A Zero-Cost Solution for Remote Identification and Tracking of sUAS in Low Altitude Flights

A Ford Motor Company Whitepaper

Adi Singh, James Carthew, Weifeng Xiong

We discuss here the urgent relevance of remote identification, and key factors that should be considered while devising a system to achieve it. In addition, we propose a technical solution based on visible light communication (VLC) developed at Ford Research & Innovation Center for universally identifying sUAS in low altitude flights. Merits of the approach are subsequently discussed as we attempt to strike balance between acceptable levels of intrusiveness and effectiveness of an identification framework.

1. The Need for Universal Actor Identification

Despite government attempts at regulating the operation of small Unmanned Aircraft Systems (sUAS or drones) through 14 CFR Part 107[1], there remains debate on how effective the rule has been in improving the safety of citizens and infrastructure impacted by the use of drones. Given how ubiquitous sUAS technology has become in the US over the last decade, a robust framework of operator and device identification could be the cornerstone of an effective regulatory scheme.

With the FAA forecasting almost 4 million sUAS occupying US airspace by 2021[2], it is becoming increasingly important that we have the ability to remotely identity drones in operation and report their misuse.

1.1 Ground Transportation Model

Considering (1) the ease and cost at which drones can be acquired, (2) how little training is required to operate them, and (3) the scalability of their manufacturing processes, Ford views sUAS more as aerial extensions of ground-based vehicles than smaller versions of traditional aircrafts, and as such, finds it appropriate to explore ground transportation frameworks as models for a remote identification and tracking system for drones.

In ground traffic enforcement, the notion of accountability is derived by relating a vehicle to its owner through a combination of DMV registration and license plates. All street-legal vehicles are required to display their license plates in a manner that they can be unmistakably discerned from a minimum threshold distance, enabling anyone within vicinity of the vehicle to identify and

[1] Department of Transportation, 2016. Operation and Certification of Small Unmanned Aircraft Systems. Federal Aviation Administration. Available at: https://www.faa.gov/uas/media/RIN_2120-AJ60_Clean_Signed.pdf [Accessed May 2017].

[2] Department of Transportation, 2017. FAA Aerospace Forecast, Fiscal Years 2017-2037, pp.31-32. Federal Aviation Administration. Available at: https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2017-37_FAA_Aerospace_Forecast.pdf [Accessed September 2017].

report it to law enforcement. Officials with relevant clearance can then access DMV databases to trace the corresponding vehicle's registration, and obtain the details of the person responsible for operating the vehicle.

1.2 Analogous Criterion for Drones

This model produces two salient implications central to traffic safety:

1. the possibility of being tracked down by authorities once the vehicle's *publicly visible* license plate has been noted deters drivers from breaking the law, and
2. the ability of *any and all civilians* to note and report a vehicle's license plate assuages public anxiety over rogue operations.

There is comfort knowing that violations of one's safety would not go without the offender being held accountable; an idea that is enabled by universal identification and should be inherent to any version of sUAS ID and tracking.

Thus, a system parallel to road vehicles that combines a registration database with publicly discernible "license plates" can be effective in not only tracking the operations of sUAS, but also in addressing concomitant issues like social acceptance and hit-and-run scenarios. The underlying element in both being a method that allows anyone – law enforcement and civilians alike – within reasonable range of a drone to obtain its identifier without needing special equipment[3].

It should be clarified here that the nature of drone flights – their remoteness of operation, their much smaller footprint, their agility in 3D space – precludes the use of a conventional license plate system for identification and tracking. Therefore, the precise technical solution suitable for remote identification of sUAS will undoubtedly be different from what is used for ground-based transportation, but the guiding principles of the solution to achieve it ought still be equivalent across both domains.

2. The Interests of Operators

While the need for remote identification is imminent, and Ford supports the sentiment behind sUAS tracking, the approach to achieve it must take measures to safeguard the interests of operators.

2.1 Operator Privacy

For a tracking solution to be compelling and successful, it should never convey the impression of requiring owners to plug their devices into an authoritarian system which constantly monitors every detail of their operation, as ordinary network-based passive logging setups would. Public misgivings about mass surveillance have shown to fuel distrust in government efforts, lead to

[3] With over 77% Americans now owning a smartphone (Pew Research Center, 2017), it is fair to argue that these devices are not "special equipment", but rather, common tools of everyday life, especially when their use does not rely on any aftermarket accessories.

widespread reduction in use of a technology, and encourage end-users to find loopholes that protect their privacy[4].

An effective ID and tracking system should discourage only the misuse of a technology, not its legitimate use. We should be cautious of an overregulated system that does not protect the interests of sUAS users, as it could discourage mass compliance with identification requirements.

2.2 Operator Safety

Furthermore, universal identification of devices should not be conflated with universal determination of the owners' personal details. Only authorized government agencies should be able to retrieve an operator's contact information based on a given device's identifier. Private information of owners and operators should not be available to the public without a traceable process that first evaluates the need to access such data.

This would prevent situations where citizens concerned about drone flights – justifiably or otherwise – take matters into their own hands, and directly confront a drone operator without proper mediation by law enforcement; an unnecessary and potentially unsafe scenario for all involved parties.

3. A Localized Software Framework with Tiered Information Access

A practical solution must thus strike a healthy balance between identifying sUAS and protecting their operators' interests. We believe a localized visual range system with tiered access to personally identifiable information (PII) achieves the aforementioned policy objectives. The following sections analyze the features of one such system implemented by Ford, which uses the anti-collision lights on a drone to broadcast its unique 10-digit FAA registration number as visually discernable serialized blinks. A technical overview of the solution is presented in Appendix A.

3.1 Backward Compatible Software

An approach that relays information through existing components saves on the already limited space onboard a sUAS, and continues to maintain flight time, battery life and weight distribution characteristics of the equipment. System performance is not compromised as signal modulation for controlling LED blinks is a trivial software task, and operators need not worry about diverting any serious resources from their processor to fulfill legal requirements. Besides, such concepts do not require the installation of supplementary identification accessories, saving sUAS owners from being cost disadvantaged for compliance with the framework.

Furthermore, a solution based entirely on software updates greatly eases distribution. Ford's implementation can be shared as a free open-source library that could function as either (1) a stand-alone GPIO controller for OEMs to add to their proprietary software, or (2) an integration

[4] A 2015 study by Pew Research Center found that public disclosure of the PRISM program was followed by 34% of respondents taking steps to hide or shield their information from the government (Americans' Privacy Strategies Post-Snowden, 2015).

into popular GCS suites like *Mission Planner* or *QGroundControl* for hobbyists and hackers to complete during setup[5]. Any patches to the library arising from bug fixes or policy changes can be similarly made available. Having the capacity to distribute the solution to all users instantaneously and free of cost means the technology can be feasibly adopted across the US *within hours to days of its release*.

3.2 Visible Spectrum Broadcast

A key advantage of signals transmitted in the visible spectrum is that the system continues to function in areas lacking reliable radio or satellite connectivity. Serialized blinks broadcasted by the sUAS can be captured by any consumer-grade camera, and the video feed can be post-processed for decoding the identifier without much overhead.

Simultaneously, the same feed that identifies a drone can be used as visual evidence for determining its alleged misuse. At a psychological level, the addition of flashing lights broadcasting an identifier thus serves as a constant reminder to the operator that they are responsible for their actions, and that they could be easily tracked by law enforcement in the event of any misuse.

Although ambient light noise arising from sunlight, object reflections or complicated sceneries could obfuscate a visual light broadcast, it must be clarified that these signals are not meant to be interpreted by the naked eye. Unlike convention car plates, the remote identification signals are designed to be read by trained computer vision software, and post-processing algorithms can be robustly coached to handle edge-cases and anomalies in light conditions[6].

Figure 1: *Multiple lighting apparatus being tested for optimizing VLC broadcasts.*

3.3 Range Limitation

The algorithms developed at Ford have been able to reliably identify drones from up to 80 feet using an unmodified phone camera in daytime operational environments. With optical zoom lenses, like those on standard DSLR cameras, this range can be further extended by 12-20x depending on the magnification and sensor equipment. Identification capability at even greater distances, although possible, is conceivably unnecessary.

It is when a drone is within immediate vicinity of someone that it becomes a perceived threat to one's privacy and security; a barely visible speck flying a mile away does not sound alarm bells for the common layperson. Reliable methods to identify drones at short-range will prove to be most useful for the general public.

VLC-based methods additionally protect operator privacy, allowing their equipment to be recognized only when actively monitored within a reasonable range of direct sight. The localized

[5] See Appendix A, Figure 6 for a screenshot of sample UI integration for ground control stations.

[6] Appendix A, Section 3 provides an overview of the process we applied for training identification algorithms.

nature of these methods allow people to spot and report potentially threatening devices around them, but restrict them from monitoring all sUAS operations across the board needlessly.

This is analogous to principles applied for identifying cars via license plates today. Even though the reckless use of automobiles can arguably cause harm to people and property, we do not mandate all drivers to plug in their cars into a central system which continuously monitors their location and operation. Logistical difficulties apart, a universal passive logging system potentially breaches the privacy of drivers..

Figure 2: *Capturing and decoding a drone's identifier with a standard smartphone camera.*

3.4 Tiered PII Access

Finally, regardless of the transmission technology used, only entities with predetermined jurisdiction should be able to trace the contact details of an owner or operator given a sUAS identifier. For the public to feel safe, it must be assured that individuals can report incidents with

information that holds offenders accountable. But for law abiding drone operators to feel safe, they must be assured that only unbiased third-parties with legal authority would confront them about complaints.

A tiered-access information system would cater to these conditions, and allow law enforcement to become a valuable buffer between sUAS users and the portion of society that feels anxious about civilian drone operations.

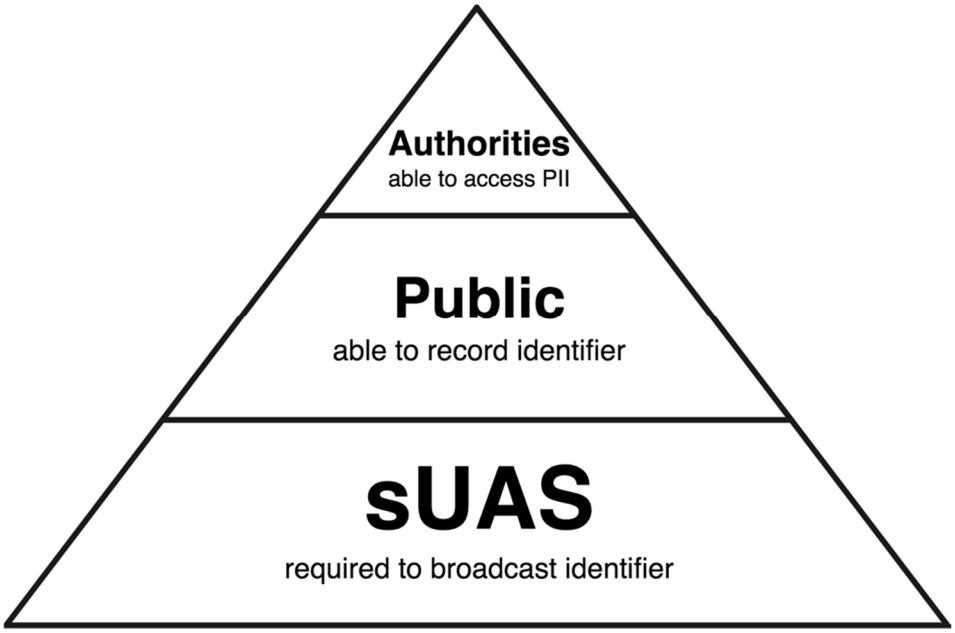

Figure 3: *A balance catering to the interests of law enforcement, drone operators and the general public.*

4. Categories of Implementation

4.1 Expanded Operations

The framework thus described enables identification and tracking within the general vicinity of a drone, but it is entirely foreseeable for law enforcement to be interested in more comprehensive information about a sUAS under special circumstances, like flights in restricted airspace or for equipment transporting unusual payloads. For such expanded operations, the equipment can be required to comply with additional, more rigorous identification technology that transmits over longer ranges, perhaps even to BVLOS receivers. Alternatives like C2, wireless or other networked solutions can be used as secondary equipment to satisfy these more rigorous standards.

We adopt this approach because requiring such rigor off hobbyists and consumers conducting basic operations could lead to mass non-compliance with rules; a scenario counterproductive to the objectives of an identification framework. Make the rules too difficult or too expensive to adopt, and individuals might rather take their chances with flying without ID equipment and abandoning their drone if caught.

4.2 Exemptions

Moreover, in the spirit of building upon existing policies, the tiniest of drones with barely enough capacity to accommodate a motor controller should be exempt from identification requirements. This understanding is already inherent in existing FAA rules that exempt registration for sUAS

lighter than 250 grams[7]. Since the unique identifier being transmitted *is* the FAA registration number, any drone exempt from registration must also be exempt from identification for consistency within the framework.

This must, however, be the only exemption allowed by the system. Further exceptions based on operational classes or subcases can lead down a slippery slope where the differences between non-compliant drones and exempted drones would not be immediately obvious, delaying response time for genuine security threats. To avoid such scenarios, any sUAS weighing above 250 grams – hobby or otherwise – that operates in US airspace should come under the purview of a unified registration, identification and tracking framework.

Requirement / Category	Transmit Identifier	Localized Visual Range	Secondary / Long Range
Under 250 grams	✘	✘	✘
Over 250 grams	✔	✔	✘
Expanded operations	✔	✔	✔

Figure 4: *Requirement buckets for implementing a unified sUAS operating framework.*

Ford's VLC solution, built upon the existing safety subsystem of sUAS beacon lights, has the potential to make our skies *safer* by improving equipment visibility and *more secure* by providing a dependable aerial version of a car license plate.

[7] This categorization can be revisited at some point in the future if drone technology is found to follow Moore's Law (Gordon Moore, 1965). Presently, however, these drones have very short flight times and very little payload capacities, rendering their threat potential negligible.

Appendix A

1. Technology Concept

The American Standard Code for Information Interchange (ASCII) is an encoding standard for electronic communication that assigns a numerical value to the most commonly used characters[8]. A collection of ASCII characters can thereby be expressed as a continuous sequence of numbers. Representing this sequence in base2 binary allows for the transmission of data over any medium that can be modulated between 2 states.

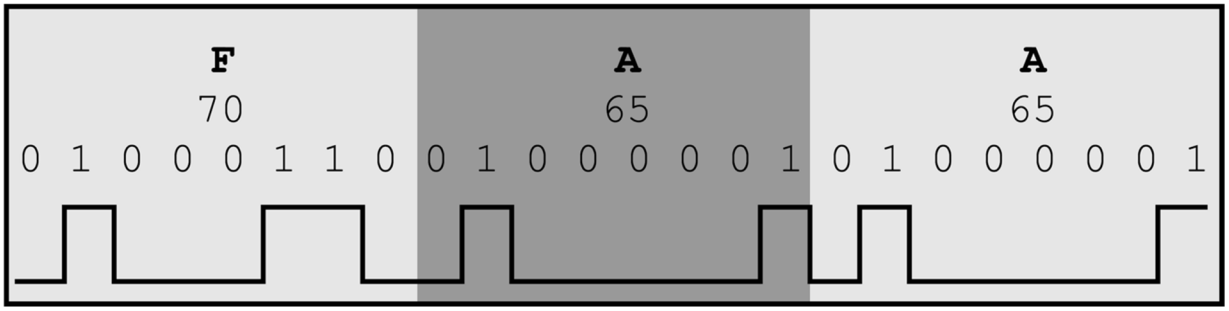

Figure 5: *The alphabet sequence "FAA" translated to an ASCII-based square wave.*

We propose a solution based on Visible Light Communication that makes use of bright anti-collision lights onboard a sUAS to broadcast the device's unique 10-digit FAA registration number. This identifier is beamed as an ASCII-to-binary signal at a preset baud synchronized across the framework for universal decoding compatibility. In its simplest implementation, this baud rate can be dictated by the frame rate[9] of a standard smartphone camera. A custom application running on the smartphone would enable it to act as a ground receiver capable of capturing and interpreting the encoded ASCII signal carrying the drone's identifier.

2. Airborne Component

The onboard computer or flight controller of a sUAS will be programmed to sequence the anti-collision lights based on a given binary sequence input. The FAA identifier can then be translated to this binary sequence and uploaded to the drone during initial setup via GCS applications like DJI Go, QGroundControl or APM Planner. In the event of ownership transfer, the certificate number can be updated using the same UI setup.

An open source toolkit for encoding and decoding registration signals can be distributed via GitHub[10] to enable community inspection and contribution towards the software. The solution

[8] Internet Assigned Numbers Authority, 2013. US-ASCII Character Set. Available at: https://www.iana.org/assignments/character-sets/character-sets.xhtml [Accessed March 2017].

[9] Frame rate is of importance because the recording apparatus needs to be able to read the signal *at least* as fast as it is being transmitted, that is, at least 1 frame should be able to capture any single binary bit broadcasted.

[10] GitHub (https://github.com/) is a version control development platform that is popular within the open-source community for hosting, distributing and managing collaborative software projects.

can be provided as a stand-alone GPIO modulation library for manufacturers to embed in their proprietary software, and plugin pull-requests can be issued for integration with GCS repositories most popular amongst amateur hobbyists.

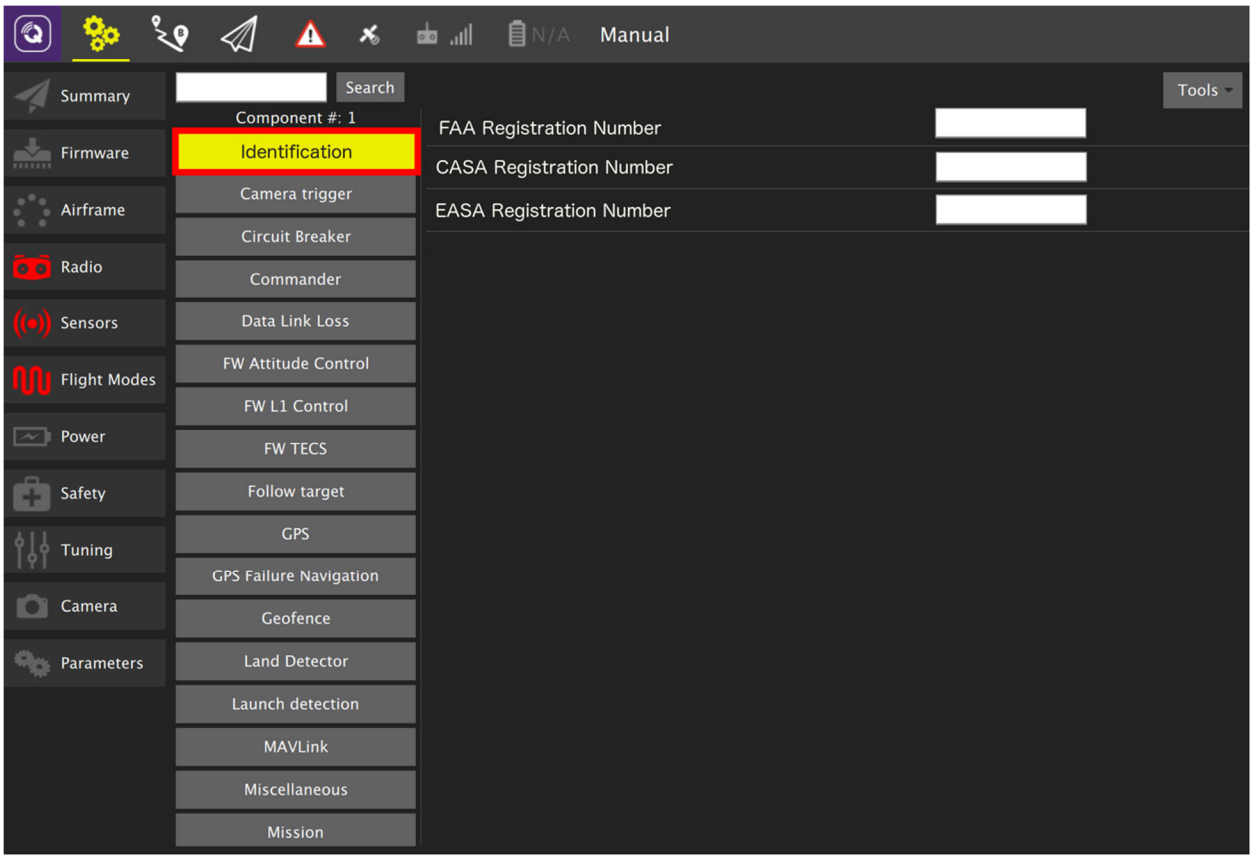

Figure 6: *Sample QGroundControl integration for uploading a registration sequence during initial setup.*

The light control software can be programmed such that the identifier signal is transmitted whenever a sUAS is armed or is in flight mode. In a more advanced implementation, the system can disable take-off entirely if the device is not set up with a valid FAA registration number prior to operation.

3. Ground Component

The ground receiver can be any apparatus capable of recording video, ranging from low fidelity mobile phones to advanced DSLR cameras. Post-processing the captured video of the sUAS allows for extraction of the device identifier. The range of reliable detection and decoding can be linearly extended with optical zoom lenses. Basic post-processing of the feed can be conducted in near real-time via an OpenCV[11] application running on the smartphone. More advanced processing for saved videos can be done in offline mode through dedicated desktop programs based on similar algorithms.

[11] An open source computer vision and machine learning software library (https://opencv.org/).

Decoding the emitted signal requires translating the pixel representation of the flashing light in each video frame to a binary digit, and eventually to ASCII characters. This is complicated by background noise, variations in outdoor natural light and the motion of a flying sUAS.

Ford has developed computer vision algorithms which enable recognition and tracking of “anti-collision light”-like features in an image. Classifiers have been developed using mature computer vision techniques that operate on specific semantics within a given pixel space. These classifiers, however, are unable to independently recognize drones of varying shapes and sizes; a prerequisite for universal implementation of the solution. This was countered by training a deep Convolutional Neural Network (CNN) with TensorFlow[12] using approximately 5000 handpicked images of drones. This approach has resulted in a more generic sUAS classifier capable of recognizing and tracking a broad range of drone form-factors, even ones that look fairly different from any image contained in the training data-set.

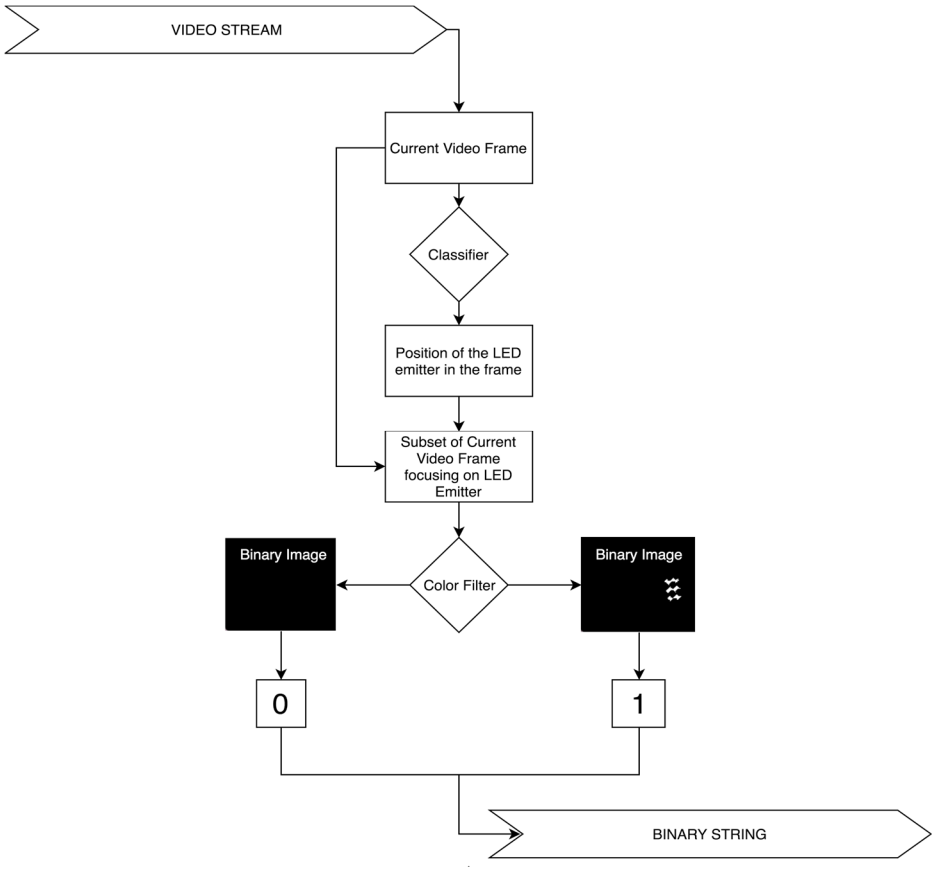

Figure 7: *Parser workflow to obtain sUAS identifier from raw video stream.*

Real-time tracking of a sUAS in successive frames then allows for the processing area to be reduced to only the section containing the drone’s anti-collision lights. Subsequent processing performed only within this area of interest – instead of the entire video frame – has shown to

[12] A software library developed by Google for machine learning applications (https://www.tensorflow.org/).

vastly reduce the likelihood of error caused by natural light and other surrounding factors in our experiments.

From there, measuring the light intensity local to the anti-collision lights gives a binary bit, and repeating this for the entire video stream provides the binary sequence representing the drone's identifier. Further pattern analysis of this sequence rejects temporal errors and duplicate readings, thus furnishing a very reliable decoding of the sUAS broadcast.

Since the system is designed to identify devices only within a relatively short visual range of the receiver, the GPS coordinates of the receiver itself provide an acceptable estimation of the drone's instantaneous location. These coordinates can be saved with their corresponding timestamp and device identifier in a central FAA database similar to the one that relates registration numbers to owner PII. Collating all coordinates for a given identifier collected from potentially multiple receivers that have captured the same broadcast can then provide the path a sUAS over time. Thus, identification *and* tracking are both achieved without the need for additional transmission and decoding overhead.

4. Database Component

Registering a sUAS with the FAA assigns a unique 10-digit alphanumeric identifier to the device, and saves it to a database (presumably under DoT purview) that relates the identifier to its owner's PII. Once a drone's identifier is supplied by the ground receiver, this database can be used by authorities to obtain the specifics of the sUAS and its owner/operator. A permission-based tiered access identification system can thus be realized.

5. Technology Readiness Level

The VLC technology underlying this solution is mature and its use has been demonstrated in a range of dynamic applications over the years[13]. The specific context of sUAS identification and tracking provides very limited published literature to reference, but the prototype developed at Ford currently stands at TRL 7[14].

Besides being tested and shown to work in an operational environment, the Unmanned Aerial Systems research group at Ford is conducting a comprehensive study on the major parameters affecting VLC in mid-air sUAS identification and their optimal operational ranges. We plan to publish the results of this study in due course.

[13] Khan, L.U., 2017. Visible light communication: Applications, architecture, standardization and research challenges. Digital Communications and Networks, 3(2), pp.78–88. Available at: http://www.sciencedirect.com/science/article/pii/S2352864816300335 [Accessed September 2017].

[14] NASA, Technology Readiness Level Definitions. Available at: https://www.nasa.gov/pdf/458490main_TRL_Definitions.pdf [Accessed May 2017].