


Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models

Khalifa Al-Room, Zayed University, UAE

Farkhund Iqbal, Zayed University, UAE


Thar Baker, Liverpool John Moores University, UK

 <https://orcid.org/0000-0002-5166-4873>

Babar Shah, Zayed University, UAE

Benjamin Yankson, University of Ontario Institute of Technology, Canada & Sheridan College, Canada

Aine MacDermott, Liverpool John Moores University, UK

 <https://orcid.org/0000-0001-8939-4664>

Patrick C. K. Hung, University of Ontario Institute of Technology, Canada

ABSTRACT

Drones (a.k.a. unmanned aerial vehicles – UAV) have become a societal norm in our daily lives. The ability of drones capture high-quality photos from an aerial view and store and transmit such data presents a multi-facet problem. These actions possess privacy challenges to innocent users who can be spied on or drone owner's data which may be intercepted by a hacker. With all technological paradigms, utilities can be misused, and this is an increasing occurrence with drones. As a result, it is imperative to develop a novel methodological approach for the digital forensic analysis of a seized drone. This paper investigates six brands of drones commonly used in criminal activities and extracts forensically relevant data such as location information, captured images and videos, drones' flight paths, and data related to the ownership of the confiscated drone. The experimental results indicate that drone forensics would facilitate law enforcement in collecting significant information necessary for criminal investigations.

KEYWORDS

Bebob Parrot, DJI Phantom3, DJI Phantom4, Drones, Forensic.Syma x5c, Xiang Yu

1. INTRODUCTION

Recently there has been a rapid growth in the interest of UAV technology. Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, are aircraft with no pilots that can be controlled either remotely or autonomously based on a pre-programmed flight path. Due to the varied uses in civil life, the technology once reserved for military use has evolved greatly. Such uses include area

DOI: 10.4018/IJDCF.2021010101

This article, published as an Open Access article on February 4, 2021 in the gold Open Access journal, International Journal of Digital Crime and Forensics (IJDCF) (converted to gold Open Access January 1, 2021), is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

surveillance, inspection, surveying, unarmed cargo, and aerial photography. As airspace becomes more congested, the risk of collisions increases. Safeguards against drone incidents are likely to be considerably more challenging than for conventional aircraft. This increased congestion can result in high levels of signal interference, and hence generating unreliable and intermittent data and control-streams. In controlled airspace, drones create new challenges for the interactions between pilots and air traffic controllers (Matyszozyk, 2016).

Drones are becoming a popular thing to see in shared use space or whenever visiting public events. To most people, a drone is one of two very different types of pilotless aircraft: a toy, or a weapon. It is either a small insect-like device flying around in parks or on beaches or a large aircraft spying on civilians equipped with a weapon. The first category '*recreational drones*' is aimed at consumers. There were around two million items sold around the world in 2014, and this is increasing swiftly (Clarke & Moses, 2014). The second category, '*military drones*', accounts for nearly 90% of the worldwide sales of drones (Clarke & Moses, 2014).

The DJI Phantom 4, is one of the most popular drones on the market. The DJI Phantom 4 weighs 3 pounds in total and can fly at least 4 miles away from its operator without losing its video stream or remote controls. While the Phantom can carry just over 1 pound while in flight, its beefier brother, the DJI S900, has a maximum payload of just under 7 pounds. Anyone looking to spend about \$2000 dollars to purchase one can likely fly over a prison yard, and deliver a sizeable illicit contraband package to their friends on the inside (Fox News, 2017). Drones allow their users to accomplish certain tasks such as taking in aerial views, or hard to access spaces; which in the past has proven difficult due to physical restriction or barrier. The main motivation behind using drones in this manner is to explore a new way of gaining access to uncharted environments to capture (filming or taking pictures) or deploy resources.

The unique features of drone application are its' capacity to be deployed almost anywhere (in theory) to conduct reconnaissance, retrieve data or resources, deploy resources, and its flexibility in carrying different payloads. These functionalities explain why different agencies and organizations have looked towards implementing the use of drones within their services. For example, the American Red Cross is looking toward using drones in their search and rescue missions (McFarland, 2015; Preston, 2015). In the state of Virginia (USA), fire departments are considering the use of drones in the essence of spotting emerging fire and locating lost tourists (Preston, 2015).

With the ability to reach places that cannot be accessed physically, and in a stealthy manner, the drone can be used to perform criminal activities for reconnaissance. For example, an enemy military intelligence can use drones to take pictures of sensitive local territories. Someone could use a drone to violate the privacy of other people by taking pictures of their own home backyard. On January 26th in 2015, a drone crashed on the White House lawn but the incident was ruled as an accident (Sanchez, 2015). This incident highlighted a clear vulnerability that a terrorist could have used the function of the drone, such as a camera to breach privacy. The matter is not only limited to the camera being used but also the drone could have been carrying a payload to commit the malicious act on the White House grounds. Such notable issues for the US government is drug smuggling using drones is an issue for the American and Mexican border since 2010 (Sanchez, 2015).

Several law enforcement agencies across the globe have identified the drone as the go-to machinery to infiltrate jails and drop contrabands. Small commercial drones are being used to lift packages containing illicit goods such as guns, to synthetic drugs into jails in Canada, USA, Russia, Australia, Greece, and England; where they threaten the security of the jail (Milmo, 2015) (Fox News, 2017). Recorded incidents include a 2011 incident where staff at a Moscow prison confiscated 700 grams of heroin dropped by a drone. In 2016, a riot broke out over a package dropped by a drone at Mansfield Correctional Institution (a prison in the state of Ohio, USA). The same year a drone was discovered dropping mobile phones, drugs, hacksaw blades, and other materials into a prison in the state of Oklahoma. The threat of drones is not just limited to prisons; countries across the globe are

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/drone-forensics/267147

Related Content

Tracing Cyber Crimes with a Privacy-Enabled Forensic Profiling System

Pallavi Kahai, Kamesh Namuduri and Ravi Pense (2006). *Digital Crime and Forensic Science in Cyberspace* (pp. 137-154).

www.irma-international.org/chapter/tracing-cyber-crimes-privacy-enabled/8353

CBC-Based Synthetic Speech Detection

Jichen Yang, Qianhua He, Yongjian Hu and Weiqiang Pan (2019). *International Journal of Digital Crime and Forensics* (pp. 63-74).

www.irma-international.org/article/cbc-based-synthetic-speech-detection/223942

E-Government, Security, and Cyber-Privacy: Individual Rights versus Government Responsibility

Ross Wolf and Ronnie Korosec (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1314-1327).

www.irma-international.org/chapter/government-security-cyber-privacy/61011

Lane Detection Algorithm Based on Road Structure and Extended Kalman Filter

Jinsheng Xiao, Wenxin Xiong, Yuan Yao, Liang Li and Reinhard Klette (2020). *International Journal of Digital Crime and Forensics* (pp. 1-20).

www.irma-international.org/article/lane-detection-algorithm-based-on-road-structure-and-extended-kalman-filter/246835

An Improved Fingerprinting Algorithm for Detection of Video Frame Duplication Forgery

Yongjian Hu, Chang-Tsun Li, Yufei Wang and Bei-Bei Liu (2012). *International Journal of Digital Crime and Forensics* (pp. 20-32).

www.irma-international.org/article/improved-fingerprinting-algorithm-detection-video/72322