大幅面多光谱遥感图像快速自动配准

徐丽燕 张洁玉 孙巍巍 孙权森 夏德深
(南京理工大学计算机科学与技术学院 南京 210094)

摘 要 针对大幅面多光谱遥感图像的配准需求,提出一种基于特征点的快速全自动配准方法。由于多光谱遥感图像的尺寸较大,计算量大,因此提出特征网格理论,即根据图像灰度值、信息熵值及特征分布均匀性准则,在二级规则网格中选取特征网格参与后续运算,以减小计算量。同时,该理论为SIFT(Scale Invariant Feature Transform)特征点提取算法的并行运行及特征点初匹配方法的改进提供了条件,提高了算法的效率及配准精度。利用本算法对CBERS-02B拍摄的遥感图像进行了实验。结果表明,该方法能够达到亚像素级配准精度,且计算速度快,能够满足大幅面遥感图像处理的要求。

关键词 遥感图像,特征网格,SIFT
中图法分类号 TP391.41 **文献标识码** A

Fast and Automatic Registration Method for Large Multi-spectral Remote Sensing Images

XU Li-yan ZHANG Jie-yu SUN Wei-wei SUN Quan-sen XIA De-shen
(School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract Aiming at the registration of large multi-spectral remote sensing images, a fast and automatic registration method based on feature points was proposed. Because the size of the multi-spectral remote sensing image is quite large, and the amount of calculation is also very great, the theory of feature grid based on grey value, entropy and uniformity principle was proposed. Feature grids chosen from a two-degree regular mesh are calculated in the subsequent process to reduce the calculation. Meanwhile, the theory provides condition for detecting SIFT(Scale Invariant Feature Transform) feature points parallelly, and for improving the primary feature matching step, so the efficiency and accuracy are increased. The proposed method was applied to remote sensing images taken by CBERS-02B. The experimental results with large remote sensing images clearly indicate that the proposed approach can achieve sub-pixel precision, decrease the runtime of the process, and the requirement of large remote sensing image process is satisfied.

Keywords Remote sensing images, Feature grid, SIFT

1 引言

近年来随着航空航天事业的突飞猛进,遥感数据的多元化和信息量不断提高,为城市规划、天气预报、变化检测、地理信息处理等实际应用提供了丰富的资源。但是多时相、多遥感器、多光谱等多源遥感图像在分辨率、灰度属性、旋转和平移等方面存在差异,并且遥感图像一般尺寸较大,因此实现大幅面遥感图像的快速自动配准算法是所有后续遥感数据应用的前提。

图像配准是指在同一场景、不同时间、从不同视角或由不同传感器拍摄的两幅或多幅图像之间确定最佳匹配的过程[1]。传统的遥感图像配准方法依靠人工手动选取特征点对,要耗费几个小时甚至几天的时间才能完成一幅图像的配准[6],十分费时费力,不能满足大数据量的应用需求。另外,由于受到人的主观因素的影响,人工处理的配准精度得不到有效保证。因此,近年来亚像素级大幅面遥感图像快速自动配准方法逐渐成为专家学者们研究的重点。

配准算法一般可分为基于灰度和基于特征两大类。基于灰度的配准算法[2,3]直接利用图像的灰度信息建立图像之间的相似性度量,然后按照某种搜索策略来确定使得相似性度量最大的变换参数。虽然这种方法具有较高的精度,但由于图像中所有的像素点均参与了计算,因此算法计算量大,运行效率低,不适用于大幅面遥感图像的配准。基于特征的配准算法[4,5]首先提取图像中的显著特征(如角点、边缘、直线等)形成特征集,然后确定两幅图像特征集中各个特征的对应关系,计算出变换参数,从而实现图像的配准。这类算法仅利用了图像中的显著特征参与计算,减小了计算量,速度较快,因此在遥感图像配准领域获得了广泛应用。文献[4]提出了一种由粗到精的遥感图像自动配准方法,先用SIFT(Scale Invariant Feature Transform)算法提取特征点进行粗配准,然

到稿日期:2011-04-15 返修日期:2011-06-29 本文受国家自然科学基金(61003108)资助。
徐丽燕(1983—),女,博士生,主要研究方向为图像处理、遥感信息系统等,E-mail:leeann666@126.com;张洁玉(1980—),女,博士生,主要研究方向为计算机视觉、模式识别等;孙巍巍(1985—),男,硕士生,主要研究方向为模式识别、图像处理等;孙权森(1963—),男,教授,博士生导师,主要研究方向为模式识别、遥感信息系统等;夏德深(1941—),男,教授,博士生导师,主要研究方向为图像处理、卫星遥感等。

后利用 Harris 算子提取特征点建立不规则三角网(TIN:Triangulated Irregular Networks)进行精配准。文献[7]在特征匹配步骤中结合了特征点的空间位置关系与相似度信息以提高特征点的匹配准确度,从而得到较高的配准精度。文献[8]通过结合 Harris 角点特征和 Canny 边缘特征获取变换参数进行配准。但是这些方法都没有考虑到特征分布的均匀性以及进一步剔除特征误匹配的问题,并且其运行时间不能达到大幅面遥感图像批量处理的要求。

本文从大幅面遥感图像快速自动配准的需求出发,在权衡配准精度与运行时间的基础上,提出一种基于 SIFT 特征点的网格化的大幅面遥感图像快速自动配准算法。首先在大幅面遥感图像上建立二级规则网格,通过图像灰度值、信息熵值及特征分布均匀性准则选取特征网格,确保特征点的数量及其在整幅图像上分布的均匀性;然后在各特征网格中并行地采用 SIFT 方法提取特征点,并利用改进的 SIFT 特征点匹配算法建立两个特征点集之间的初匹配;再依据相关性原理及特征点之间的空间距离约束关系去除误匹配点对;最后根据仿射变换模型计算出变换参数,实现图像配准。

2 特征提取

2.1 特征网格选取

信息熵是图像所具有的信息量的度量,熵值越大,表明信息量越大,特征存在的可能性越高[9],因此可以将信息熵的值作为特征是否存在的判断依据。

$$E=-\sum_{i=0}^{N} p_i \log p_i \tag{1}$$

式中,$N=255$,p_i 表示灰度为 i 的像素在图像中出现的概率。

在图像上建立规则网格,该网格包含粗、细两种网格(见图 1)。细网格用虚线划分,粗网格用实线划分,相邻的 4 个细网格组成一个粗网格。选取特征网格的步骤如下:

1)剔除 0 灰度级过半的网格;

2)计算各细网格的信息熵,将熵值从大到小排序,对应熵值排在前 1/4 的细网格直接作为特征网格(如图 1 中灰色细网格);

3)在不含特征网格的粗网格中,选取熵值最大的细网格作为特征网格(如图 1 中斜线细网格)。

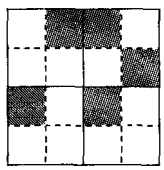
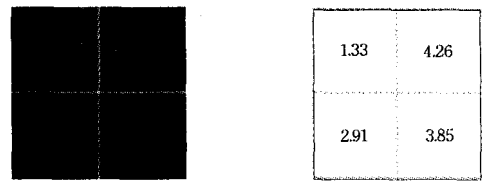


图 1 二级规则网格

本文算法的研究对象是经过系统几何校正的二级图像,由于经过旋转,图像四周以灰度值为 0 的像素点填充。为了提高算法效率,首先去除 0 灰度级过半的仅含有少量信息的细网格(如图 2(a)左上角网格);然后计算其余所有细网格的信息熵(如图 2(b)所示),取熵值排在前列的细网格直接作为参与后续运算的特征网格(如图 2(a)右上角网格),这样能够确保图像信息丰富的区域参与后续运算,提取到足够多的特征点;最后再考察每个粗网格内是否含有特征网格,若不含,则在此粗网格内选取信息熵值最大的细网格作为特征网格,以此保证特征网格在整幅图像中分布的均匀性。



(a)划分网格 (b)(a)中各网格对应熵值

图 2 特征网格选取

通过上述步骤选取特征网格,可以保证图像中灰度变化剧烈、信息量大的区域有较多的特征网格,而在灰度变化小、信息量少的区域也有特征网格,使得在特征网格中提取的特征点能够在大幅面遥感图像上呈现均匀分布,从而提高配准精度[1]。通过选取特征网格,缩小特征点的提取范围,可以大大减小算法的计算量,提高配准速度。

2.2 SIFT 特征点提取

SIFT 特征点是 Lowe[10] 提出的一种局部不变量特征提取方法。该特征点具有较高的重复率,对图像的旋转、缩放以及亮度变化具有不变性,且对仿射变换、视角变换及噪声有一定程度的鲁棒性,因而已被广泛应用于图像拼接、目标跟踪及三维重建等多个领域[11-13]。SIFT 特征点提取方法主要分为 3 步:(1)特征点检测及定位;(2)生成特征描述符;(3)特征点初匹配。文献[10]给出的特征点匹配方法,是对待配准图像中的每个特征点,遍历参考图像的特征点集,计算特征向量的欧式距离,找到最近邻(NN)和次近邻(SCN),根据 NN/SCN 的值对两幅图像的特征点进行匹配。

经过几何校正的大幅面多光谱遥感图像之间,绝大部分区域的像差为 1~2,小部分区域像差达 3~5,因此正确的匹配点对的像差也应该在此范围内。针对这个特点,本文对初匹配步骤进行了改进:对待配准图像(如图 3(b))中的特征点,以改点为中心建立 11×11 像素的邻域(图 3(b)中小方框),只计算它和位于基准图像相应邻域(图 3(a)中小方框)内各特征点的欧式距离,然后依据阈值判断其是否匹配。由于不需要遍历参考图像中的所有特征点,并且约束了特征点的坐标位置,因此能有效减小算法的计算量,提高匹配效率,同时减小误匹配的概率。

(a)基准图像 (b)待配准图像

图 3 改进的特征点初匹配

3 特征匹配

所谓特征点匹配,就是在待配准图像中找到基准图像中每个特征点的唯一匹配点[14]。本文算法依据相关性原理[14]及特征点之间的空间距离约束关系[14],剔除初匹配点集中的误匹配,建立待配准图像与基准图像的特征点之间正确的一一对应的匹配关系。

1)相关性原理

假设参考图像 X 和待配准图像 Y 的 SIFT 初匹配点集分别为 X_P 和 Y_P(其中:P 为初匹配特征点集中的匹配点对

数)：$\{X_p=[x_p,y_p]\mid p=1,\cdots,P\}$，$\{Y_p=[x_p',y_p']\mid p=1,\cdots,P\}$，对于点集 X_P 中的任意一点(x_p,y_p)构造$(2m+1)(2n+1)$像素的邻域，则两幅图像任意特征点对(x_p,y_p)和(x_p',y_p')的互相关系数为：

$$\rho=\frac{\sum XY-\frac{\sum X\sum Y}{(2m+1)(2n+1)}}{\sqrt{\left(\sum X^2-\frac{\sum X\sum X}{(2m+1)*(2n+1)}\right)*\left(\sum Y^2-\frac{\sum Y\sum Y}{(2m+1)*(2n+1)}\right)}} \tag{2}$$

式中，$\sum X$ 表示图像 X 对应邻域的像素灰度值之和；$\sum Y$ 表示图像 Y 对应邻域的像素灰度值之和；$\sum XY$ 表示两幅图像中对应像素的灰度值的乘积。

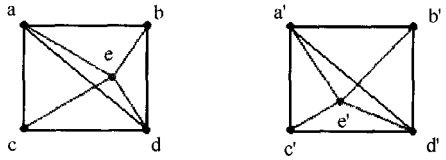
通过 SIFT 特征点提取及初匹配步骤得到的初匹配点对中，可能存在“一对多”或者“多对一”的情况。“一对多”是指基准图像中的一个特征点在待配准图像特征点集中有多个特征点与之相匹配；“多对一”是指基准图像中的多个特征点都与待配准图像特征点集中的一个特征点有匹配关系。显然，这样的匹配关系是错误的。为了去除这类误匹配，首先在初匹配点对中找到“一对多”和“多对一”的点对，然后计算每个点对的互相关系数，将互相关系数最大的点对视为正确的匹配点对并予以保留，而将其他点对都剔除。经过该步骤后，基准图像与待配准图像的特征点之间均为一一对应的匹配关系。

2)空间距离约束

由于多光谱遥感图像的各谱段图像之间不存在缩放，因此，可以运用空间距离约束条件进一步剔除误匹配特征点对。

一个点 $Y_k(x',y')$是特征点 $X_k(x,y)$的正确对应点的充要条件是 $Y_k(x',y')$到其他特征点正确对应点 $Y_i(x',y')$的距离和特征点 $X_k(x,y)$到其对应的特征点 $X_i(x,y)$的距离相等[13]。

如图 4 所示，图 4(a)是基准图像，图 4(b)是待配准的图像，a 和 a'，b 和 b'，c 和 c'，d 和 d'是正确的匹配点对，而 e 和 e'是误匹配点对。则 a 到 b 的距离和 a'到 b'的距离理论上应该相等，即$|ab|=|a'b'|$，同理有$|ac|=|a'c'|$，$|ad|=|a'd'|$，$|bc|=|b'c'|$，$|bd|=|b'd'|$，$|cd|=|c'd'|$。而 e 和 e'到其它点的距离则不满足这个距离约束条件。



(a) 基准图像　　(b)待配准图像

图 4　空间距离约束

由于特征点存在自身定位的误差，即使是正确的匹配点对之间，实际计算得到的距离也不可能完全相等，一般认为误差在 0.5 个像素之内的都满足距离约束条件。

4　算法流程

算法步骤(见图 5)

1. 在基准图像和待配准图像上建立二级规则网格，依据图像灰度值、信息熵值及特征分布均匀性准则来选取特征细网格；

2. 在各个特征细网格中提取 SIFT 特征点，将两幅图像对应细网格中的特征点按照改进的基于位置约束的特征点匹配方法建立初匹配关系；

3. 利用相关性原理及特征点之间的空间距离约束关系剔除初匹配点集中的误匹配；

4. 运用最小二乘法计算仿射变换参数，并通过二次线性插值得到变换后的图像，完成配准。

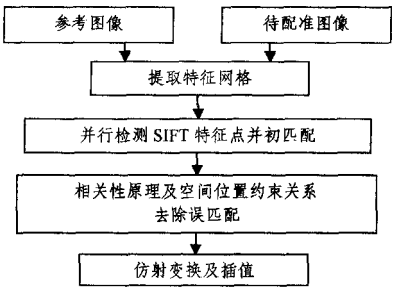


图 5　算法流程图

由于采用了网格技术，各细网格在前三步处理中是相互独立的，因此编程中在 SIFT 特征点提取、初匹配及去除误匹配步骤，可以采用并行处理，以缩短处理时间。

算法中 SIFT 参数的设置与特征网格的熵值相关：熵值较大，说明该网格内信息较丰富，可设置较大的 SIFT 阈值；熵值较小，表明该网格内信息量较小，应设置较小的 SIFT 阈值。为了较少人机交互，实现全自动配准，在程序中将 SIFT 参数的范围设为 0.02～0.0008(见表 1)，而每个网格的具体参数由程序根据各个网格的熵值进一步确定。

表 1　SIFT 阈值设定

信息熵值	>5	>4.5	>3.8	>3	>2	>1	≤1
SIFT 阈值	0.02	0.016	0.008	0.006	0.004	0.002	0.0008

5　实验结果与分析

用 Visual C++ 6.0 在 PC 机(Pentium E2180 2.0GHz、2G 内存)上实现了全部算法并进行了测试。测试所用图像来源于中国资源卫星应用中心网站[17]，是 CBERS-02B 星拍摄的分辨率为 20m、幅宽为 113km 的大幅面遥感图像。

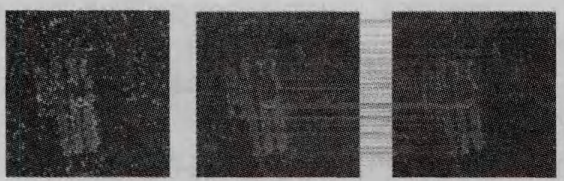
程序中 SIFT 初匹配位置约束为 11×11 像素大小的窗口，欧式距离阈值为 0.39。在测试中采用均方根误差(RMSE:Root Mean-Square Error)[4]进行配准效果评价。

5.1　实验 1

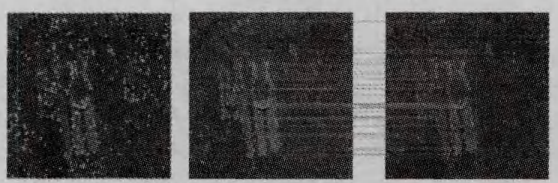
在原图像上截取大小为 512×512 像素的图像，用 SIFT 算法提取特征点后，分别用文献[10]的方法和本文初匹配方法进行特征点匹配。图 6(a)为 3 谱段图像，将其作为基准图像，提取到 441 个 SIFT 特征点；图 6(b)为 4 谱段图像，将其作为待配准图像，提取到 369 个 SIFT 特征点；图 6(c)和图 6(d)分别为文献[10]的匹配方法和本文方法得到的特征点对的匹配结果。由于同组多光谱图像之间像差不大，因此对应特征点之间的连线基本上是水平的。而图 6(c)中出现了明显的斜线，说明存在错误匹配的点对。

表 2 定量地给出了两种方法的对比。图 6(a)与图 6(b)的正确匹配点对应为 94 对，文献[10]的方法耗时 68ms，得到

103 对匹配点对，其中有 9 对错误点对；本文的初匹配方法耗时 2ms，得到 96 对匹配点对，有 2 对错误点对。表 2 表明本文提出的特征点初匹配方法较原方法在运行时间及匹配正确率方面均有显著提高。



(a)基准图像　　(c)文献[10]的匹配方法



(b)待配准图像　　(d)本文的初匹配方法

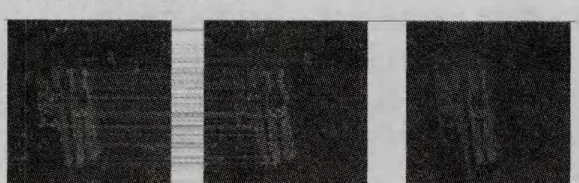
图 6　特征点提取及初匹配结果

表 2　文献[10]与本文初匹配方法对比

	运行时间(ms)	匹配点对	正确率(%)
文献[10]方法	68	103	91.26
本文方法	2	96	97.92

5.2　实验 2

本文方法在完成特征点初匹配后，进一步利用相关性原理及特征点之间的空间距离约束关系剔除误匹配点对。图 7(a)为对图 6(d)采用相关性原理及空间距离约束(耗时 1ms)后得到的 94 对正确匹配特征点的对应情况，图 7(b)为图 6(b)配准后的图像。表 3 给出了基准图像与待配准图像(见图 6(a)与(b))、初匹配后直接进行仿射变换以及利用本文方法剔除误匹配后进行变换得到的 RMSE。基准图像与待配准图像的像差为 1.12；直接利用初匹配得到的 96 对点对计算仿射变换参数得到的图像与图 6(a)的像差为 0.455；本文方法的配准精度达到 0.155。由表 3 可以得出结论：相关性原理及特征点间的空间距离约束关系能够有效去除误匹配，提高配准精度，改善配准效果。



(a) 相关性原理及空间距离约束后匹配点对　　(b) 图 4(a)配准后图像

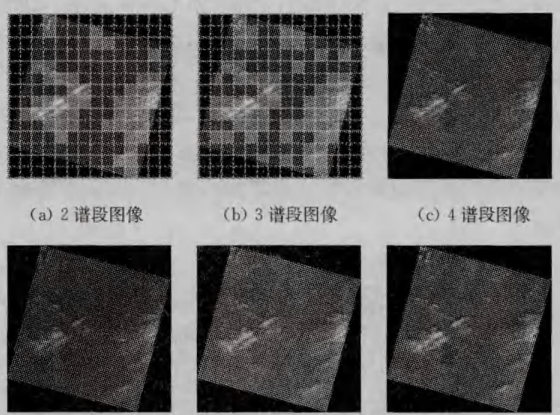
图 7　最终匹配结果及配准后图像

表 3　RMSE 值对比

	图 6(a)(b)	直接变换	本文方法
RMSE	1.12	0.455	0.155

5.3　实验 3

利用本文算法对大幅面多光谱遥感图像进行配准。图 8(a)(b)(c)所示图像分别为 2、3、4 三个谱段的多光谱遥感图像(图像大小 7080×7072 像素，灰度级 0－255)。首先在图像上建立二级规则网格，细网格大小为 500×500 像素(见图 8(d)虚线所绘网格)；相邻 4 个细网格组成一个粗网格，粗网格大小为 1000×1000 像素(见图 8(d)实线所绘网格)，因此规则网格中有 14×14 个细网格，7×7 个粗网格。通过计算各个细网格的信息熵值，取熵值较大的前 1/4 个(即 49 个)细网格作为特征网格(如图 8(d)中增亮的细网格)。由于该组图像左右两侧纹理较丰富，因此依据信息熵值选取的 49 个特征网格也集中分布在左右两侧，而图像的上、下及中间部分几乎没有。考虑到特征分布均匀性对配准精度的重大影响，需进行二次特征网格提取，在没有特征网格的粗网格中，将熵值最大的细网格也作为特征网格。该组图像在二次特征网格提取时又增加了 17 个特征网格，因此共有 66 个细网格作为最终的特征网格(如图 8(e)中增亮的细网格)，且特征网格较均匀地分布于整幅图像。将图 8(b)作为参考图像，对图 8(a)、(c)进行配准，将配准后的图像与参考图像合成得到的图像为图 8(f)(3、4、2 三谱段图像分别作为 R、G、B 三通道合成 BMP 图像)。



(a) 2 谱段图像　(b) 3 谱段图像　(c) 4 谱段图像

(d) 4 谱段-49 个特征网格　(e) 4 谱段-66 个特征网格　(f) 结果图

图 8　图像配准过程

表 4 给出了图 8(a)、(c)在配准过程中的相关数据及配准前后的 RMSE 值。由表 4 可以看到，两幅图像的配准时间小于 20s，且配准精度小于 0.3 像素。

表 4　图 8 配准结果

待配准图像	运行时间(s)	特征网格数	匹配点对数	配准前 RMSE	配准后 RMSE
图 8(a)	19.36	67	2163	1.06	0.25
图 8(c)	17.52	66	2118	1.13	0.29

5.4　实验 4

从中国资源卫星应用中心网站[17]上下载了 15 组 CBERS-02B 星拍摄的大幅面多光谱遥感图像(图像大小约为 7000×7000 像素，灰度级 0－255)，按照纹理的丰富程度将其划分为高、中、低三类，对每类 5 组图像进行了实验。实验中，均以第 3 谱段图像作为基准图像，第 2 谱段和第 4 谱段图像为待配准图像。配准结果如表 5 所列。

表 5　配准结果

评价项	运行时间(s)		特征网格数		匹配点对数		配准前 RMSE		配准后 RMSE	
图像	2 谱段	4 谱段	2 谱段	4 谱段	2 谱段	4 谱段	2 谱段	4 谱段	2 谱段	4 谱段
最大值	50.1	49.7	71	72	26768	30346	1.06	1.24	0.35	0.41
最小值	19.4	17.5	60	63	1443	1404	0.73	0.76	0.23	0.29
均值	32	34.6	66	68	7798	11735	0.91	0.95	0.29	0.34

结束语 为了实现大幅面多光谱遥感图像配准的批量处理，提出了一种快速自动配准算法。该方法利用图像灰度值、信息熵及特征分布均匀性准则从二级规则网格中选取特征网格，然后采用 SIFT 算法在筛选获取的特征网格中并行地提取特征点，从而减少了运算时间。在特征匹配步骤，改进了原算法的匹配方法，提出了基于位置约束的快速初匹配方法，并利用相关性原理及特征点之间的空间距离约束关系进一步剔除了误匹配，提高了特征匹配准确度。实验结果表明，本文方法能够实现大幅面遥感图像的快速、自动、亚像素级配准。

参 考 文 献

[1] Zitova B, Flusser J. Image registration methods: a survey[J]. Image and Vision Computing, 2003, 21(11): 977-1000

[2] Kern J P, Pattichis M S. Robust Multispectral Image Registration Using Mutual-Information Models[J]. IEEE Transaction on Geoscience and Remote Sensing, 2007, 45(5): 1494-1505

[3] Anthony A, Loffeld O. Image Registration Using a Combination of Mutual Information and Spatial Information[C]// IEEE International Conference on Geoscience and Remote Sensing Symposium. Colorado, U. S. A, 2006: 4012-4016

[4] Yu Le, Zhang Deng-rong, Holden E-J. A Fast and Fully Automatic Registration Approach Based on Point[J]. Computers & Geosciences, 2008, 34(7): 838-848

[5] Zhang Jun. A Study on Automated Image Registration Based on Straight Line Features[J]. 2009 Urban Remote Sensing Joint Event, 2009: 1-6

[6] Eastman R D, Moigne J L, Netanyahu N S. Research issues in image registration for remote sensing[C]// IEEE Conference on Computer Vision and Pattern Recognition. Minneapolis, MN, USA, 2007: 1-8

[7] Wen Gong-jian, Lv Jin-jian, Yu Wen-xian. A High-Performance Feature-Matching Method for Image Registration by Combining Spatial and Similarity Information[J]. IEEE Transactions on Geoscience and Remote Sensing, 2008, 46(4): 1266-1277

[8] Lin Hui, Du Pei-jun, Zhao Wei-chang, et al. Huasheng Sun. Image Registration Based on Corner Detection And Affine Transformation[C]// 3rd International Congress on Image and Signal Processing(CISP). 2010, 5: 2184-2188

[9] 夏德深，傅德胜. 计算机图像处理及应用[M]. 南京：东南大学出版社，2004

[10] Lowe D G. Distinctive image features from scale2invariant keypoints[J]. International Journal of Computer Vision, 2004, 60(2): 91-110

[11] 李志华，陈耀武. 基于多摄像头的目标连续跟踪[J]. 电子测量与仪器学报，2009, 23(2): 46-51

[12] 乔警卫，胡少兴. 三维重建中特征点提取与匹配算法研究[J]. 系统仿真学报，2008, 20: 400-403

[13] 李云霞，曾毅，钟瑞艳，等. 基于 SIFT 特征匹配的图像拼接算法[J]. 计算机技术与发展，2009, 19(1): 43-52

[14] 胡明昊，任明武，杨静宇. 一种快速实用的特征点匹配算法[J]. 计算机工程，2004, 30(9): 31-33

[15] 张迁，刘政凯，庞彦伟，等. 基于 SUSAN 算法的航空影像的自动配准[J]. 测绘学报，2003, 32(3): 245-250

[16] 刘贵喜，刘冬梅，刘凤鹏，等. 一种稳健的特征点配准算法[J]. 光学学报，2008, 28(3): 454-461

[17] 中国资源卫星应用中心[EB/OL]. http://www.cresda.com/cn/. 2011.6

(上接第 60 页)

验平台的具体步骤如下。

1) 完成硬件描述语言(如 Verilog, VHDL 等语言)对 DES 加密算法的描述，并编写合适的测试激励函数。

2) 经 Modelsim 逻辑仿真，验证正确后，在相应测试点设置测试激励函数，生成所关心信号量的 VCD(Value Change Dump)文件。VCD 文件实质上是记录了相应时间测试点功耗波形的二进制形式的文件。

3) 通过 Visual C++语言编程处理 VCD 文件，描绘出 DES 加密算法功耗攻击波形曲线。

4) 采用 DPA 攻击方法和穷举法得到 DES 加密算法的密钥。

图 3 所示的是 DES 加密算法在 3000 条明文下对第一轮的子密钥进行 DPA 攻击成功的波形。

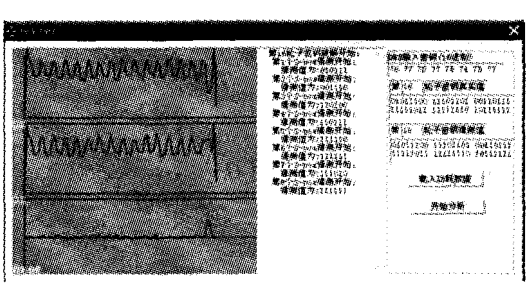


图 3 DPA 攻击成功

结束语 差分功耗分析(DPA)攻击不同于常规的针对加密算法的穷举攻击策略，其原理设计巧妙，攻击设备虽贵但易于软件仿真实现。本文建立了 DES 加密过程的 DPA 攻击仿真平台，利用该仿真平台，在没有复杂测试设备与测试手段的情况下分析了 DES 加密算法在面临 DPA 攻击时的脆弱性，从而为 DES 算法的理论研究与设计工作者提供了有益的参考价值。

参 考 文 献

[1] Data Encryption Standard. Federal Information Processing Standard(FIPS) Publication 46, National Bureau of Standards[S]. US Department of Commerce, Washington DC, 1977

[2] Kocher P, Jaffe J, Jun B. Differential Power Analysis[C]// Proceedings of Advances in Cryptology-CRYPTO99. Springer-Verlag, 1999: 388-397

[3] Alioto M, Poli M. A general model for differential power analysis attacks to static logic circuit s[C]// PPISCAS 2008. Piscataway, NJ: IEEE, 2008: 3346-3349

[4] 李浪，李仁发，童元满，等. 嵌入式加密芯片功耗分析攻击与防御研究进展[J]. 计算机研究与发展，2010, 47(4): 595-604

[5] 陈开颜，赵强，褚杰，等. 差分功耗分析单片机 DES 加密实现的旁路攻击[J]. 计算机科学，2007, 34(11): 20-22

[6] Rabaey J M. Digital Integrated Circuits[M]. Englewood Cliffs, NJ: Prentice-Hall, 1996