

基于自适应格网划分的遥感影像感知哈希认证算法

丁凯孟¹ 朱长青¹ 卢付强¹

¹ 南京师范大学虚拟地理环境教育部重点实验室,江苏 南京,210023

摘 要:针对遥感影像大数据量和信息分布不均匀的特点,提出了一种基于自适应格网划分的遥感影像感知哈希算法,并将其用于遥感影像的完整性认证。该算法基于自适应策略对信息丰富的影像区域进行粒度更细的完整性认证,首先对原始影像进行波段融合,然后根据信息熵对波段融合结果进行自适应的格网划分,最后提取格网单元的局部特征构造感知哈希序列。影像接收端通过收到的感知哈希序列实现影像的认证。实验表明,本文算法能够识别遥感影像局部细节篡改,并对保持内容不变的操作具有鲁棒性,实现了遥感影像基于内容的完整性认证。

关键词:感知哈希;自适应格网划分;完整性认证;遥感影像

中图分类号:P208; P237.9 **文献标志码:**A

遥感影像数据是重要的地理信息资源,在众多领域得到重要的应用。但遥感影像在传输、存储与使用过程中容易遭受各种无意或有意的篡改攻击。遥感影像本身具有高精度、安全性等特性,如果完整性、真实性受到影响,其使用价值将大打折扣,甚至不再具有实用价值。因此,遥感影像的认证问题变得愈发重要。

传统的密码学 Hash 函数能够一定程度上满足遥感影像的认证需求,但仍存在不足。Hash 函数(如 SHA1 和 MD5)对数据的变化过于敏感,即使一个比特发生改动,也会产生截然不同的哈希序列(即雪崩效应)。但是,遥感影像在使用与传输过程中进行格式转换、水印嵌入等操作之后,承载的内容信息并没有改变,改变的只是内容信息的载体。这种情况下,Hash 函数不能很好地对影像数据进行认证。感知哈希(perceptual hashing)为遥感影像的认证提供了一种可行的解决方法。感知哈希与 Hash 函数有着显著的区别,图像经过格式转换或水印嵌入等不改变内容的操作,感知哈希序列不发生变化或变化很小。本文结合遥感影像的数据特征,研究了基于感知哈希的遥感影像认证算法。

1 算法原理与流程描述

感知哈希是多媒体数据集到感知摘要集的一

类单向映射,将具有相同感知内容的多媒体数字表示唯一地映射为一段数字摘要,并满足感知鲁棒性和安全性^[1]。根据多媒体对象的不同,感知哈希包括图像感知哈希、音频感知哈希、视频感知哈希等。感知哈希具有鲁棒性、唯一性、安全性等特征^[2]。已经有许多学者展开了图像感知哈希的研究,但是,针对遥感影像的相关研究并不多见。

遥感影像与普通图像的表现形式相同,但作为重要的地理空间数据,遥感影像对量测精度有较高的要求,因此,遥感影像的认证算法必须能够检测出影像的局部细微篡改。而且相对于普通图像,遥感影像普遍具有数据海量性的特点。感知哈希本质上是用尽可能少的比特表示图像整体信息^[3],如果将现有的图像感知哈希算法直接应用于遥感影像的认证,长度有限的感知哈希序列将无法有效地感知大数据量遥感影像的局部细微变化,不能满足遥感影像对精度的要求。此外,遥感影像往往不存在单一或者明确的主题^[4],因此其承载的内容信息往往不是均匀分布的,不同区域的信息量可能差别较大。而人类视觉系统对不同区域的敏感性也不相同,对信息较少的平滑区域更为敏感,而对信息丰富的纹理区域往往不够敏感^[5]。因此,遥感影像信息丰富的区域需要进行更为严格的认证,以利于遥感影像的有效利用。

本文针对遥感影像大数据量和信息分布不均

收稿日期:2013-10-12

项目来源:国家自然科学基金资助项目(41301413);国家社科基金重大资助项目(11&·ZD162)。

第一作者:丁凯孟,博士生,主要从事地理数据安全研究。E-mail: dingkaimeng@foxmail.com

匀等特点,结合信息熵与格网划分理论,提出了一种基于自适应格网划分的遥感影像感知哈希认证算法,对信息丰富的影像纹理区域实施强度更高的完整性认证。在地理学中,格网是将连续的工作区域的平面空间离散化^[6]。本文采用格网将影像划分为不同的区域,然后提取影像不同区域的局部特征。由于感知哈希算法大多针对图像全局进行特征提取,因此,为了区分基于局部区域特征的感知哈希,以便于算法流程描述,本文将遥感影像局部区域的内容特征映射为数字摘要的过程称

为单元感知哈希(unit perceptual hashing, UPH),简称单元哈希。单元感知哈希生成的结果称为单元感知哈希序列,或单元哈希序列。

本文算法总体由遥感影像的发送端和接收端两部分组成,如图1所示。影像发送端对遥感影像进行波段融合(单波段影像不进行这一步骤的操作);然后对融合影像进行基于信息熵的自适应格网划分,提取每个格网单元的内容特征生成单元感知哈希。接收端认证遥感影像的内容完整性,并对认证结果进行描述。

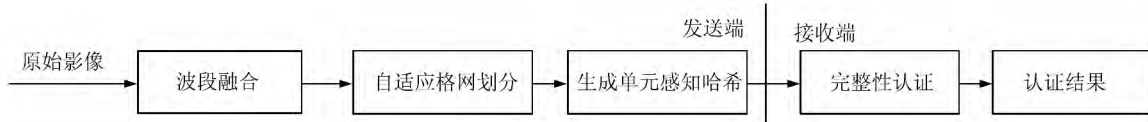


图1 本文算法流程图

Fig. 1 Flow Chart of Proposed Algorithm

1.1 原始影像的波段融合

本文算法顾及遥感影像多波段的特性,采用加权融合法对多波段影像进行波段融合。设原始影像和融合后的影像分别表示为 I 和 F , 则

$$F(i, j) = \sum_{k=1}^N \alpha_k I^k(i, j) \quad (1)$$

式中, I^k 表示原始影像的不同波段; N 表示波段数; $I^k(i, j)$ 和 $F(i, j)$ 分别表示波段 I^k 和融合影像 F 坐标 (i, j) 的像素值; α_k 表示像素加权的权值 ($\sum_{k=1}^N \alpha_k = 1$)。这里, α_k 的取值应根据实际影像的波段内容的相关性而定。本文实验中,实验对象为三波段的真彩影像,为了使融合结果更符合人眼的视觉特点,加权系数分别取 0.30、0.59、0.11。对于单波段影像,则不需要进行波段融合操作。

1.2 基于信息熵的自适应格网划分

对融合影像 F (或未经过波段融合操作的单波段影像 I), 进行基于信息熵的自适应格网划分。先对融合影像 F 进行隐形格网划分,将其分割为大小相等的区域;然后基于局部自适应策略,根据信息熵自适应地对格网单元进行格网加密操作(不同于密码学中的加密)。

信息熵^[7]是信息不确定性的度量,能够反映影像不同区域信息的丰富程度。对于格网单元 Q_{ij} (255 阶的灰度图), 其信息熵为:

$$E(Q_{ij}) = - \sum_{n=0}^{255} p_n \ln p_n \quad (2)$$

其中, p_n 表示格网单元 Q_{ij} 中灰度值为 n 的像素出现的概率。

设定信息熵的两个阈值 T_1 与 T_2 ($T_2 > T_1$), 融合影像自适应格网划分的具体步骤如下。

1) 对 F 进行 $W \times H$ (W 与 H 为正整数) 的格网划分, 每个格网单元记为 Q_{ij} , 其中 i, j 表示格网坐标。

2) 根据格网单元的信息熵进行自适应格网加密。如果格网单元的信息熵 $E(Q_{ij})$ 大于阈值 T_2 , 该格网进一步进行 $w_1 \times h_1$ 的格网划分; 如果格网单元的信息熵 $E(Q_{ij})$ 大于阈值 T_1 且小于阈值 T_2 , 该格网进一步进行 $w_2 \times h_2$ ($w_1 > w_2, h_1 > h_2$) 的格网划分。加密之后的格网记为 Q_{ij}^p , p, q 表示加密后的二级坐标。

3) 如果格网单元的信息熵 $E(Q_{ij})$ 小于 T_1 , 说明该区域为平坦区域, 不进行格网加密。

格网划分的粒度将直接影响算法的性能, 若格网划分的过细、格网单元过小, 将会消耗更多的存储空间、计算时间以及网络带宽; 若格网单元过大, 可能无法感知遥感影像局部细微的篡改。分析算法流程可以得出: 原始影像进行 $W \times H$ 的格网划分之后, 格网单元 Q_{ij} 应大于 256 像素 \times 256 像素, 且小于 512 像素 \times 512 像素; 格网加密过程中, 最小的格网单元不宜小于 64 像素 \times 64 像素。本文实验中, 设定 $w_1 = h_1 = 4, w_2 = h_2 = 2$ 。

自适应的格网划分过程中, 阈值 T_1 与 T_2 的选择应尽可能地反映格网信息熵的分布情况。本文采用窗口扫描法来选取其中一个阈值, 即选取信息熵分布最密集的区间的中心作为信息熵的一个阈值(另一个阈值取格网信息熵的平均值)。具体过程如下。

1) 将所有格网单元的信息熵映射到一维数

轴上。

2) 以每个信息熵作为窗口中心,通过固定大小的窗口扫描数轴上的信息熵。这里的窗口指的是以信息熵为中心的区间,窗口大小就是区间的长度。

3) 统计落入每个窗口内信息熵的个数。

4) 信息熵个数最多的窗口就是信息熵分布最密集的区间,该窗口的中心就是信息熵的一个阈值。如果出现信息熵个数相同的窗口,那么阈值取多个窗口中心的平均值。

这一过程的关键在于窗口大小的选择。通过实验,本文选择窗口大小为 0.1,也就是扫描数轴过程中以信息熵为中心的区间长度为 0.1。实验过程中发现,窗口扫描得到的最大两个峰值往往十分相近,所以本文选择格网信息熵的平均值作为另一个阈值。

1.3 单元感知哈希序列生成

计算每个格网单元的单元感知哈希。感知哈希算法主要包括基于图像统计特征的方法^[8]、基于 DCT 变换的方法^[2,9,10]、基于 DWT 变换的方法^[11]和基于特征点的方法^[12]等。其中,DCT 变换是最为常用的特征提取方式,能够很好地满足鲁棒性、摘要性、唯一性等要求^[10]。图像经过 DCT 变换之后,部分较大的交流系数(即 AC(alternating current)系数)保持着大量的能量和纹理信息,可以很好地反映图像的内容特征。本文采用 DCT 变换的方法生成单元感知哈希,具体步骤(见图 2)如下。

1) 预处理,通过重采样处理将分辨率统一为 $m \times m$ (实验中 $m=32$)。

2) 将 $m \times m$ 的灰度图分成 $n \times n$ (实验中 $n=8$) 的小块,每个小块进行 DCT 变换(离散余弦变换),并选取变换后的一个直流系数(即 DC(direct-current)系数)和 7 个低频 AC 系数作为内容特征。

3) 量化提取的系数为二值序列。AC 系数的量化规则为:系数为正,置为 1;系数为负,置为 0。DC 系数的量化规则为:大于各分块 DC 系数的均值,置为 1,否则置为 0。

4) 量化后的二值序列采用加密算法(基于密钥长度灵活性的考虑,本文实验中选择 RC4 算法)进行加密,得到的序列就是该格网的单元感知哈希,记为 UPH_{ij}^{pq} ,其中, i, j, p, q 均表示格网单元的坐标(对于未进行加密的平滑区域,仅通过 i 与 j 进行标识)。分析可知,单元感知哈希的长度 L 取决于预处理的大小、分块大小以及选取的

DCT 系数的个数。

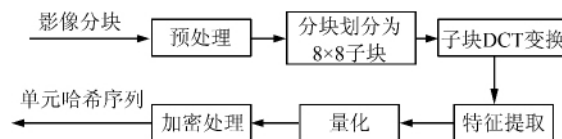


图 2 单元感知哈希生成流程图

Fig. 2 Unit Perceptual Hash Generation

1.4 认证过程

遥感影像接收端对影像进行完整性验证。待认证影像采用相同的过程生成格网的单元感知哈希,记为 UPH'_{ij}^{pq} ,并将发送端发送的单元感知哈希记为 UPH_{ij}^{pq} ,然后通过比较 UPH_{ij}^{pq} 与 UPH'_{ij}^{pq} 之间的差异来验证相应格网的内容完整性。由于本文算法未限定单元感知哈希的长度,因此采用更为直观的归一化 Hamming 距离来衡量单元感知哈希之间的差异。对于两个长度相等的单元感知哈希 h_1 和 h_2 (二值序列表示),归一化 Hamming 距离如式(2)所示:

$$\text{Distance} = \left(\sum_{i=1}^L |h_1(i) - h_2(i)| \right) / L \quad (3)$$

其中, L 是 h_1 和 h_2 的序列长度。两个单元感知哈希的归一化 Hamming 距离实际上是 0~1 之间的浮点数。如果归一化 Hamming 距离低于设置的阈值 T_h ,说明相应的区域内容没有发生明显变化;反之,说明相应的区域内容发生较大变化,也就是遭到了某种篡改。

2 实验过程与分析

2.1 实验过程

本文选取如图 3 所示的两幅三波段 Tiff 格式遥感影像进行测试与分析,大小分别为 3 000 像素 \times 3 000 像素、4 000 像素 \times 4 000 像素。实验硬件平台为 3.1 GHz 主频的 CPU,可用内存 2 G;软件开发平台为 Visual Studio 2010 和 C++,并基于 GDAL 库函数实现遥感影像的读取。



(a) 原始遥感影像 A

(b) 原始遥感影像 B

图 3 实验影像

Fig. 3 Experimental Images

实验影像首先通过加权融合法进行波段融合(加权系数分别为 0.30、0.59、0.11),然后对融合结果进行自适应的格网划分。融合影像分别进行 10×10 的初步格网划分后,采用窗口扫描法和均值法确定格网加密的两个信息熵阈值:影像 A 的两个阈值分别为 3.89 和 5.15,影像 B 的两个阈值分别为 4.74 和 4.84。自适应格网划分的结果如图 4 所示。通过 DCT 变换提取格网特征,并生成相应的单元感知哈希。

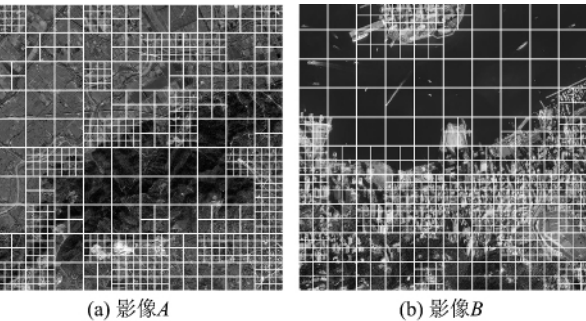


图 4 自适应格网划分结果
Fig. 4 Adaptive Grid Partition

影像接收端重新计算每个格网单元的单元感知哈希,并与收到的相应单元感知哈希进行对比。本文通过实验设定归一化 Hamming 距离阈值 T_h 为 0.02。

2.2 测试与分析

1) 篡改敏感性与鲁棒性测试

认证过程必须能够检测出影像局部的恶意篡改。以遥感影像 A 格网 $BLOCK_{6,8}^{2,1}$ 为例进行测试,如图 5(a)所示。图 5(b)~ 5(d)所示为该格网单元的篡改示例,分别是增加地物、减少地物、变换地物等篡改操作。格网单元篡改之后,与原始的单元感知哈希之间的归一化 Hamming 距离篡改示例 1、示例 2、示例 3 分别为 0.075 125、0.031 250、0.093 750,均高于设定的阈值。这就说明本文算法能够识别出遥感影像的局部内容篡改。



图 5 篡改检测测试
Fig. 5 Tampering Test

对不改变内容的操作保持鲁棒性是感知哈希与 Hash 函数最显著的区别。下面以格式转换、JPEG 压缩和水印嵌入为例进行鲁棒性测试,其中,水印嵌入以最低有效位(least significant bit,

LSB)算法为例。这里采用归一化 Hamming 距离低于阈值的格网比例来描述算法的鲁棒性,结果见表 1。由表 1 可知,该算法能对格式转换和水印嵌入操作保持很好的鲁棒性,对 JPEG 压缩也具有较好的鲁棒性。

表 1 鲁棒性测试/%
Tab. 1 Robustness Test/%

	影像 A	影像 B
格式转为 BMP	100	100
LSB 水印嵌入	100	100
JPEG 压缩	95	100

算法的鲁棒性可以通过归一化 Hamming 距离的阈值 T_h 进行调节, T_h 越大,算法的鲁棒性越强。但是,鲁棒性与篡改敏感性之间是矛盾的关系,过分强调鲁棒性,就可能无法检测影像的局部细微篡改。

2) 多尺度的局部细节篡改检测

为了验证算法自适应格网划分的有效性,下面进行多尺度的局部细节篡改检测,也就是遥感影像经过局部的细微篡改之后,分别在不同尺度下提取特征,并生成单元感知哈希,以检测篡改。图 6(b)与 6(d)是经过相同篡改之后不同大小的影像格网单元,表 2 所示为检测结果对比。



图 6 局部篡改测试
Fig. 6 Local Tampering Test

表 2 不同尺度的篡改检测对比
Tab. 2 Tampering Detection Under Different Scales

	归一化 Hamming 距离
原始遥感影像	0
300×300 格网单元	0.031 250
150×150 格网单元	0.109 375

从表 2 可见,从原始影像全局提取特征构造的感知哈希序列没能识别出这一局部细节篡改;大小为 300×300 的格网单元感知哈希能够识别

篡改,但归一化 Hamming 距离偏小,如果篡改更微小,就很有可能检测不到;大小为 150×150 的格网单元感知哈希则很容易地识别出篡改。也就是说,不同尺度下构造的感知哈希序列的篡改识别能力也不相同。这就说明,本文算法通过自适应的格网划分能够有效感知遥感影像细节的篡改,而且对信息丰富的区域进行细粒更细的认证,克服了常规图像感知哈希不能有效检测海量遥感影像局部细节篡改的不足。

3 结 语

本文以遥感影像的认证为目的,针对遥感影像具有大数据量和信息分布不均匀的特点,提出一种基于自适应格网划分的遥感影像感知哈希认证算法。该算法基于自适应策略,对影像进行波段融合后,根据遥感影像不同区域的信息熵对影像进行自适应格网划分,然后提取格网单元的内容特征构造单元感知哈希序列。本文算法克服了常规图像感知哈希算法不能有效感知遥感影像局部细节篡改的缺陷,能够对信息丰富的纹理区域进行更为严格的完整性认证。实验表明,该算法能够识别遥感影像的局部细节篡改,对保持内容不变的操作具有鲁棒性,实现了遥感影像基于内容的完整性认证。

但是,本文算法在鲁棒性方面有待进一步研究。结合迁移学习、影像空间语义计算等方面的工作,研究更为鲁棒、有效的影像特征提取方法是下一步研究的重点。

参 考 文 献

- [1] Niu Xiamu, Jiao Yuhua. An Overview of Perceptual Hashing[J]. *Acta Electronica Sinica*, 2008, 36(7): 1 405-1 411(牛夏牧, 焦玉华. 感知哈希综述[J]. *电子学报*, 2008, 36(7): 1 405-1 411)
- [2] Zhang Weike, Kong Xiangwei, You Xingang. Secure and Robust Image Perceptual Hashing[J]. *Journal of Southeast University (Natural Science Edition)*, 2007, 37(1): 188-192(张维克, 孔祥维, 尤新刚. 安全鲁棒的图像感知哈希技术[J]. *东南大学学报(自然科学版)*, 2007, 37(1): 188-192)
- [3] Sun Rui, Yan Xiaoxing, Ding Zhizhong, et al. Perceptual Hashing Method Use for Image Authentication[J]. *Journal of System Simulation*, 2010, 22(2): 483-486(孙锐, 闫晓星, 丁志中, 等. 一种用于图像认证的感知哈希方法[J]. *系统仿真学报*, 2010, 22(2): 483-486)
- [4] Cheng Qimin. Remote Sensing Image Retrieval Technologies [M]. Wuhan: Wuhan University Press Co., Ltd., 2011(程启敏. 遥感图像检索技术[M]. 武汉: 武汉大学出版社, 2011)
- [5] Wang Zhiwei, Zhu Changqing, Wang Qisheng, et al. An Adaptive Watermarking Algorithm for Raster Map Based on HVS and DFT[J]. *Geomatics and Information Science of Wuhan University*, 2011, 36(3): 351-354(王志伟, 朱长青, 王奇胜, 等. 一种基于 HVS 和 DFT 的栅格地图自适应数字水印算法[J]. *武汉大学学报·信息科学版*, 2011, 36(3): 351-354)
- [6] Li Qi, Luo Zhiqing, Hao Li, et al. Research on Urban Grid System and Geocodes[J]. *Geomatics and Information Science of Wuhan University*, 2005, 30(5): 408-411(李琦, 罗志清, 郝力, 等. 基于不规则网格的城市管理网格体系与地理编码[J]. *武汉大学学报·信息科学版*, 2005, 30(5): 408-411)
- [7] Han Peng, Gong Jianya, Li Zhilin, et al. A New Approach for Choice of Optimal Spatial Scale in Image Classification Based on Entropy[J]. *Geomatics and Information Science of Wuhan University*, 2008, 33(7): 676-679(韩鹏, 龚健雅, 李志林, 等. 基于信息熵的遥感分类最优空间尺度选择方法[J]. *武汉大学学报·信息科学版*, 2008, 33(7): 676-679)
- [8] Kailasanathan C, Naini R S. Image Authentication Surviving Acceptable Modifications Using Statistical Measures and K-mean Segmentation [C]. *IEEE-EURASIP Workshop Nonlinear Signal and Image*, Baltimore, Maryland, USA, 2001
- [9] Lu C S, Liao H Y M. Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme[J]. *IEEE Transactions on Multimedia*, 2003, 5(2): 161-173
- [10] Chang L, Yan W G, Wang W D. Research on Robust Image Perceptual Hashing Technology Based on Discrete Cosine Transform[C]//Business, Economics, Financial Sciences, and Management. Berlin, Heidelberg ;Springer, 2012: 799-809
- [11] Swaminathan A, Mao Y, Wu M. Robust and Secure Image Hashing[J]. *IEEE Transactions on Information Forensics and Security*, 2006, 1(2): 215-230
- [12] Liu Zhaoqing, Li Qiong, Liu Jingrui, et al. SIFT Based Image Hashing Algorithm[J]. *Chinese Journal of Scientific Instrument*, 2011, 32(9): 2 024-2 028(刘兆庆, 李琼, 刘景瑞, 等. 一种基于 SIFT 的图像哈希算法[J]. *仪器仪表学报*, 2011, 32(9): 2 024-2 028)

(下转第 743 页)

Geometric Correction for Images of Intersection Taken by Hovering UAV

WANG Jionghua¹ XU Tao¹ LI Xiang¹

¹ Key Laboratory of Geographical Information Science, Ministry of Education, East China Normal University, Shanghai 200241, China

Abstract: Low-altitude unmanned aerial vehicle (UAV) images have increasingly demonstrated unique advantages in the fields of transport planning, urban management, emergency monitoring. To understand the advantages of UAV images, rapid and accurate correction and registration of the image are a necessary premise. This paper takes a image of intersection taken by hovering UAV as its research target, and discusses the method of geometric correction and registration for such images. The image contains a large number of similar features and moving objects, which makes it difficult to be corrected in traditional way, based on spatial domain or frequency domain. Thus, this paper proposes an image registering method based on semantic information extracted from zebra lines. To realize images registration between arbitrary frames, the following steps are necessary: patterns extraction, zebra line patterns preparation and classification, axis fitting and image registration. Finally, a test is performed with a video taken by UAV. The results demonstrate that the method is robust and effective.

Key words: low-altitude UAV image; geometric correction; zebra lines; image registering

First author: WANG Jionghua, postgraduate, specializes in prediction information based emergency response fleets deployment. E-mail: 871718152@qq.com

Corresponding author: LI Xiang, PhD, professor. E-mail: xli@ecnu.edu.cn

Foundation support: The Doctoral Fund of Ministry of Education of China, No. 20130076110014; the National 863 Program of China, No. 2013AA122302; the National Natural Science Foundation of China, No. 41271441.

+++++

(上接第 720 页)

An Adaptive Grid Partition Based Perceptual Hash Algorithm for Remote Sensing Image Authentication

DING Kaimeng¹ ZHU Changqing¹ LU Fuqiang¹

¹ Key Laboratory of VGE, Ministry of Education, Nanjing Normal University, Nanjing 210023, China

Abstract: In the light of the big data characteristics of remote sensing images, a perceptual Hashing algorithm based on adaptive grid division for remote sensing image authentication is proposed. This method, based on adaptive strategy, can authenticate information intensive regions at a fine-grained level. First, the bands of the remote sensing image are fused. The fusion image is adaptively divided into grid units based on information entropy. Then the local features of each grid unit are extracted to generate perceptual Hash value. Authentication verifies the content integrity of the remote sensing image through the received Hash value. Experiments show that the algorithm can detect malicious tampering of remote sensing images, while tolerating legitimate content distortion, thus achieving content integrity authentication for remote sensing image.

Key words: perceptual Hashing; adaptive grid partition; integrity authentication; remote sensing image

First author: DING Kaimeng, PhD candidate, specializes in data security. E-mail: dingkaimeng@foxmail.com

Foundation support: The National Natural Science Foundation of China, No. 41301413; the National Social Science Fund, No. 11&ZD162.