Computer Science and Application 计算机科学与应用, 2018, 8(5), 757-762
Published Online May 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.85084

Hans汉斯

On the Digital Forensics of the UAV's Illegal Operations

Yanheng Li*, Liping Teng, Jingran Zhang

Jiangsu Police Institute, Nanjing Jiangsu
Email: *1070543256@qq.com

Received: May 4th, 2018; accepted: May 22nd, 2018; published: May 29th, 2018

Abstract

Recently, with the development of civilian drones, not only it is convenient for our daily life, but also it has been a new tool for crimes. Due to their low cost, some criminals began to make use of them to do drug smuggling, spy on another's privacy, and disturb public wireless services and so on. Besides, after the accidents or incidents, some effective measures and solutions are urgently needed. Moreover, it is difficult to do the UAV's digital forensic, for example, the difficulty to identify the manipulators and the lack of norms to save the operation logs. So, it is necessary to strengthen the management of the log retention's legislation and regulation and to improve its forensics steps. And also, it is essential to determine the identity of the manipulators by digital and traditional forensics and to look into the recovery and analysis of the important flight data storage.

Keywords

The UAV, Digital Forensic, Safety Management, Data Recovery

无人机非法操作的电子取证

李延蘅*，滕丽萍，张井然

江苏警官学院，江苏 南京
Email: *1070543256@qq.com

收稿日期：2018年5月4日；录用日期：2018年5月22日；发布日期：2018年5月29日

摘 要

近几年民用无人机快速发展，方便了我们的日常生活，同时也为犯罪分子提供了新的作案工具。一些人

*通讯作者。

文章引用: 李延蘅, 滕丽萍, 张井然. 无人机非法操作的电子取证[J]. 计算机科学与应用, 2018, 8(5): 757-762.
DOI: 10.12677/csa.2018.85084

开始使用低成本无人机从事非法活动，使用无人机运送毒品、窥探他人隐私，干扰公共服务等等。无人机发生意外事故或安全事件后还缺乏有效的调查方式和方法。无人机电子取证面临一些困难，操纵者身份认证判定难，无人机操作日志(Vlog)保存缺乏规范，等等。需要加强日志留存立法、规范管理，进一步完善无人机取证步骤，电子取证和传统取证相结合判定操纵者身份，研究重要飞行数据存储恢复与分析。

关键词

无人机，电子取证，安全管理，数据恢复

1. 引言

无人机是无人驾驶飞机的简称(UAV, Unmanned Aerial Vehicle)，是利用无线电遥控设备和自备的程序控制装置的不载人飞机。据统计，2015 年，我国无人机销量约 9 万架，消费级无人机产品销售规模达到 23.3 亿元。预测显示到 2018 年，我国民用无人机市场规模将达到 110.9 亿元，到 2020 年，年销量预计达到 65 万架，呈现井喷式增长。虽然无人机已经在全球范围内展现出极高的发展潜力，但是它也在全世界造成了许多上至国家安全，下至个人隐私的事故，无人机侵入军事地域、干扰军用飞行器正常飞行、航拍“偷窥”国防设施、泄露国防机密等事件不断增多。

非法无人机飞行活动已经引起了执法部门的注意。2015 年，美国边防巡逻队在加州缉拿了两名利用无人机运输 25 斤海洛因的犯罪分子；同年又在亚利桑那州揪出了另一处利用无人机运输毒品的犯罪团伙。2016 年，英国警方收到了 3456 起无人机相关事件的报警——较 2015 年上升了 3 倍，而较 2014 年上升了 12 倍，相当于每一天英国警察都会收到至少 10 起无人机相关投诉。而这些无人机的出警事件有大有小，有些只是邻里无人机的飞行范围问题，而有的却是利用无人机运输毒品和枪支。非法无人机飞行活动向监狱偷运的不仅仅是毒品，还有手机、刀、手机 SIM 卡、USB 驱动器以及 DVD 播放器等其他违禁品，国内发生多起无人机非法飞行，造成民航机场航班不能正常起降。从民众安全的角度看，对无人机进行执法也非常必要。在足球比赛、大型音乐会等大型活动中，就常常会出现无人机的身影。比如在 2016 年西雅图的一次游行中，一名女性就被无人机砸中致伤。关于无人机的取证变得越来越重要。

2. 无人机取证现状

无人机犯罪属于高科技犯罪，相应的管控需要从事前预防、事中干预及事后调查三方面入手。在事前预防上无人机电子围栏与无人机云系统采用高科技手段实现无人机飞行计划管理、飞行状态监控及重点空域管控。无人机反制手段(包括阻断干扰和物理反制)是事中干预的有力手段。

无人机取证属于事后调查，需要结合传统计算机取证(文件系统取证、图像取证等)和移动设备取证等多种技术，乃至处理传统物证(痕迹、指纹、毛发)等多种手段展开。针对无人机的电子证据包括三种：物理证据、电子数据和传统证据。其中无人机的电子数据是无人机取证的重点，通过分析无人机的数据流，结合事前预防、事中干预的相关工作，收集相关证据，使无人机的事后调查管控流程化、一体化。

在取证技术上，瑞典 MSAB 公司率先将无人机取证结合到了其手机取证软件 XRY 中。以色列著名

的 Cellebrite 公司生产的新一代、高性能的手机司法取证设备 UFED Touch Ultimate 具有无人机数据获取功能，同时使用 PA 解析软件可以分析得到某些型号无人机的起点和终点，通过地图分析功能可以清晰地看到嫌疑人的窝藏地点[1]。具有支持文件和物理提取、支持大容量存储(内部存储 SD 卡，提取无人驾驶飞行旅程)等特点，提取资料的类型包括图像、视频、位置和其他详细信息(取决于解码)。在国内厦门美亚柏科公司的手机取证系列软件已增加对大疆旗下主流型号无人机的取证支持。

3. 无人机违法违规操作电子取证思路

无人机取证不同于常规电子取证，涉及多种取证手段，应具有多变的取证思路。

1) 全面针对无人机数据流获取电子证据

飞行的无人机只是整个电子证据数据流的一部分。这个数据流包括智能手机、控制器以及传感器等外围设备，通过外围设备收集 GPS 定位数据、视频图像。而通过对视频数据进行分析，还能够确定无人机的位置信息等等。调查人员在获得无人机或是其组件后，对其中的信息进行提取。在飞行过程中遥控器将控制指令发送给无人机，遥控器接收无人机传输的飞行数据和图像信号后通过 USB 数据线传输至手机；同时，由于手机还承担了通过移动网络与无人机服务器连接的功能，从这个控制逻辑分析，手机上是保存了所有飞行数据的，所以，无人机取证的需求首先可以明确为对手机控制 App 的取证，其次对整个数据流的每一部分进行有效电子证据的获取。

2) 无人机出厂进行身份认证及飞行记录设置

无人机制造商可帮助调查人员，比如有的无人机系统会将用户飞行控制应用程序的登录名和密码未经加密注入无人机设备，这意味调查人员可以轻松获取相关操纵者的登录名和密码，从而检查用户的飞行视频和飞行记录。也就是说，只要在犯罪现场找到无人机，即便没有抓到操纵者，也能够提取到相关信息。

除此之外，厂商出于质量跟踪和合法性要求，一般会在设计时对消费级无人机加入飞行数据记录器(Flight Data Recorder)功能，便于在飞机坠落或损坏后及时排查原因，或用于无人机调试使用，所以，无人机取证的另一个切入点是无人机自带的飞行记录器。通过对.dat 文件进行数据转换，获取日志文件无人机的飞行状态及各传感器的数值记录。通过对经纬度数值的获取可找到该次飞行起飞地点的准确位置[2]。

3) 无人机通讯及飞行数据截取

无人机控制模块采用的日志系统写入速率低，在通信过程中采用串口接收遥控数据包和飞控的数据包。超声波和激光模块与单片微型计算机(Micro controller Unit, MCU)采用串口通信。利用数据截取技术对无人机通讯及飞行数据截取，采用网络监听和电磁波捕获两种方式截取有效信息，见图 1 [3]。

4. 无人机违法违规操作取证难点

由于涉及的技术含量高，要查明事实、有效对无人机违法违规操作取证存在以下难点：

1) 无人机操纵者身份认证判定困难

由于无人机往往都是远程控制的，且无人机低成本的属性使之在必要时候可以丢弃，所以在将无人机与操纵者相关联时具有一定的困难。在发现无人机违规违法操作后，通常会有三种可能：a) 无法确定无人机操纵者。b) 只找到了无人机的一些碎片。c) 仅仅怀疑某人非法操纵，但却没有找到无人机。

在捕获违规操作的无人机后，需要通过查找现场及无人机的线索来对操作者进行关联，而无人机操作者的身份锁定需要通过对无人机的电子取证和传统取证手段相结合。

2) 调取无人机操作日志困难

在确定无人机操纵者的身份时，需明确嫌疑人使用过无人机进行非法活动。无人机的操作日志调取

是无人机电子取证分析的主要内容，通过操作日志追溯违规操作的范围和时间等信息。

一方面，一些无人机没有保存飞行日志；另一方面，无人机操纵者可以通过一些简单的技巧来隐匿无人机的飞行轨迹。通过关闭某些手机设置来屏蔽无人机写入飞行日志。此外通过简单手段可以修改操纵者的位置，无人机操纵者很容易隐匿其行踪。仅仅是利用锡箔纸在无人机的 GPS 天线周围制作了一个法拉第笼，就能够避免无人机写入飞行日志[4]。

5. 针对现阶段无人机电子取证的建议

1) 无人机取证工作步骤完善

无人机取证工作的步骤需要进一步完善。根据美国专家 Warren G·Kruse 和 Jay G·Heiser 的观点，电子证据取证是“对计算机介质进行保存、鉴定、提取、归档及阐释，以作为证据和/或进行根本原因分析”。针对无人机违规违法操作的电子取证，应将对不同取证元素组织到一个逻辑流程中，保证公正、客观、全面，将常规电子取证手段根据无人机云台及旋翼无人机的特点发展和运用，图 2 为无人机现场取证流程[5]。

应对操纵者身份认证判定难，在现场取证过程中，要及时发现生物检材，电子取证和传统取证相结

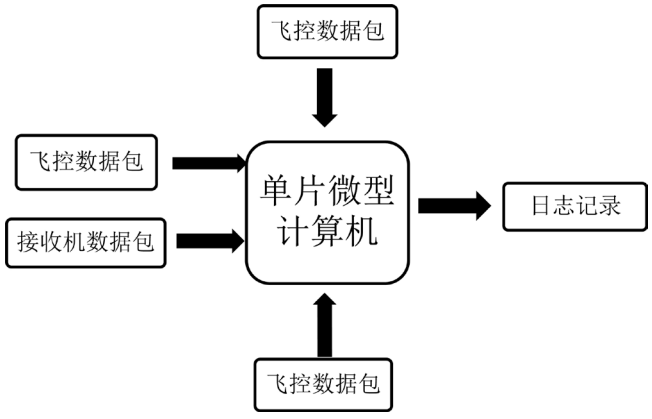

Figure 1. Diagram of MCU
图 1. MCU 框图

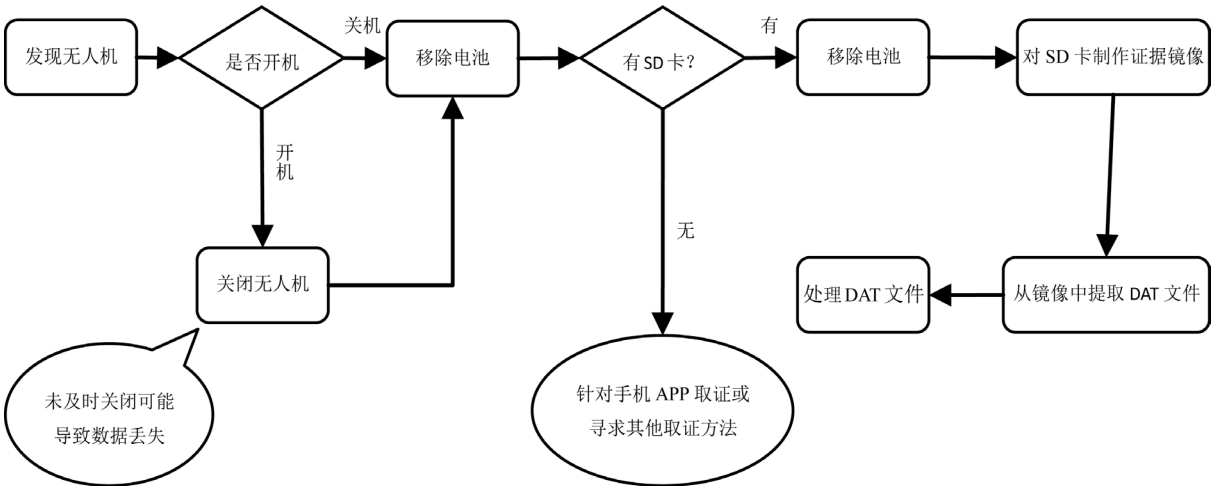

Figure 2. UAV forensics process
图 2. 无人机现场取证流程

合判定操纵者身份。

2) 无人机恶意覆盖或删除的数据恢复

在对无人机进行取证时，很有可能一些电子证据已经被破坏，无法得到完整的数据，因此必须要对这些电子证据进行复原，最大程度恢复被破坏的数据。现代科技研发的无人机系统应具备自动生成备份数据的能力，并对数据进行恢复。

在无人机违规操作中，操作者极有可能删除飞行数据、损坏存储介质导致数据丢失又或者故意坠机导致视频文件无法播放等等。大疆无人机的碎片交叉存储带来碎片定位和分离极其困难的技术问题，目前市面上尚无相应的专业恢复工具，需要电子数据取证和视频数据恢复人员合作加以研究。

大疆无人机在生成视频文件时会同时生成两个同名文件，其中一个为 MP4，一个为 MOV，这两个文件一个是用于预览的“小视频”使用高度压缩的视频(音频)编码；另一个才是真正的高清视频，一大一小两个同名文件组成一组。

由于在传输的时候一组甚至多组大小视频同时进行(理论上还是排队写入的，只是这种速度已经很快，给人感觉像是同步进行)，这个时候大小两个视频文件就产生了交叉存储也就是“碎片化”。普通恢复软件在恢复时只会查找文件头来定位文件，如果存在碎片化，那么其恢复出来的数据必定是无效的。

针对大疆无人机的数据恢复，需要分析底层视频编码结构从而开发出了碎片重组程序，实现快速定位碎片并自动分析重组功能。保证精确定位高清视频碎片，对于由于坠机导致视频无法播放的文件也可以有效修复。同时需要支持对 SD 卡、大容量硬盘，对存储介质任意创建区域及对 NTFS、FAT32、ExFAT 以及 RAW 等不同格式的扫描和对存储介质进行镜像备份的功能。查看存储介质的 HEX 值并保存“扫描结果”和“加载扫描结果”[6]。

3) 无人机的数据记录与保存

《中华人民共和国网络安全法》规定，网络运营者应当履行安全保护义务，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志。

无人机飞行日志至关重要，但是目前国内并没有留存无人机飞行日志记录的相关强制规定，参照网络安全法，有关部门应加强立法，强制要求留存飞行日志，规范管理。

6. 结束语

无人机犯罪属于高科技犯罪，电子证据是打击此类犯罪的基石。无人机的电子取证不同于传统的电子取证技术，需要结合多种类型数据，结合无人机的无人机云、无人机电子围栏及无人机反制手段进行数据的采集和分析。无人机取证的关键在于飞行日志中的飞行数据，针对数据的保存、采集、恢复、分析等工作需要技术的发展与国家立法相互配合，从而进一步加强对无人机的管控、保障公共安全和公民隐私。

项目基金

江苏省高等学校大学生实践创新训练计划一般项目(民用无人机的安全管理技术研究 2017103290934Y)；江苏高校品牌专业建设工程资助项目(Top-notch Academic Programs Project of Jiangsu Higher Education Institutions, TAPP)；江苏省教育厅项目(大数据时代社交网络用户隐私保护问题研究 2017SJB0471)；江苏警官学院教改项目(网络安全与执法专业实践教学体系及运行模式研究 2016B09)。

参考文献

[1] 太极取证. UFED 无人机获取技术——开启取证新篇章[J]. 太极公共安全, 2018(2).

[2] 无人机取证方法浅析，我们有的是方法让机器开口! [EB/OL] http://www.sohu.com/a/143937617_401311, 2017-05-27.

[3] 刘巧，吕新良，蒲路，琚泽立. 基于无人机的风电叶片巡检[J]. 电子质量, 2017.11.

[4] 全球鹰无人机飞行学院. 非法无人机越来越多警方如何调查取证? [EB/OL] http://uav.huanqiu.com/hyg/2017-08/11078261.html, 2017-08-04.

[5] 孙奕. 无人机取证，电子数据取证与鉴定[EB/OL]. http://www.sohu.com/a/164908924_505860, 2017-08-16.

[6] CHS 数据恢复实验室. 大疆无人机数据安全及恢复方法[EB/OL]. http://digital.it168.com/a2017/0817/3165/000003165153.shtml, 2017-08-17.