

基于交比图像量测技术检测建筑物表面损伤面积的方法

崔文超, 李旭琛, 施云飞

(三峡大学计算机与信息学院, 湖北 宜昌 443002)

摘要: 文章提出了基于交比图像量测技术检测建筑物表面损伤面积的方法, 针对建筑物外表面损伤部分检测困难, 几何信息难以提取的问题, 文章将基于交比的单幅图像量测技术应用至含有丰富三维空间平行线的建筑物图像量测中。首先, 对图像进行畸变的矫正; 再利用建筑物结构中的垂直水平等几何关系, 找到消失点, 结合已知长度的参考线段以及消失点、消失线构建交比, 框选出待测区域, 多次嵌套后实现对框选区域边长的量测; 再通过数字图像处理技术, 对目标区域进行透视变换还原成矩形, 并实现二值化、形态学滤波等处理; 最后在计算出框选区域实际面积后, 统计出框选区域总像素点个数以及损伤区域像素点个数, 找到比例关系, 计算得到损伤区域面积。

关键词: 交比; 建筑损伤; 表面损伤测量; 图像量测; 面积计算

中图分类号: TP391

文献标识码: A

文章编号: 2096-9759(2023)06-0020-05

Method for Detecting Surface Damage Area of Buildings Based on Intersection Ratio Image Measurement Technology

CUI Wenchao, LI Xuchen, SHI Yunfei*

(China Three Gorges University, College of Computer and Information Technology, Yichang 443002)

Abstract: This paper proposes a method for detecting the surface damage area of buildings based on intersection ratio image measurement technology. In response to the difficulty of detecting surface damage on the exterior of buildings and the difficulty in extracting geometric information, this paper applies the intersection ratio-based single-image measurement technology to the measurement of building images with rich three-dimensional space parallel lines. First, the image is corrected for distortion. Then, using the vertical and horizontal geometric relationships in the building structure, the vanishing point is found. Combined with a known length reference segment and vanishing point, a vanishing line is constructed, and an intersection ratio is formed to select the test area. After multiple nesting, the edge length of the selected area is measured. Next, digital image processing technology is used to perform perspective transformation on the target area and restore it to a rectangle, and then binaryzation and morphological filtering are applied. Finally, after calculating the actual area of the selected area, the total number of pixels in the selected area and the number of pixels in the damaged area are counted, and the ratio relationship is found to calculate the damaged area.

Keyword: Intersection ratio; building damage; surface damage measurement; image measurement; area calculation

1 引言

随着我国经济和人民生活水平的提高, 建筑工程的数量不断增长, 为人们的日常生活和经济发展提供了很大的支持。然而, 随着时间的推移, 大量已建成的房屋将进入中老年期, 这也就意味着需要面对建筑物老化和损伤的问题。在过去的几十年里, 许多建筑物经历了各种天气条件和外部因素的影响, 例如高温、低温、降雨、风暴等, 这些因素不可避免地对建筑物造成了一定的损伤^[10-11]。

对于这些已经超出设计使用寿命的建筑物, 其外表面往往会出现裂缝、剥落等现象, 这不仅会影响建筑物的美观和品质, 也会增加安全隐患。因此, 及时发现和修复这些问题至关重要。同时, 建筑物损伤的修复也是一项复杂而繁琐的工作, 需要耗费大量的时间、人力和资金。对于一些严重损坏的建筑物, 甚至需要进行拆除和重建, 这就给社会带来了不小的负担。

综上所述, 建筑物损伤是一个不容忽视的问题, 对于社会和人民的安全和福利都有着深远的影响。通过应用先进的检

测技术, 及时发现和修复建筑物损伤, 不仅可以提高建筑物的安全性和品质, 也可以节约维修成本和减少不必要的浪费, 有助于推动城市和社会的可持续发展。

为了应对这些问题, 目前已经出现了一些先进的建筑物损伤检测技术。例如, 三维扫描技术可以对建筑物进行全面的测量和分析, 从而快速准确地发现损伤和缺陷^[9]。热红外像技术可以通过检测建筑物表面的温度差异来发现隐蔽的损伤和缺陷。超声波检测技术则可以探测建筑物内部的缺陷和损伤。这些技术的出现, 为建筑物的保护和维修提供了更多的手段和可能性。

其中, 三维激光扫描技术因成本问题, 工程上的应用并未普及。利用 kinect 传感器, 通过对点云的预处理, 在 GIS (Geographic Information System, 地理信息系统) 环境下实现对不规则损伤几何特征属性量化提取的技术, 由于 kinect 设备本身视场较小, 而不能应用于大规模或者较远距离的损伤区域检测。

热红外像技术虽能对较大区域的损伤部位进行快速扫描, 但其只能对损伤区域出现的位置做出判断, 并不能量化提取其几何属性。

收稿日期: 2023-04-05

基金项目: 国家自然科学基金资助项目 (Nos. 61871258)

作者简介: 崔文超 (1979-), 男, 副教授, 博士, 主要研究方向: 医学信号和图像处理; 李旭琛 (1996-), 男, 硕士, 研究生, 主要研究方向: 计算机视觉, 三维重建; 施云飞 (1993-), 男, 硕士, 研究生, 主要研究方向: 计算机视觉, 三维重建。

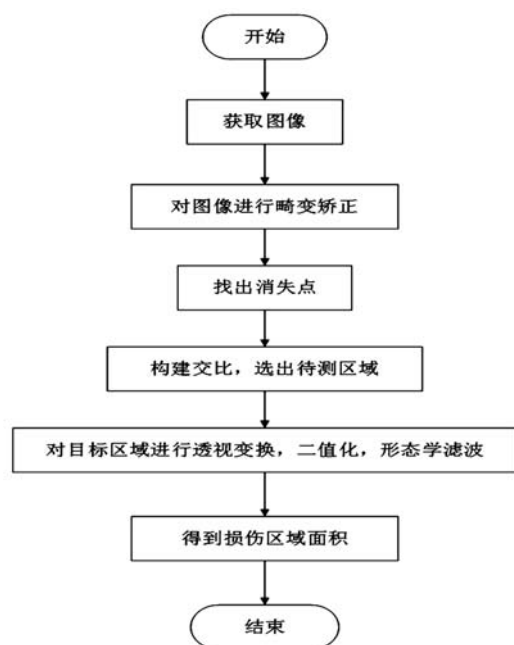


图1 本文方法的总体流程图

超声波检测技术侧重于对混凝土表面损伤层厚度的检测,且需将超声波发射和接收的换能器置于混凝土表面,对于人工难以到达的位置则无法测量。

针对现有技术的不足,本文提出了基于交比图像量测技术的建筑物表面损伤面积检测方法,其总体流程如图1所示。

2 单图量测方法的研究现状

数码相机的拍照过程将客观世界的三维信息压缩到二维的像平面空间,因此会发生信息压缩和几何变形。在三维空间中,一组平行线经过射影变换后通常不再平行,而是汇聚于一个点,这个点被称为这组平行线的灭点^[4]。灭点通常对应三维空间中直线上位于无穷远处的一点。两个灭点的连线被称为平面的灭线,每个平面只有一条灭线^[6-7]。

在摄影前后,大多数目标的几何特征都会受到变形的影响,例如长度变化、失去平行关系等。然而,也有一些量不受射影的影响,保持射影不变性。这些不变性是可以加以利用的重要信息源和特性。

根据使用的图像数量,图像量测方法可以分为两种:基于两幅或多幅图像的量测方法和基于单幅图像的量测方法。

基于单幅图像的量测方法是一种新兴的图像测量系统,它的主要特点在于利用图像中的场景结构信息,从而实现对空间对象的几何量测^[12]。这种方法可以极大地提高测量的效率和准确度,使得人们在日常生活和科学研究中能够更加方便地进行测量和分析。

在这方面的研究中,许多学者已经做出了很多有价值的工作。例如,Johnson^[1]通过多边形、灭点灭线和圆形三种技术,对单幅图像进行了量测的研究。他的工作为单幅图像的几何量测提供了一种新的思路和方法。此外,Mendonca^[2]也介绍了一种利用单视图实现喷气发动机测量的应用实例,并展示了单视图图像在城市三维重建中的研究成果。他的工作为单幅图像的应用拓展提供了有力的支持。还有 Hoiem^[3]的单幅图像三维建模的研究工作,他采用了一种基于光滑曲面拟合的方法,能够从单幅图像中恢复出物体的三维结构,并实现对物体

的几何量测。除此之外,Hedau^[4]还成功地利用单幅图像恢复了室内场景的自由空间,他的工作为单幅图像的应用提供了一种新的思路和方法。总之,基于单幅图像的量测方法在图像处理、机器视觉和三维重建等领域具有广阔的应用前景和发展潜力。这一方法的研究成果将为人们的生产和生活带来更多的便利和效益。

单图量测算法是一种基于交比^[15]不变量的测量方法,可以通过单张图像中的像素坐标信息,计算出相应物体的真实尺寸和位置^[13]。

具体而言,单图量测算法利用了摄像机内外参数和场景物体的交比不变量之间的关系,通过对摄像机成像原理的理解和对摄像机内部参数的校准,可以准确地计算出摄像机成像时的场景信息,从而实现对物体尺寸和位置的测量。

交比不仅是摄影几何中的基本不变量^[5],也是计算机视觉领域中常用的几何不变量。在计算机视觉领域中,交比不仅可以用于测量物体的尺寸和位置^[8],还可以用于图像的配准、物体的跟踪和识别等方面。

3 基于交比图像量测技术检测建筑物表面损伤面积的方法

3.1 图像输入与预处理

首先输入一幅待测图像,图像需要包含损伤区域和整个墙面以及明显的边缘线条。然后使用 Matlab 图像处理函数库中的 `undistortImage` 函数进行畸变矫正。接下来选择待测图像中破损部分所在的墙面作为测量平面,并手动选取水平和垂直方向上的两条平行线。通过计算这两条平行线的交点坐标值,确定测量平面的位置。选取测量平面上的线段时,应选择墙面的线条而非墙面轮廓的边缘线或窗户的轮廓线。任意两点在待测图像上能够确定一条直线。因此,选取两条在现实场景中平行的线段,并在待测图像上选取它们的对应线段,根据透视原理,这两条线在图像上会相交于一点,这个点即为消失点。根据上述选取方法选取图像对应在实际场景中水平方向上的消失点 v_1 和垂直方向上的消失点 v_2 ,两个消失点的连线为消失线 v_l ,如图2所示。

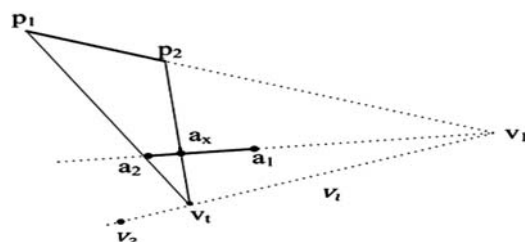


图2 平面内平行直线的交比示意图

得到经过畸变校正的图像后,标记待测图像中测量平面上的矩形参考物体,记录下矩形参考物体四个顶点位置在图像坐标系中的坐标值;人为选择测量平面上的部分区域作为参考矩形区域,参考矩形区域的长和宽分别与畸变矫正时所选取的图像中水平方向线段和垂直方向线段平行,且参考矩形区域的边长通过实际测量是已知的:长和宽分别为 d_1 、 d_2 ,选取参考矩形区域的四个顶点,记录下顶点的坐标信息,设四个顶点的坐标分别为 p_1, p_2, p_3, p_4 ;其中 p_1, p_2, p_3, p_4 与图像中水平方向线段平行, p_1, p_3, p_2, p_4 与图像中垂直方向线段平行, $p_1, p_2 = d_1$, $p_1, p_3 = d_2$ 。

手动选择待测图像中破损部分的最小外接矩形,记录下

矩形四个顶点在图像坐标系中的位置。利用这些顶点构建交比,通过几何关系来测量矩形边长。测量时,矩形的长和宽要与畸变矫正时所选取的水平 and 垂直方向线段平行。选取最小外接矩形框的四个顶点,记录下四个顶点位置在图像坐标系中的坐标值,设四个顶点的坐标分别为 a_1, a_2, a_3, a_4 , 其中 a_1a_2, a_3a_4 与图像中水平方向线段平行, a_1a_3, a_2a_4 与图像中垂直方向线段平行,如图 3 所示;

在待测图像上,连接 p_1a_2 并延长,与水平消失线 v_1 相交于 v_1 , 连接 p_2v_1 , 交 a_1a_2 的延长线于 a_x 点; 其中 p_1p_2 和 a_1a_2 均为平行于步骤 3 所述现实场景中水平方向线的线段, v_1 为所述测量平面消失线上的一点, 该平面所有经过 v_1 的直线在现实空间中均平行, 则 p_1a_2 和 p_2a_x 在空间中也互为平行线, 由几何知识得到四边形 $p_1p_2a_2a_x$ 在现实空间中为平行四边形, 因此 p_1p_2 和 a_2a_x 在空间中的实际长度相等。

3.2 消失点计算与交比构建

由 3.1 节可知, a_2, a_x, a_1, v_1 为图像中一条直线上的四点, v_1 为这条直线在图像中的消失点, a_2, a_x, a_1, v_1 在现实空间的对应点分别为 a_2, a_x, a_1, v_1 , V_1, A_2A_1 的实际长度为 d_1 , 根据线段交比几何关系有:

$$\text{Cross}(A_2, A_x, A_1, V_1) = \text{Cross}(a_2, a_x, a_1, v_1) \quad (1)$$

$\text{Cross}(A_2, A_x, A_1, V_1)$ 代表现实场景中四个点 A_2, A_x, A_1, V_1 的交比, $\text{Cross}(a_2, a_x, a_1, v_1)$ 代表现实场景中点在图像上的对应四个点 a_2, a_x, a_1, v_1 的交比, 式(1)表明图像中一条直线上四点位置的交比, 等于图像中这四点在空间位置的交比;

式(1)用距离的形式表示为:

$$\lim_{V \rightarrow \infty} \frac{d(A_2, A_x)d(A_1, V_1)}{d(A_2, A_1)d(A_x, V_1)} = \frac{d(a_2, a_x)d(a_1, v_1)}{d(a_2, a_1)d(a_x, v_1)} \quad (2)$$

其中, $d(A_2, A_x)$ 表示现实空间上两点 A_2, A_x 的距离, $d(A_1, V_1)$ 表示现实空间上两点 A_1, V_1 的距离, $d(A_2, A_1)$ 表示现实空间上两点 A_2, A_1 的距离, $d(A_x, V_1)$ 表示现实空间上两点 A_x, V_1 的距离, $d(A_2, A_x)$ 表示图像上两点 A_2, A_x 的距离, $d(A_1, v_1)$ 表示图像上两点 A_1, v_1 的距离, $d(a_2, a_1)$ 表示图像上两点 a_2, a_1 的距离, $d(a_x, v_1)$ 表示图像上两点 a_x, v_1 的距离;

由于现实空间中, V_1 为无穷远处的点, 则式(2)化简为:

$$\lim_{V \rightarrow \infty} \frac{d(A_2, A_x)}{d(A_2, A_1)} = \frac{d(a_2, a_x)d(a_1, v_1)}{d(a_2, a_1)d(a_x, v_1)} \quad (3)$$

式(3)中等式的右边的值通过记录的坐标计算得到, 设等式的右边的值为 cr_1 , 则通过 $d(A_2, A_1) = d_1/cr_1$ 能够求 A_2, A_1 直接的距离。

a_4, a_x, a_2, v_2 为图像中一条直线上的四点, v_2 为这条直线在图像中的消失点, a_4, a_x, a_2, v_2 在现实空间的对应点分别为 a_4, a_x, a_2, v_2 , A_4A_2 的实际长度为 d_2 。

此时, 式(1)用距离的形式表示为:

$$\lim_{V \rightarrow \infty} \frac{d(A_4, A_x)d(A_2, V_2)}{d(A_4, A_2)d(A_x, V_2)} = \frac{d(a_4, a_x)d(a_2, v_2)}{d(a_4, a_2)d(a_x, v_2)} \quad (4)$$

其中, $d(A_4, A_x)$ 表示现实空间上两点 A_4, A_x 的距离, $d(A_2, V_2)$ 表示现实空间上两点 A_2, V_2 的距离, $d(A_4, A_2)$ 表示现实空间上两点 A_4, A_2 的距离, $d(A_x, V_2)$ 表示现实空间上两点 A_x, V_2 的距离, $d(a_4, a_x)$ 表示图像上两点 a_4, a_x 的距离, $d(a_2, v_2)$ 表示图像上两点 a_2, v_2 的距离, $d(a_4, a_2)$ 表示图像上两点 a_4, a_2 的距离, $d(a_x, v_2)$ 表示图像上两点 a_x, v_2 的距离;

由于现实空间中, v_2 为无穷远处的点, 则式(4)化简为:

$$\lim_{V \rightarrow \infty} \frac{d(A_4, A_x)}{d(A_4, A_2)} = \frac{d(a_4, a_x)d(a_2, v_2)}{d(a_4, a_2)d(a_x, v_2)} \quad (5)$$

式(5)中等式的右边的值通过记录的坐标计算得到, 设等式的右边的值为 cr_2 , 则通过 $d(A_4, A_2) = d_2/cr_2$ 能够求 A_4, A_2 直接的距离。

3.3 图像处理

对 3.2 节中选取的测量区域进行透视变换还原成矩形, 并进行二值化、形态学滤波处理; 在实际工程检测时, 将建筑物外表面出现损伤的区域依照测试平面内的几何关系用四边形框框选出, 该框选出的区域为测量区域。接着对四边形进行透视变换, 将图像中的平行四边形转换成矩形, 并依据 3.1 中所述的方法计算出测量区域的边长, 得到测量区域的实际面积 $S = d(A_2, A_1)d(A_2, A_4)$, 再对测量区域进行二值化和形态学滤波, 得到建筑物表面损伤区域的二值图像。其中, 图像二值化就是将图像上的像素点的灰度值设置为 0 或 255, 整个图像呈现出明显的黑白效果。形态学滤波是通过膨胀(或扩张)、腐蚀(或侵蚀)、开运算和闭运算四个基本运算对二值化图像进行滤波处理。

3.4 损伤区域面积计算

统计图像中损伤部分的像素个数, 经过二值化处理, 损伤部分在图像中显示为白色, 完整区域显示为黑色, 对整个测量区域每一个像素点进行判断, 如果像素值为 255, 该像素点即为白色像素点, 统计测量区域中白色像素点的总个数, 结合测量区域的面积经过比例运算得到损伤部分的实际面积 W :

$$W = \frac{M}{N} \times S \quad (6)$$

其中, M 表示损伤部分像素个数, N 表示测量区域像素个数。

4 实例分析

为了使本文的目的、方法及优点更直观的体现, 本节结合应用实例, 对第 3 节中的方法进行进一步详细说明。

实例中选取一幅建筑物外表面有明显损伤的图像, 由尼康 D7200 数码相机拍摄, 由于数码相机拍摄时出现畸变的现象无法避免, 因此采用 Matlab 的单目相机标定工具箱 Camera Calibrator toolbox 进行标定操作, 并用 undistortImage (image, cameraParams) 函数进行畸变校正, 校正后的图像大小为 1383×913; 如图 3 所示, 点和直线信息的提取以人机交互的形式获得, 将窗 1 作为参考对象, 测得其边长 B_1B_3, B_1B_2 分别为 1.78m, 1.16m, 框选区 $A_1A_2A_3A_4$ 为待测区域;

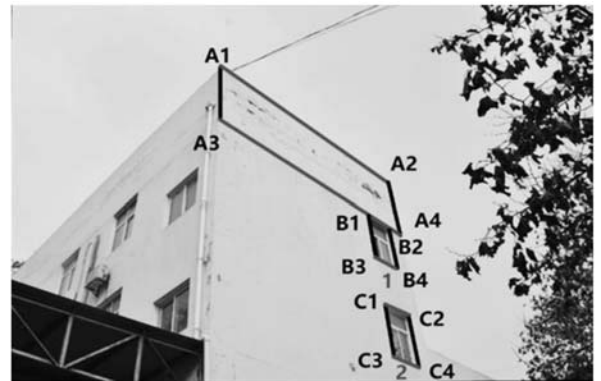


图 3 在畸变校正后的图像选取测量区域

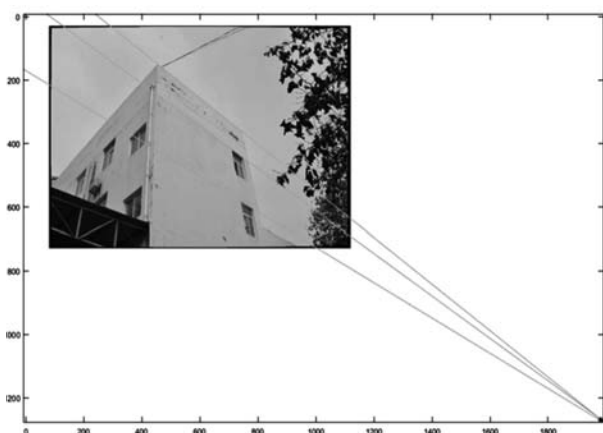


图4 待测图像的第一个消失点

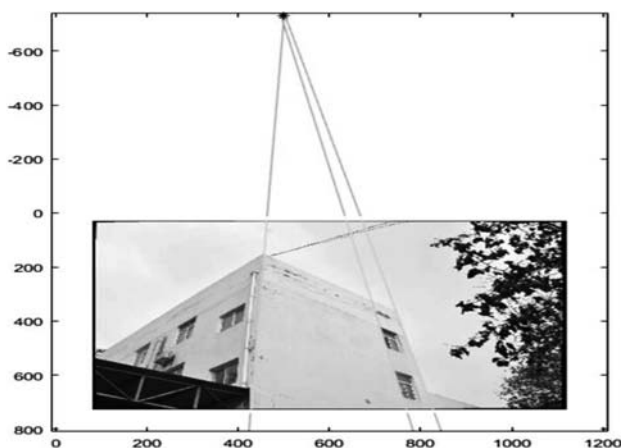


图5 待测图像的第二消失点

如图4和图5所示,本实例利用两组平行线,分别确定消失点 V_1, V_2 ,并由这两个消失点确定出该平面的消失线。所获取消失点坐标分别为(2056.3, 1326.3)与(497.1, -725.2)。

基于 B_1B_2 与 B_1B_1 的实测距离,利用交比性质求得图3框选区域 $A_1A_2A_3A_4$ 的边长 A_1A_3, A_2A_4 分别为 2.5992 m, 9.2159 m。通过 OpenCV 函数库中的函数 `getPerspectiveTransform` 函数和 `warpPerspective` 函数对四边形进行透视变换还原成矩形,将 `getPerspectiveTransform` 函数求得的变换矩阵带人 `warpPerspective` 函数中得到还原矩形,并计算出该矩形框选区域出实际面积为 23.9539m²。

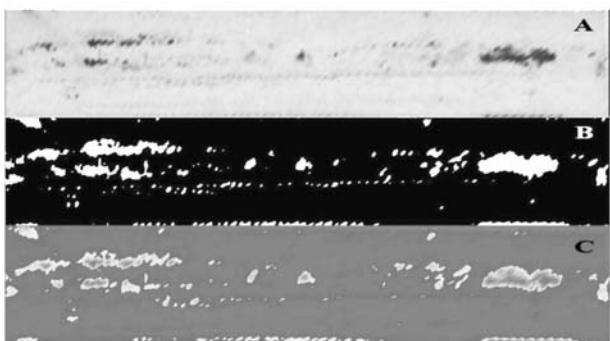


图6 建筑物破损区域的灰度图与二值图的对比分析

为准确提取损伤部分,本文采用 Otsu 分割方法得到最优阈值 $T=156$,并采用该阈值对图像分割得到二值图像。通过开运算、闭运算、膨胀和腐蚀相关常用形态学滤波步骤,可得如图6所示图像处理结果,图中,最上方的A区域表示灰度图,

中间部分的B区域是二值图,最下方的C区域是灰度图与二值图叠加图。统计图像中像素值为 255 (白色像素点) 像素点的个数与测量区域像素点总个数,按式(3)计算出损伤区域面积为 2.83966 m²,如表1所示。破损区域二值图像与实际破损面基本吻合。因此,本文测量方法在工程检测中的能有效检测建筑物表面损伤面积。

表1 建筑物选择区域内破损区域的测量结果

白色像素点个数	28300
测量区域总像素点个数	243144
测量区域损伤比	11.6392%
框选区域面积	23.9539m ²
测量区域损伤面积	2.83966m ²

5 结语

针对建筑物外表面损伤部分检测困难,几何信息难以提取的问题,本文将基于交比的单幅图像量测技术应用至含有丰富三维空间平行线的建筑物图像量测中。首先,对图像进行畸变的矫正;再利用建筑物结构中的垂直水平等几何关系,找到消失点,结合已知长度的参考线段以及消失点、消失线构建交比,框选出测量区域,多次嵌套后实现对测量区域边长的量测;再通过数字图像处理技术,对测量区域进行透视变换还原成矩形,并实现二值化、形态学滤波等处理;最后在计算出测量区域实际面积,统计出策略测量区域总像素点个数以及白色像素点个数,找到比例关系,得到损伤区域面积,对实验结果及可行性进行分析。本文利用计算机视觉测量技术,实现了较大范围、远距离的建筑物外表面损伤区域检测,并量化不规则损伤区域的面积属性,且仅使用手机或相机拍摄单幅照片即可完成,不仅成本低,而且极大的方便了建筑运维管理人员对建筑表面损伤的分布以及损伤程度的判断,进而合理的安排损伤修复或结构加固的维修计划。

参考文献:

- [1] Johnson M K, Farid H. Metric measurements on a plane from a single image[J].2006.
- [2] Mendonca P R S, Kaucic R. Single View Metrology: A Practical Example[C]//2008 IEEE Workshop on Applications of Computer Vision. IEEE, 2008:1-8.
- [3] Hoiem D, Efros A A, Hebert M. Automatic photo pop-up [M]//ACM SIGGRAPH 2005 Papers. 2005:577-584.
- [4] Hedau V, Hoiem D, Forsyth D. Recovering free space of indoor scenes from a single image[C]//2012 IEEE conference on computer vision and pattern recognition. IEEE, 2012: 2807-2814.
- [5] 王美珍, 刘学军, 甄艳, 卢玥. 基于交比的单幅图像平面几何信息提取算法[J]. 武汉大学学报(信息科学版), 2011, 36(02): 190-194. DOI:10.13203/j.whugis.2011.02.023.
- [6] Criminisi A, Reid I, Zisserman A. Single view metrology[J]. International Journal of Computer Vision, 2000, 40: 123-148.
- [7] Debevec P E, Taylor C J, Malik J. Modeling and rendering architecture from photographs: A hybrid geometry-and image-based approach [C]//Proceedings of the 23rd annual conference on Computer graphics and interactive techniques. 1996:11-20.
- [8] 隋铭明, 高天宇. 单幅未标定像片进行树木形态测量的新方法[J]. 森林工程, 2013, 29(05): 12-15+18. DOI: 10.16270/j.cnki.slgc.2013.05.036.

(下转第28页)

值以及一般的整数加法运算,因此其比特复杂度为 $O(n^3 \lg m)$ 。

求解热带 LP 矩阵作用问题的复杂度可以采用穷举的方法。对于一个 n 阶的热带 LP 矩阵,总共有 n^2 个元素,除了对角线上的元素是相等以外,其余位置都是不相同的,不相同的元素一共有 $n^2 - n$ 个。这些不同的元素将会在给定的热带 LP 矩阵设置的取值范围内随机选取,同样的,对角线上的元素只有一个值,也将会在给定的热带 LP 矩阵设置的取值范围内随机选取。综合这两种情形,就可以穷举出一个热带 LP 矩阵中的所有情形。因为热带 LP 矩阵作用问题有两个不同的热带 LP 矩阵,最后将这两种矩阵的情形相乘即可得到求解热带 LP 矩阵问题的穷举复杂度,如表 3 所示。

表 3 对比本方案在不同参数下公钥与私钥的最大上界

Table 3 Compare the maximum upper bound of the public and private keys of this scheme under different parameters

矩阵阶数	对角线上元素的取值范围	非对角线上元素的取值范围	公钥大小	私钥大小
30	[-50,0)	[50,100)	2.64kb	3.57kb
40	[-50,0)	[50,100)	4.69kb	6.33kb
50	[-50,0)	[50,100)	7.32kb	9.86kb
30	[-100,0)	[100,200)	3.52kb	5.33kb
40	[-100,0)	[100,200)	6.25kb	9.45kb
50	[-100,0)	[100,200)	9.77kb	14.75kb

公钥与私钥的最大上界的值是根据矩阵的阶数决定的。一个阶矩阵里的每一个元素都在取值范围内随机选取一个值,将每个元素随机选取值的比特大小累加,就可得到对应的公钥与私钥的最大上界。

5 结语

本文利用极小加热带半环的 Linde-de-la Puente 型矩阵设计了基于热带 LP 矩阵作用问题的密钥交换协议和公钥加密方案。热带 LP 矩阵具有和 Linde-de-la Puente 矩阵一样的交换性的性质,因此双方在进行密钥交换协议过程中,可以得到相同的密钥,从而达到明文消息在公开信道上可以进行加密通讯的目的。最后还对一些可能对本方案造成的攻击进行了分析,并说明其不可行性。

还有待研究的问题包括:(1)研究求解热带半环的非线性方程组的算法,虽然一般该问题是 NP 困难的,但在某些特殊情形下,有可能存在有效的算法。(2)利用其他热带交换矩阵设计类似的公钥密码系统。

参考文献:

- [1] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6):644-654.

- [2] Shor, P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM J. Comput. 1997, 26(5), 1484-1509.
- [3] Gerard M, Chris M, Joachim R. A public key cryptosystem based on actions by semigroups[C]//IEEE International Symposium on Information Theory-Proceedings. 2002:266-289.
- [4] Maze, G.; Monico, C.; Rosenthal, J. Public Key Cryptography based on semigroup Actions[J]. Adv. Math. Commun. 2007, 1(4), 489-507.
- [5] Stickel. A new method for exchanging secret keys[C]. In Third International Conference on Information Technology and Applications (ICITA'05), volume 2, pages 426-430. IEEE, 2005.
- [6] Vandiver H S. Note on a simple type of algebra in which the cancellation law of addition does not hold[J]. Plant Physiology, 1934, 125(4):1854-1869.
- [7] Simon I. Recognizable sets with multiplicities in the tropical semiring[C]//International Symposium on Mathematical Foundations of Computer Science. Springer, Berlin, Heidelberg, 1988:107-120.
- [8] Simon I. On semigroups of matrices over the tropical semiring [J]. RAIRO-Theoretical Informatics and Applications, 1994, 28(3-4): 277-294.
- [9] Grigoriev D, Shpilrain V. Tropical cryptography [J]. Communications in Algebra, 2014, 42(6):2624-2632.
- [10] Kotov M, Ushakov A. Analysis of a key exchange protocol based on tropical matrix algebra[J]. Journal of Mathematical Cryptology, 2018, 12(3):137-141.
- [11] Grigoriev, D.; Shpilrain, V. Tropical cryptography II-Extensions by homomorphisms. [J]. Communications in Algebra, 2019, 47(10), 4224-4229.
- [12] Rudy, D.; Monico, C. Remarks on a Tropical Key Exchange System[J]. Journal of Mathematical Cryptology, 2021, 15(1), 280-283.
- [13] Isaac S, Kahrobaei D. A closer look at the tropical cryptography[J]. International Journal of Computer Mathematics: Computer Systems Theory, 2021, 6(2):137-142.
- [14] Huang H, Li C, Deng L. Public-Key Cryptography Based on Tropical Circular Matrices[J]. Applied Sciences, 2022, 12(15):7401.
- [15] Ahmed K, Pal S, Mohan R. Key exchange protocol based upon a modified tropical structure[J]. Communications in Algebra, 2022:1-10.
- [16] Linde J, De L. Matrices commuting with a given normal tropical matrix[J]. Linear Algebra & Its Applications, 2015, 482:101-121.
- [17] Muanalifah A, Sergeev S. Modifying the tropical version of Stickel's key exchange protocol[J]. Applications of Mathematics, 2020, 65(6):727-753.

+++++

(上接第 23 页)

- [9] Dunker K F, Rabbat B G. Why America's bridges are crumbling[J]. Scientific American, 1993, 268(3): 66-72.
- [10] Love P E D, Li H. Quantifying the causes and costs of rework in construction[J]. Construction management & economics, 2000, 18(4): 479-490.
- [11] Mills A, Love P E, Williams P. Defect costs in residential construction [J]. Journal of Construction Engineering and Management, 2009, 135(1):12-16.
- [12] Criminisi A. Accurate visual metrology from single and mul-

tle uncalibrated images[M]. Springer Science & Business Media, 2001.

- [13] 张剑清,王强.基于近景单影像的房檐改正计算方法[J].武汉大学学报(信息科学版),2007(12):1091-1094.
- [14] Rother C. A new approach to vanishing point detection in architectural environments[J]. Image and Vision Computing, 2002, 20(9-10): 647-655.
- [15] Lei G. Recognition of planar objects in 3-D space from single perspective views using cross ratio[J]. IEEE Transactions on Robotics and Automation, 1990, 6(4):432-437.