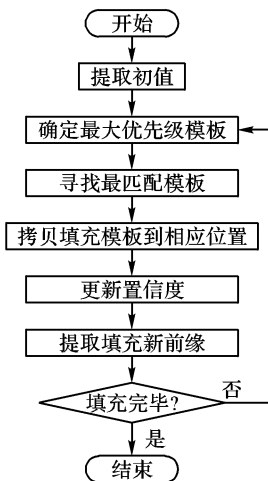


图 2 算法流程

## 2 遥感图像机密信息隐藏算法实现

一般来说这种基于样本图像修补方法用于遥感图像最大的不足应该是完成时间过长, 因为在寻找最佳匹配模板时, 通常都是对整幅图像进行扫描、计算, 对于一幅很大的遥感图像来说完成修补的时间无疑是很长的。考虑到遥感图像纹理之间相关性很强, 我们完全可以根据图像的实际情况在修补区附近限定一个比较小的区域进行最佳匹配模板的寻找, 这样就可以很大程度上缩短完成的时间。需要说明的是如果图像

是 RGB 模式, 可分别处理以后再合成, 本文处理的是灰度图像<sup>[6]</sup>。

主要步骤如下:

1) 在遥感图像中分割出机密图像块 (机密信息在遥感图像中的位置可以记下来)。

2) 在提取出机密图像块的空白区附近人工限制一区域, 最好取机密信息区位于限制区的中心位置, 可以根据图像本身特点决定, 要求限制区一定要完全包含机密信息区。

3) 计算模板优先级, 首先修补最大优先级模板。  $\psi_p$  取  $3 \times 3$  大小, 对于离散点, 模板  $\psi_p$  的面积  $|\psi_p|$  取像素的个数 9。设  $p$  点坐标  $(x, y)$ , 由于  $p$  点位于修补区的轮廓线上, 可能的情况是  $p$  点左右或者上下方向有某一点在修补区内, 本文在计算  $\nabla I_p^\perp$  时采取差分的方法:  $u(x, y)$  表示点  $(x, y)$  的像素值。

$$u_x = u(x+1, y) - u(x, y) \quad (\text{向前差分})$$

$$u_x = u(x, y) - u(x-1, y) \quad (\text{向后差分})$$

类似可计算  $u_y$  得到:

$$\nabla I_p = (u_x, u_y)$$

$$\nabla I_p^\perp = (-u_y, u_x)$$

对于  $\mathbf{n}_p$  的计算方法, 本文采用如下计算方法: 在修补区轮廓线上与  $p$  点相邻的两像素点确定一向量,  $\mathbf{n}_p$  即是与该向量垂直的向量。利用式 (1)、(2) 计算模板优先级。

4) 选取最佳匹配模板时只在限制区选择。把源区域同样分成  $3 \times 3$  大小并与最高优先级块进行比较。设目标块  $\psi_p$  具有最高优先级, 记  $\Phi_p$  是源区域中与  $\psi_p$  最相似的源块 (有意义的源块  $\Phi_p$  应该整块都包含在  $\Phi$  中) 则:

$$\Phi_{p'} = \arg \min_{\Phi_p} d(\Phi_p, \psi_p)$$

这里  $d(\Phi_p, \psi_p)$  定义为 2 个块中已经填充的像素的平方误差的和。

5) 将最佳匹配模板内的像素复制填充到模板  $\psi_p$  的相应位置上。

6) 更新模板  $\psi_p$  内新填充像素点的置信值。

7) 重复以上步骤直至轮廓线为空。

## 3 与数字水印结合的遥感图像机密信息隐藏

### 3.1 算法思想

在第 2 章提出了一种基于样本的图像修补方法用于遥感图像机密信息隐藏, 该方法直接去除了机密信息, 但是不同的用户权限是否可以看见机密信息的要求是不同的, 对于某些特殊用户是应该有权限<sup>[7-8]</sup>看到该机密信息的。本章利用数字水印技术对上述方法进一步改进, 使该方法可以实现该区分。

数字水印技术是将一些标志信息 (即数字水印) 直接嵌入数字载体 (包括多媒体、文档、软件等) 当中, 但不影响原载体的使用价值, 也不容易被人的知觉系统 (如视觉或听觉系统) 觉察或注意到。通过这些隐藏在载体中的信息, 可以达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。数字水印作为一种有效的保护数字产品版权的技术, 无论是理论研究还是实际应用都取得了很高的成就。数字水印系统包括的水印嵌入过程和水印提取 (检测) 过程正是本文所提到的区分用户权限的关键<sup>[9-10]</sup>。

### 3.2 算法实现

首先将遥感影像中的机密信息分割提取出来, 然后对空

白区域进行灰度补值,得到一幅不含机密信息的伪遥感图像。最后把分割出来的机密信息作为水印嵌入到伪遥感图像中,用户可以利用密钥提取机密信息并恢复出原始遥感图像。算法框架如图 3 所示。

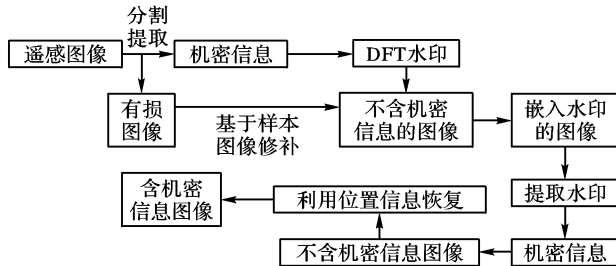


图3 遥感图像机密信息隐藏及恢复框架

机密信息分割提取出来的过程要保存分割图像在原始图像中的位置信息,再利用离散傅里叶变换(Discrete Fourier Transform, DFT)水印技术嵌入到修复后的遥感图像中。提取水印即机密信息后,利用已知的位置信息恢复出含有机密信息的遥感图像。该方法的主要步骤是图像修复和水印算法的选择<sup>[11-12]</sup>。

嵌入水印隐藏机密信息步骤如下:

1) 对含有机密信息的遥感图像预处理,可采取人工分割提取的方法,把机密信息提取出来另存为水印图像,记为  $W = \{w(i, j), 0 \leq i < P, 0 \leq j < Q\}$ ,并记录下其在原始图像的位置及大小;

2) 采用第二章基于样本的图像修补技术对有损的遥感图像修复,记为:  $I = \{g(i, j), 0 \leq i < M, 0 \leq j < N\}$ ;

3) 把  $w$  作为水印嵌入到修复好的遥感图像中。

恢复含有机密信息的步骤如下:

1) 提取水印过程按照嵌入的逆过程进行,得到机密信息图像,记为:  $W' = \{w'(i, j), 0 \leq i < P, 0 \leq j < Q\}$ ;

2) 将机密信息图像  $W'$  结合位置信息置回原位置即可恢复成含有机密信息的遥感图像。

从以上算法可知,可以根据用户的权限来提供密钥,以确定用户是否可以查看到遥感图像的机密信息。

#### 4 仿真实验与结果分析

把实现这一过程的实验结果进行比较,结果如图 4、5 所示。图 4 中,(a)为含有机密信息的原始遥感图像,其中阴影部分为机密信息;(b)为分割提取机密信息后的图像;(c)为提取出的机密信息;(d)为修复后的不含机密信息的遥感图像。图 5 中,(a)为嵌入水印的不含机密信息的遥感图像;(b)为提取出的机密信息水印;(c)为恢复了含机密信息的遥感图像。

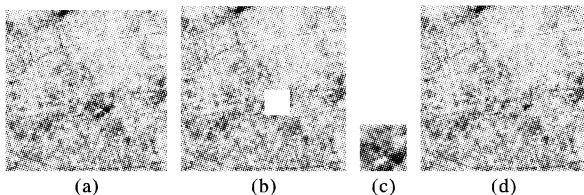


图4 分割提取机密信息,修复后图像

可以从直观上看到该方法对隐藏、提取、恢复机密信息的效果十分理想。表 1 为各个过程中遥感图像自身统计特征信息<sup>[13]</sup>的对比情况。从表 1 中可以看出遥感图像很好地保持了自身的统计特性。

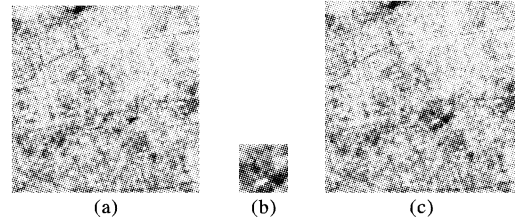


图5 提取机密信息,恢复图像

表 1 各阶段遥感图像自身统计信息表

图像	像元最小 灰度值	像元最大 灰度值	像元平均 灰度值	像元中位 灰度值	像元标 准方差
原始图像	0	254	173.499	180	42.785
修复后图像	0	254	174.443	182	41.709
嵌入水印图像	0	254	174.388	181	41.714
恢复后图像	0	254	173.444	180	42.788

图 6 是各阶段遥感图像直方图对比,(a)是原始图像的直方图,(b)是提取出机密信息修复后图像的直方图,(c)是嵌入水印后图像的直方图,(d)是恢复为含有机密信息图像的直方图。

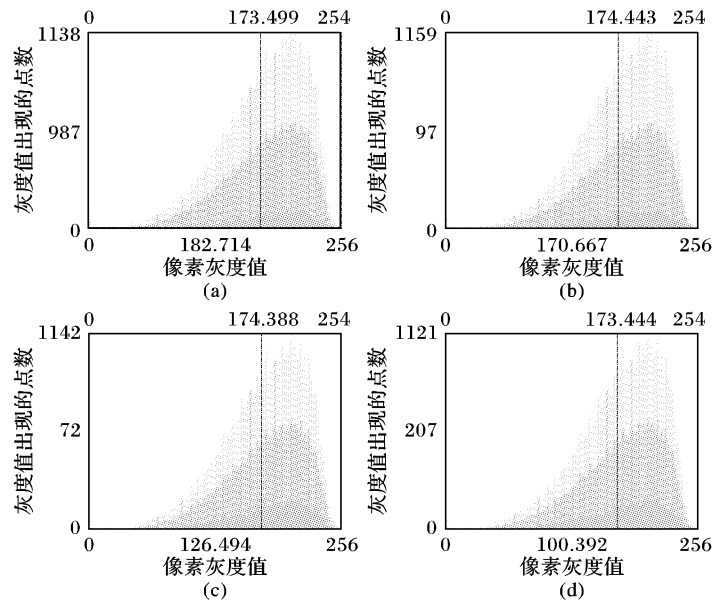


图6 各阶段遥感图像直方图

由表 1 和图 6 中统计信息可知,嵌入前后的遥感图像的自身统计特性没有发生很大的改变,直方图的分布特性也得到了较好的保持。

#### 5 结语

本文提出了一种基于数字水印与基于样本图像修补技术相结合的方法用于遥感图像的机密信息隐藏。仿真实验结果表明了该方法嵌入的水印具有良好的不可见性,实现简单,可以根据不同用户权限提供密钥以决定用户是否可以查看到机密信息,且基本不会影响到遥感图像的使用价值,说明了该方法的可行性,有效性。

(下转第 2982 页)

6) 最后  $CH_j$  通过  $k_1$  和  $k_2$  的异或运算得到  $K_{S_i-CH_j}$ , 即:

$$K_{S_i-CH_j} = k_1 \oplus k_2$$

至此, 簇首  $CH_j$  与其簇内的普通节点  $S_i$  之间建立了对称密钥, 即  $K_{CH_j-S_i}$ 。

当这一阶段完成后, 每一个簇首都与其簇内的普通节点建立了安全的通信密钥。其中一部分的簇首之间也建立了相互之间的通信密钥。由于模型中假设簇首的无线电射程足够远, 能够与基站进行直接的通信, 因此, 簇首之间两两预先全部建立密钥没有必要。完全可以在需要的时候再建立, 这是基于簇首的计算能力很强以及能量充足的假设。

### 3 网络性能评价

#### 3.1 安全性分析

本方案中, 普通节点之间没有通信, 每个普通节点都只保存一个对称密钥, 提高了网络在遭受敌方节点俘获攻击后的自我恢复能力。在网络初始化阶段, 每个簇首节点都只保存了两个一元多项式, 簇首对于其簇内的普通节点的密钥信息毫不知情。即使所有簇首的信息都泄露, 普通节点中的预分配密钥信息也不会泄露。方案中没有组密钥<sup>[6]</sup>, 簇首之间传递交换信息时, 要预先建立好对称密钥, 再进行通信。任何一个簇首被敌方俘获, 都不会影响到其他未被俘获的簇首之间的安全通信。

至于前面提及的  $t$  阶二元对称多项式存在的  $t$  门限性质<sup>[3]</sup>, 由于本文方案中假设簇首有相当充足的能量和很大的内存容量, 所以可以选择一个足够高阶的二元对称多项式用以产生簇首间的通信密钥。假如多项式的阶  $t$  大于网络中簇首的个数  $m$ <sup>[3]</sup>, 那么即使敌方俘获了所有的簇首节点, 也不能破解出这个多项式的系数, 从而确保了网络的通信安全。

#### 3.2 网络表现评价

1) 扩展性能: 由于无论网络的规模有多大, 普通节点都只存储一个密钥, 因此网络规模的大小只取决于簇首节点的个数。由于方案中假设簇首具有相当大的内存, 足够的能量和较强的数据处理能力, 因此, 从理论上讲, 只要选取合适的二元对称多项式和成簇算法, 那么本方案就适用于任何大规模的无线传感器网络<sup>[3]</sup>。从而, 本方案具有较佳的网络扩展性。

2) 存储开销: 无论网络规模有多大, 普通节点都只需要存储一个密钥, 极大地节省了内存空间。而基站和簇首的存储能力都很强, 所以它们的存储开销可以忽略不计。

3) 通信开销: 对于一般密钥预分配方案来说, 由于每个传感器节点都需要和它的邻居节点交换密钥信息, 所以通信

开销较大。而本方案中, 每个普通节点仅预先存储一个对称密钥, 无须与其他普通节点交换信息建立密钥。当有新的普通节点加入网络时, 无须额外重新分配密钥, 只要在部署前按照前面的方法分配一个密钥, 然后再根据某种规则加入到一个簇即可。基站也无须与所有簇首重新交换密钥信息<sup>[3]</sup>。所有这些都大大降低了节点间的通信开销, 延长了网络的生存周期。

### 4 结语

由于无线传感器网络及其节点所独有的特性使得其要达到较高的安全性能变得相当困难, 而且还需要面对来自多方面的攻击。因此, 为了实现传感器节点间的安全通信, 通常需要在节点部署之前, 进行密钥的预分配。二元  $t$  次多项式密钥预分配协议<sup>[6]</sup>便是在已有的密钥预分配协议上发展起来的, 针对无线传感器网络节点的存储空间、能量和计算能力有限的特性, 减少了节点间的通信开销<sup>[3]</sup>。

与其他已有的预分配密钥方案<sup>[7]</sup>和基于簇的无线传感器网络密钥管理协议<sup>[8]</sup>相比, 可以使网络在遭受节点俘获攻击后有更强的自我恢复能力, 从而具有良好的抗毁性, 能有效抵御节点的合谋攻击。通信开销也比随机密钥预分配等方案要低。而普通节点只存储一个密钥, 极大地节省了存储空间, 更加适用于大规模的无线传感器网络。当然, 本文只是在理论上对改进后的方案做了评估, 下一步的工作将是进行仿真, 从实验上验证理论的可行性。

#### 参考文献:

- [1] 黄鑫阳, 扬明. 无线传感器网络密钥管理研究综述[J]. 计算机应用研究, 2007, 24(1): 10-15.
- [2] 刘良, 邓亚平, 李钦. 一种基于 ID 的传感器网络密钥管理方案[J]. 计算机应用, 2006, 26(10): 2347-2350.
- [3] CHENG YI, AGRAWAL D P. An improved key distribution mechanism for large-scale hierarchical wireless sensor networks [J]. Ad Hoc Networks, 2007, 16(5): 35-48.
- [4] ZHANG WEN-SHENG, TRAN M, ZHU SEN-CUN. A random perturbation-based scheme for pairwise key establishment in sensor networks [J]. MobiHoc, 2007, 32(8): 90-99.
- [5] 李军, 李录明. 多项式密钥预分配协议在传感器网络上的实现[J]. 计算机工程, 2007, 33(15): 149-151.
- [6] 周贤伟, 孙晓辉, 覃伯平. 无线传感器网络密钥管理方案的研究[J]. 计算机应用研究, 2007, 24(1): 144-147.
- [7] 赵治平, 林亚平. 传感器网络中基于簇的组密钥管理方案[J]. 计算机工程, 2008, 34(5): 153-157.
- [8] 魏楚元, 郝莹, 吕橙. 基于簇的无线传感器网络密钥管理协议[J]. 计算机工程与设计, 2007, 28(20): 4901-4904.
- [7] 王贤敏, 关泽群, 吴沉寒. 遥感影像高逼真度二维信息隐藏盲算法[J]. 计算机工程与应用, 2004, 40(13): 3-5.
- [8] 王贤敏, 王乘, 周建中等. 一种新的遥感影像不同权限信息隐藏技术[J]. 计算机工程, 2006, 32(1): 28-30.
- [9] 胡英, 陈辉, 房世波. 数字水印技术在遥感图像版权保护中应用[J]. 计算机仿真, 2005, 22(3): 200-202.
- [10] 陈辉. 数字水印技术及其在遥感图像中的应用研究[D]. 成都: 成都理工大学, 2005.
- [11] 曹荣, 王颖, 李象霖. 一种自适应的 DFT 域数字水印算法[J]. 计算机工程与应用, 2006, 42(10): 77-78.
- [12] 王向阳, 杨红颖, 邵俊. 基于内容的离散余弦变换域自适应遥感图像数字水印算法[J]. 测绘学报, 2005, 34(4): 324-330.
- [13] 党安荣, 王晓栋, 陈晓峰, 等. ERDAS imagine 遥感图像处理方法[M]. 北京: 清华大学出版社, 2003.

(上接第 2979 页)

#### 参考文献:

- [1] 周成虎, 骆剑承, 刘庆生, 等. 遥感影像地学理解与分析[M]. 北京: 科学出版社, 1999.
- [2] 张红英. 数字图像修复技术的研究与应用[D]. 成都: 电子科技大学, 2006.
- [3] CRIMINISI A, PEREZ P, TOYAMA K. Region filling and object removal by exemplar-based image inpainting [J]. IEEE Transactions on Image Processing, 2004, 13(9): 1200-1212.
- [4] 彭宏京, 侯文秀, 官宁生. 改进的基于样例修补的目标移除方法[J]. 计算机辅助设计与图形学学报, 2006, 18(9): 1345-1349.
- [5] 戴磊, 魏宝刚. 图像复原的算法研究[J]. 计算机工程与设计, 2006, 27(2): 184-187.
- [6] 袁金国. 遥感图像数字处理[M]. 北京: 中国环境科学出版社, 2006.