geomatics

MDPI

Article

GNSS Metadata Integrity in Consumer Smartphones During Commercial Flights: GPS Spoofing Artifacts, JPEG Tampering Detection, and Implications for UAV Precision Agriculture

Emil-Cătălin Șchiopu, Oliviu-Mihnea Gămulescu *, Florin Grofu, Roxana-Gabriela Popa, Irina-Ramona Pecingină and Adrian Runceanu *

Faculty of Engineering, "Constantin Brancusi" University of Targu Jiu, 210185 Targu Jiu, Romania; florin.grofu@e-ucb.ro (F.G.); roxana.popa@e-ucb.ro (R.-G.P.); irina.pecingina@e-ucb.ro (I.-R.P.)
* Correspondence: oliviu.gamulescu@apia.org.ro (O.-M.G.); adrian.runceanu@e-ucb.ro (A.R.)

Highlights

What are the main findings?

- Samsung Galaxy A72 records GPS in EXIF at 100% capture rate (Timestamp Camera) at altitudes up to 11,439 m WGS84—to the authors' knowledge, among the highest EXIF altitude profiles reported in consumer mobile photography, pending a dedicated systematic review; velocity spikes (1560–1875 km/h)—one at cruise altitude, one during landing approach—are indistinguishable from GPS position-jump spoofing at the EXIF metadata level.
- Phantom geolocation is absent in flight (0/442, 0%) vs. 37.3% in terrestrial environments with the same device ($z = 13.86$, $p < 0.0001$); 88% of Samsung Galaxy A72 JPEG files lack the EOI marker, causing systematic false positives in integrity validators.

What are the implications of the main findings?

- Consumer-grade GNSS failure modes (phantom geolocation, velocity artifacts, EOI anomalies) may affect UAV precision agriculture orthophoto georeferencing and automated crop classification accuracy; this implication is plausible given the shared consumer-grade GNSS receiver class but has not been tested on UAV platforms and requires validation under UAV operational conditions, including beyond the mid-latitude European conditions studied here.
- EXIF GPS metadata validation using the proposed anti-spoofing/anti-sniffing/anti-tampering framework is recommended for EU AI Act Regulation (EU) 2024/1689 Article 10(3) data quality compliance in high-risk AI systems.

Abstract

Smartphone GNSS metadata remains an underexplored source for evaluating navigation-signal integrity in real-world conditions. We investigated GPS behavior recorded by a Samsung Galaxy A72 smartphone across two European flights (EXP03: Rome–Bucharest, n = 377; EXP10: Bucharest–Lisbon, n = 78) and 275 terrestrial reference photographs (Cabo da Roca, Portugal). A total of 730 photographs were analyzed using a seven-indicator taxonomy, conceptually inspired by Receiver Autonomous Integrity Monitoring (RAIM) principles, covering anti-spoofing, anti-sniffing, and anti-tampering checks. GPS capture rates reached 100% (Timestamp Camera) and 83.3% (native camera) up to 11,439 m WGS84, among the highest EXIF altitude profiles reported to date. Velocity spikes (1560–1875 km/h), one at cruise altitude and one during landing, were indistinguishable from GPS spoofing at the EXIF level, and their physical origin is undetermined. Phantom

Check for updates

Academic Editor: Gino Dardanelli

Received: 14 July 2026
Revised: 18 August 2026
Accepted: 20 August 2026
Published: 23 August 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

geolocation was absent in flight (0/442) versus 37.3% on the ground, consistent with GPS constellation visibility as the primary factor. In total, 88% (n = 920) of JPEG files lacked the standard EOI marker, generating false positives in integrity validators. Findings are device-specific, derived from non-independent observations, and require replication before generalizing to other GNSS receivers or latitudes. The framework offers a methodological basis for EXIF integrity analysis relevant to EU AI Act Article 10(3) data quality and UAV precision-agriculture georeferencing.

Keywords: GNSS metadata integrity; GPS spoofing detection; EXIF GPS analysis; phantom geolocation; commercial aviation GNSS; UAV precision agriculture; JPEG integrity anti-tampering; EU AI Act data quality; Samsung Galaxy A72

1. Introduction

The proliferation of consumer smartphones equipped with multi-constellation GNSS receivers has transformed geographic metadata into ubiquitous information in personal photography. GPS fields in the EXIF standard (Exchangeable Image File Format), standardized in JEITA EXIF 2.32 [1] (where JEITA denotes the Japan Electronics and Information Technology Industries Association) are increasingly used as location evidence in legal, scientific, and regulatory contexts, including in high-risk artificial intelligence systems regulated by Regulation (EU) 2024/1689 [2]. The integrity of these fields is subject to multiple failure modes that can render them misleading or factually incorrect—failure modes that, in certain cases, are undetectable by analysis of the JPEG file structure or the nominal coordinate values.

Previous studies have documented several GPS metadata failure modes in consumer mobile photography. Gămulescu [3] documented the phantom geolocation phenomenon—the silent retention of the last valid GPS fix under signal loss conditions—during a 49 min underwater episode in Tenerife (depth −30 m, tourist submarine, August 2025). The proposed mechanism postulates that the phenomenon is determined primarily by GPS signal obstruction, not by device hardware characteristics. In parallel, the EXIF metadata integrity literature has demonstrated that messaging platforms systematically strip GPS fields through compression [4], and manufacturer-introduced differences in the EXIF specification can significantly complicate forensic analysis [4].

However, a critical dimension of GNSS behavior in consumer photography remains unexplored in the literature: GPS recording during commercial aviation at cruise altitude. Wassenaar Arrangement regulations permit civilian GPS receivers to operate up to 18,000 m in altitude [5], meaning that smartphones with GPS enabled may continue to record geographic coordinates throughout the entire flight. Carroll et al. [6] tested smartphone GPS performance at extreme altitudes using a weather balloon but without photographic EXIF metadata and without integrity analysis of the resulting data. EXIF datasets from commercial flights may contain unusual altitude values and calculated velocities that raise important questions about automated GPS metadata validation systems. This issue has direct implications for UAV drones used in precision agriculture, where GNSS receivers from the same consumer class produce systematic georeferencing errors affecting automated crop classification accuracy [7].

This study addresses this gap by reporting and analyzing two commercial flight experiments: EXP03 (Rome–Bucharest, 18 April 2026, n = 377 photographs) and EXP10 (Bucharest–Lisbon, 6 February 2024, n = 78 photographs), both conducted with the same Samsung Galaxy A72 device. A security framework structured around three modules—

anti-spoofing, anti-sniffing, and anti-tampering—is applied to each dataset, with seven indicators constituting an original post-processing taxonomy conceptually inspired by RAIM principles [8]. The specific objectives are: (1) to document GPS behavior at commercial cruise altitudes in EXIF metadata; (2) to identify and characterize velocity anomalies as physical artifacts vs. spoofing signatures; (3) to analyze JPEG structural integrity for this device family; and (4) to derive implications for data quality in high-risk AI systems and in precision agriculture with UAV drones.

The remainder of this article is structured as follows: Section 2 describes materials and methods; Section 3 reports the results; Section 4 discusses the findings and limitations; Section 5 presents the conclusions.

EXIF metadata has increasingly attracted the attention of forensic researchers as a source of authentic information timestamps, GPS coordinates, and device identity. Soni et al. investigated what happens to these fields depending on the image transfer method: USB, email, WhatsApp, Telegram, Signal, Instagram, Facebook Messenger. Their conclusion is clear: direct transfers preserve EXIF integrity, while messaging platforms effectively strip metadata through compression [4]. This observation is directly relevant to the present study. This study documents a type of GPS corruption in EXIF metadata not previously addressed in the literature—not the effect of a transfer, but the behavior of the GNSS receiver under high-altitude conditions. A separate but related issue concerns manufacturer-introduced differences in the EXIF specification implementation, which can seriously complicate metadata extraction and interpretation [4]. This is precisely what we observed in the Samsung Galaxy A72 files in our dataset, where the standard EOI marker was absent in 88% of cases.

The vulnerability of civilian GNSS signals to spoofing is well-established. Their extremely low power and open structure make them an accessible target for attacks that seek to manipulate the position solution without the receiver detecting anything suspicious [9]. Humphreys et al. demonstrated that a civilian-grade portable spoofer can induce abrupt position jumps—indistinguishable, at the receiver level, from a legitimate GPS fix [10]. The problem also arises in the UAV context. Sun et al. proposed a deep learning-based method for GPS spoofing detection on small drones, achieving an F1-Score of 0.9722 [11]; Al-Sabbagh et al. went further with a stacked ensemble learning approach combining CNN with XGBoost and magnetic field data, achieving superior detection robustness [12]. All of these studies focus on real-time detection at the signal level. What the present study addresses is different: GPS anomalies identified post hoc in EXIF metadata. There, a real physical GPS re-acquisition artifact at landing looks identical to the traces of a spoofing attack—and no documented method yet exists to distinguish them.

Little has been written about how a consumer GPS receiver behaves at high altitudes. Carroll et al. attached a Google Nexus S smartphone to a weather balloon and recorded functional GPS data up to 31.2 km—above the Wassenaar threshold of 18,000 m [6]. It is an interesting experiment but was conducted without photographs, without EXIF metadata, and therefore without any information about GPS field behavior in the context of interest here. To our knowledge, no other reference in the literature addresses this type of situation prior to the present study. Lehtola et al. show that state-of-the-art smartphone receivers achieve decimeter-level accuracy, compared to a few millimeters for professional receivers [13]. The difference matters greatly when GPS metadata from photographs is used in precision agriculture or forensic analysis contexts. The present study records, to the authors' knowledge, one of the most complete EXIF datasets documenting the GPS behavior of a commercial smartphone throughout a commercial flight—from ground level up to 11,439 m WGS84.

Georeferencing accuracy is a determining factor in the quality of data produced by UAV drones in precision agriculture [14,15]. Liu et al. evaluated the GNSS-based direct UAV georeferencing method and the impact of ground control point configuration, demonstrating that direct georeferencing offers high efficiency but critically depends on the quality of received GNSS data [16]. Zhang and Kovacs conducted a systematic review of small unmanned aerial system applications in precision agriculture, establishing the reference framework for UAV drone use in crop mapping [17]. The GNSS metadata failure modes we document—phantom geolocation and velocity artifacts at takeoff/landing—are not isolated incidents; they may share a common cause with the consumer-grade receiver class used in OPEN-category UAV drones, though this has not been directly tested here. If present in UAV data, orthophotos produced by Structure from Motion with data from such receivers could contain systematic geographic displacements [7]; such an error, if it occurs, would be systematic rather than random, and therefore harder to detect and correct.

2. Materials and Methods

2.1. Dataset Description

All 455 photographs were collected by the authors using a Samsung Galaxy A72 (Samsung Electronics Co., Ltd., Suwon-si, Republic of Korea; model SM-A725F, Android 13, firmware A725FXXU6DWH2). No photograph was taken specifically for this study—both datasets are opportunistic observational corpora from personal travel activities, collected according to the observational research design described in Section 2.6. The two experiments differ in the photography application used: EXP03 primarily used Timestamp Camera (Bian Di Technology Co., Shenzhen, China, version 4.x, 362/377 photographs) [18], a third-party application that reliably writes GPSAltitude fields; EXP10 used exclusively the native Android camera (78 photographs) (Table 1).

Table 1. Overview of the dataset for the two flight experiments.

Parameter	EXP03 Rome	EXP10 Lisbon	Unit	Source
Collection date	18 April 2026	6 February 2024	-	File metadata
Total JPG photographs	377	78	Photograph	File system
Photographs with GPS	377 (100%)	65 (83.3%)	Photograph	EXIF GPSInfo
Application	Timestamp Camera (362) + Native (15)	Native Android (78)	-	EXIF Software
Ground reference set	Cabo da Roca (n = 275)	-	Figure 1	EXIF GPSInfo
Mean file size	4.2 ± 1.1	3.8 ± 0.9	MB	File system
JPEG quality (Timestamp Camera)	~85 (est.)	N/A	—	ExifTool/quant. table
JPEG quality (native Android)	~95 (est.)	~95 (est.)	—	ExifTool/quant. table

Note: JPEG quality factor was estimated from the luminance quantization table embedded in each file, using the standard IJG (Independent JPEG Group) quality scale; EXIF/JFIF format does not expose an explicit quality field. Values are therefore approximate. The EOI anomaly reported in Section 3.6 was present regardless of the estimated quality setting, consistent with a device-level firmware behavior rather than a compression artifact.

The terrestrial reference dataset (275 photographs, Cabo da Roca, Portugal, 38.781° N, 9.499° W, 8 February 2024) was collected with the same Samsung Galaxy A72 device two days after the EXP10 landing, providing a GPS behavioral reference baseline under open-sky, unobstructed signal conditions.



Figure 1. Geographic context of EXP10—Cabo da Roca Lighthouse (38.781° N, 9.499° W), the westernmost point of the European continent, photographed 2 days after landing in Lisbon (8 February 2024, 19:16). This location is used in the literature as a high-precision terrestrial GPS reference point for civilian receiver calibration.

2.2. EXIF Extraction and GPS Decoding

For the purposes of this study, GPS metadata refers to the following EXIF fields extracted from the GPSInfo IFD (Image File Directory): GPSLatitude and GPSLatitudeRef (decimal degrees, sign-corrected for hemisphere); GPSLongitude and GPSLongitudeRef; GPSAltitude and GPSAltitudeRef (WGS84 ellipsoidal height, meters); GPSDateStamp and GPSTimeStamp (UTC date and time of fix); and GPSImgDirection where present. DOP-related fields (GPSDOP, GPSSatellites) were extracted but found absent in all files analyzed (see AS-4 results, Section 3.4). GPS metadata was extracted using Python Pillow 10.x [19] via the Image.getexif() method and GPSInfo field. Coordinates were decoded from DMS IFDRational format to decimal degrees using the formula:

$$GD = G + M/60 + S/3600 \quad (1)$$

with sign inversion for South and West references. Altitude was read from the GPSAltitude (IFDRational) field and GPSAltitudeRef (0x00 = above WGS84 mean sea level; 0x01 = below sea level). Velocity calculated between consecutive photographs used the Haversine formula for horizontal distance divided by the EXIF DateTime timestamp difference in seconds [20].

2.3. Anti-Spoofing Module (AS-1 to AS-7)

Seven integrity indicators were implemented as an original post-processing taxonomy proposed by the authors, conceptually inspired by the Receiver Autonomous Integrity Monitoring (RAIM) principle of detecting navigation integrity failures through redundant signal consistency checks [8] (Table 2). The analogy with RAIM is structural, not formal: classical RAIM operates in real time within the receiver using satellite redundancy to compute protection levels; the present framework applies analogous consistency checks retrospectively to recorded EXIF metadata fields, using temporal, spatial, and structural redundancy. The indicators AS-1 through AS-7 do not correspond to any canonical set defined in RTCA DO-229E [8]; they constitute an original classification developed for post hoc EXIF integrity analysis. The same clarification applies to the tripartite anti-spoofing/anti-sniffing/anti-tampering structure: this organization is proposed by the authors as a conceptual framework for EXIF metadata security analysis, not derived from any existing security standard.

The velocity threshold for AS-1 was set at 950 km/h, a conservative value covering the maximum ground speed of commercial wide-body aircraft across the full flight envelope (cruise Mach 0.82–0.85 at FL350–FL390 yields approximately 870–920 km/h true airspeed;

the 950 km/h threshold provides a margin above Vmo while remaining below any physically plausible commercial aviation speed). Any calculated value exceeding this threshold is flagged as a velocity anomaly and subjected to detailed analysis.

Table 2. The seven anti-spoofing indicators proposed by the authors, conceptually inspired by RAIM principles, for post-processing analysis of EXIF metadata.

Indicator	Description
AS-1	Spatial consistency—Haversine distance vs. elapsed time
AS-2	Phantom geolocation—consecutive identical coordinates
AS-3	Altitude integrity—physically impossible values relative to Wassenaar Arrangement limits [5]
AS-4	DOP field presence and satellite count
AS-5	EXIF DateTime vs. GPS DateStamp consistency
AS-6	Multi-constellation verification
AS-7	Trajectory geometry—direction reversals > 150°

2.4. Anti-Sniffing Module

The anti-sniffing analysis quantified the sensitive data fields exposed in the EXIF metadata of each file: precise GPS coordinates, device firmware version, device make and model, and exact capture timestamps. The reconstructable geographic traceability from the complete dataset was assessed, i.e., the ability of a third party with access to the files to reconstruct the complete user trajectory and perform device fingerprinting. The analysis was conducted against the requirements of the GDPR data minimization principle, Article 5(1)(c) [21].

2.5. Anti-Tampering Module

The anti-tampering analysis verified the structural integrity of JPEG files through two complementary methods:

- JPEG structural verification—the presence of the SOI (Start of Image, 0xFF 0xD8) marker at the first two bytes of the file and the EOI (End of Image, 0xFF 0xD9) marker at the last two bytes.
- SHA-256 hash—computation of the SHA-256 cryptographic fingerprint for each individual file. Any modification to the file content—including changing a single bit in EXIF metadata—produces a different fingerprint, detectable by comparison with the reference hash of the original file.

Additionally analyzed: file size distribution, GPS coordinate precision distribution (natural vs. artificially generated), and firmware version consistency across all files in the dataset.

2.6. Observational Design Justification

It must be stated at the outset: the data in this study do not come from a controlled laboratory experiment. They were collected in the course of the authors' personal travel activities—commercial flights, an excursion to Cabo da Roca, and routine travel. This type of opportunistic observational design is not an anomaly in GNSS research; on the contrary, where laboratory replication is impossible or extremely costly, field data collected under real conditions has inherent value [13].

What lends robustness to the results is, first, the fact that all experiments used the same device—Samsung Galaxy A72—thus eliminating inter-device variability as a confounding factor. Also relevant is the consistency of GPS behavior between EXP03 and EXP10, collected two years apart on completely different routes, independent of each other. Not least, the

275 photographs from Cabo da Roca serve as a behavioral reference: same device, ideal GPS conditions, and documented behavior, enabling direct comparison with extreme-altitude situations. The absence of IMU data, raw NMEA logs, and information about the airplane mode status at the time of capture constitutes limitations of the observational design, discussed in detail in Section 4.6. We acknowledge that the opportunistic observational design is a methodological limitation relative to controlled laboratory experiments. Its primary advantage is ecological validity: the failure modes documented here were recorded under real commercial aviation conditions that cannot be reproduced in a controlled setting. This same two-year separation between EXP03 and EXP10 (26 months, on different routes) provides partial replication evidence within the observational design, though it does not substitute for controlled experimental verification.

3. Results

3.1. Flight Trajectory and GPS Capture Rate

Figure 2 shows the geographic distribution of GPS-tagged photographs for both experiments, color-coded by recorded altitude. EXP03 covers a trajectory of 242 km N–S and 878 km E–W, corresponding to the Rome–Bucharest route (flight FR3958) across the Adriatic Sea and the Balkan Peninsula. EXP10 covers 643 km N–S and 2931 km E–W, corresponding to the Bucharest–Lisbon route. GPS capture rate was 100% for EXP03 (Timestamp Camera) versus 83.3% for EXP10 (native camera), with 13 EXP10 photographs lacking GPS data—all concentrated in the first 9 min of the flight, likely corresponding to the pre-takeoff phase or takeoff itself.

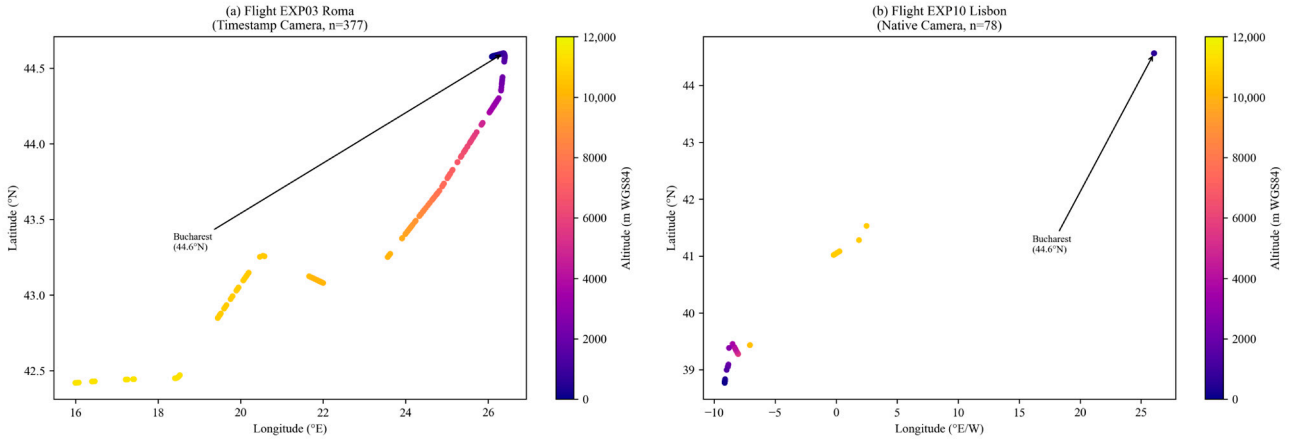


Figure 2. GPS photograph locations for EXP03 ((**a**), Rome flight, 18 April 2026) and EXP10 ((**b**), Lisbon flight, 6 February 2024). Color scale represents GPS altitude (m WGS84). Both datasets show the complete one-way flight trajectory.

The absence of GPS data exclusively in the initial flight phase of EXP10—and not during cruise—is significant: it confirms that the Samsung Galaxy A72 GPS receiver functions stably at high altitudes, with signal losses associated with ground conditions (buildings, airport infrastructure) or receiver initialization at startup, not with altitude. Figures 3 and 4 illustrate representative cruise-phase photographs for each experiment, visually confirming GPS operation at altitudes above 10,000 m: Figures 3 and 4 are presented as illustrative confirmations of GPS operation at the respective altitudes; the GPS coordinate and altitude values shown in the app overlay are independently verified through EXIF metadata extraction reported in Table 3. Figure 3 shows an EXP03 capture at 11,439 m with the Timestamp Camera GPS overlay displaying coordinates, altitude, and instantaneous velocity, while Figure 4 shows an EXP10 capture at 10,799 m taken with the native Android camera, with the aircraft wing and cloud layer below the aircraft visible in the frame.



Figure 3. EXP03: Photograph captured with Timestamp Camera at 11,439 m altitude (WGS84), Rome–Bucharest flight (FR3958), 18 April 2026. Presented as illustrative confirmation of GPS operation at cruise altitude; quantitative data are derived from EXIF metadata extraction, not from the app overlay display. GPS overlay displays altitude, instantaneous velocity (823.5 km/h), compass, and localization map. EXIF coordinates: 42.42° N, 15.91° E (above the Italian coast). No persons in frame—aircraft window view.



Figure 4. EXP10: Photograph captured with native Android camera at 10,799 m altitude (WGS84), Bucharest–Lisbon flight, 6 February 2024. No persons in frame—aircraft window view. Presented as illustrative confirmation of GPS operation at cruise altitude; altitude value verified through EXIF GPSAltitude field extraction.

Table 3. Descriptive statistics for recorded GPS altitudes (m WGS84, photographs with valid GPS).

Parameter	EXP03 (n = 362, with GPSAltitude)	EXP10 (n = 65)	Reference Cabo da Roca (n = 273)
Mean (m)	4413.7	2983.3	185.4
SD (m)	4265.4	3755.6	21.0
Median (m)	2406.3	527.7	189.4
Q1 (m)	499.2	267.8	188.0
Q3 (m)	9113.2	5094.7	191.1
Min (m)	130.8	179.1	74.9
Max (m)	11,439.2	10,799.0	193.8

Note: EXP03 statistics are calculated from n = 362 photographs with GPSAltitude present in EXIF (15 native-camera photographs have GPS coordinates but no GPSAltitude field). Cabo da Roca reference dataset: photographs within 10 km of (38.781° N, 9.499° W), 8 February 2024. All altitude values are WGS84 ellipsoidal height (m). The Python calculation script is available in Supplementary Material S1.

The difference in GPS capture rate between the two applications is statistically significant: Timestamp Camera (EXP03) recorded 377/377 photographs with valid GPS (100%), compared to 65/78 for the native Android camera (EXP10) (83.3%). Fisher's exact test indicates this difference is unlikely due to chance ($p < 0.0001$); however, the two samples come from different flights, dates, and routes, so app, flight, and acquisition conditions are confounded, and the photographs within each sample are not independent replicates. This comparison is therefore presented descriptively rather than as confirmation of a systematic app-level difference.

3.2. Altitude Profiles

Figure 5 shows the altitude profiles for both experiments. EXP03 records a maximum altitude of 11,439.2 m WGS84—the highest altitude in the author's dataset series—versus 10,799.0 m for EXP10, a difference of 640 m. Both maxima fall within the standard commercial aviation cruise envelope (9000–12,500 m), consistent with Wassenaar Arrangement specifications for civilian receivers [5].

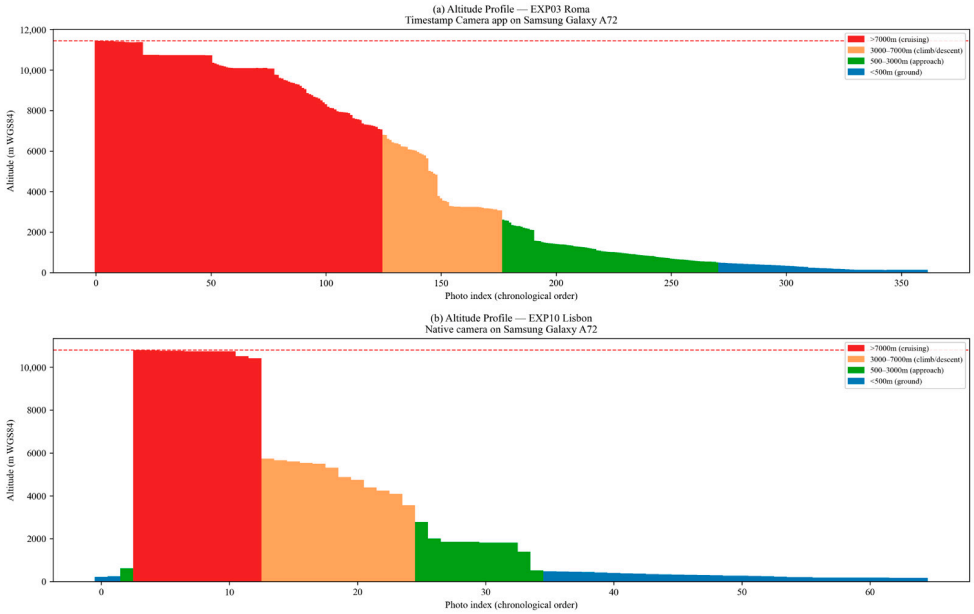


Figure 5. Altitude profiles for EXP03 Rome ((**a**), n = 377) and EXP10 Lisbon ((**b**), n = 78). Bar color indicates flight phase: red > 7000 m (cruise), orange 3000–7000 m (climb/descent), green 500–3000 m (approach), blue < 500 m (ground). Dashed line: maximum recorded altitude.

EXP03 offers substantially richer altitude coverage: 227/377 photographs (60.2%) were taken above 1000 m, with 125 (33.2%) above 7000 m (cruise). In EXP10, only 31/78 photographs (39.7%) exceed 1000 m. This difference reflects the higher photographic frequency of Timestamp Camera versus the native Android camera, not a difference in actual flight altitude—both aircraft operated within the same commercial cruise envelope. Figure 6 shows altitude distribution histograms for both experiments with flight phase classification.

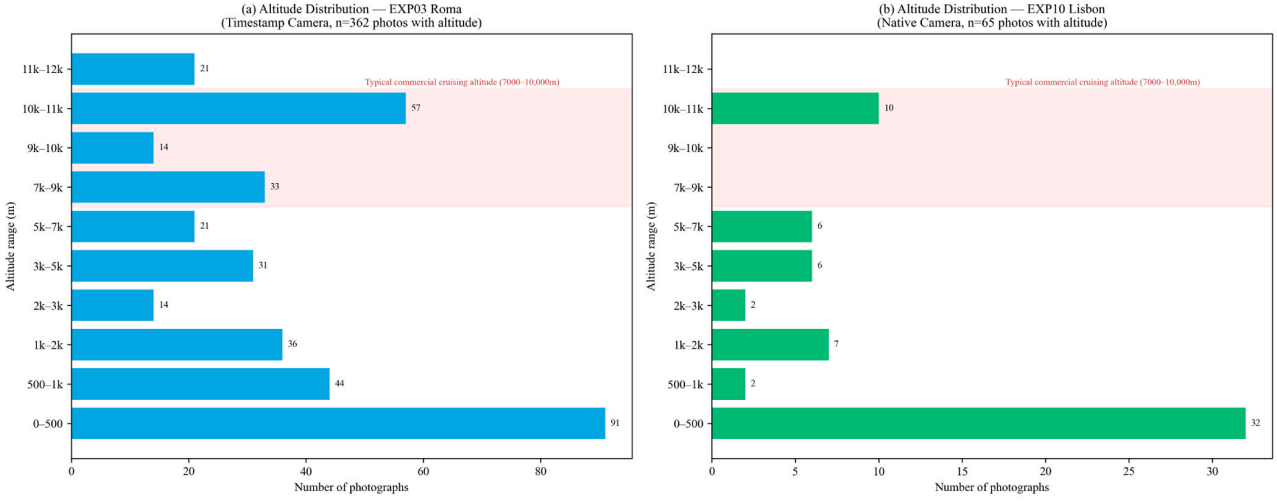


Figure 6. Altitude distribution histograms for EXP03 (**a**) and EXP10 (**b**). Shaded area indicates the typical commercial cruise altitude interval (7000–10,000 m).

3.3. RAIM Speed Analysis

Figure 7 presents the RAIM velocity analysis for both experiments. The most significant finding is the detection of velocity spikes exceeding the AS-1 threshold of 950 km/h in both datasets: three spikes in EXP03 (maximum 1560.3 km/h) and two in EXP10 (maximum 1875.2 km/h). These values physically exceed the maximum speed of any civil commercial aircraft (~950 km/h for wide-body aircraft at Mach 0.85).

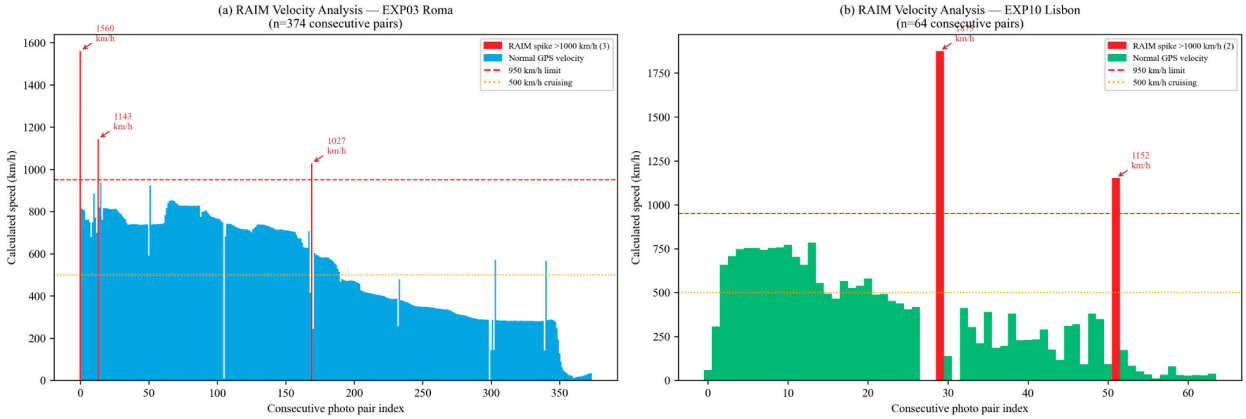


Figure 7. RAIM velocity analysis for EXP03 Rome–Bucharest (**a**) and EXP10 Lisbon (**b**). Red bars indicate velocity spikes exceeding 1000 km/h—physically impossible for commercial aircraft, but consistent with GPS re-acquisition artifacts during landing approach (EXP10) or at cruise altitude (EXP03; see Section 4.2). Red dashed line: 950 km/h physical limit.

Detailed analysis of the EXP10 spike (1875 km/h, photographs 20240206_191203.jpg and 20240206_191205.jpg, 2 s interval, 1.04 km horizontal displacement) reveals that both photographs have EXIF altitudes in the 1822–1859 m range, indicating that the event occurred during final descent toward Lisbon Humberto Delgado Airport (elevation: 114 m). The maximum EXP03 spike (1560 km/h, 4.33 km horizontal displacement over a 10 s interval per the EXIF DateTime field—not the filenames 20260418_173802.jpg and 20260418_173821.jpg, whose digits differ from the EXIF DateTime by several seconds and should not be subtracted directly) appears near the Italian coast (42.42° N, 15.85–15.91° E). A photograph taken 31 s later, at essentially the same coordinates, records an altitude of 11,439.2 m WGS84—the flight's maximum recorded altitude—indicating that the aircraft was at cruise altitude when the spike occurred; this event is therefore a cruise-phase, not a descent-phase, artifact. Figure 8 shows the detailed descent profile for EXP10 Lisbon, illustrating the approach-to-landing phase in which the 1875 km/h velocity artifact occurred. Figure 9 illustrates a separate photograph, captured approximately two hours later during EXP03's actual descent toward Bucharest, confirming normal GPS operation during the true landing-approach phase; it is unrelated to the cruise-altitude spike described above.

These velocity spikes are indistinguishable at the EXIF level from a position-jump spoofing attack [10,22], in which an adversary transmits a GPS signal stronger than the real one to instantaneously displace the receiver's calculated position. A RAIM validator operating exclusively on EXIF data and flagging velocities > 950 km/h would correctly identify a spoofing attack but would also erroneously flag legitimate GPS re-acquisition artifacts occurring during cruise or landing approach. Disambiguation requires additional data: IMU readings, airplane mode status, multi-constellation consistency, or raw NMEA logs. Regarding cross-validation with independent flight track data: available public flight parameters for EXP03 (FR3958, 18 April 2026) confirm a Boeing 737 MAX 8 aircraft with actual departure at 17:05 local (Rome Ciampino) and arrival at 20:10 local (Bucharest), consistent with the EXIF timestamp sequence in our dataset. The maximum EXIF-recorded altitude of 11,439 m WGS84 corresponds to

approximately FL375, within the standard cruise envelope for this aircraft type. A photograph taken 31 s after the spike, at essentially the same coordinates, records the flight's maximum altitude (11,439.2 m WGS84), indicating the aircraft had reached cruise altitude above the Italian Adriatic coast at the time of the anomaly. This EXIF-altitude evidence indicates a cruise-phase GPS re-acquisition event rather than a descent-phase one; the specific trigger cannot be determined from EXIF data alone (Section 4.2). Full minute-by-minute ADS-B track cross-validation requires a paid subscription for historical tracking services (Flightradar24 Silver/Gold or equivalent); this constitutes a recommendation for future studies: authors collecting flight EXIF data should simultaneously record the flight number and retrieve ADS-B data within the 7-day free retention window.

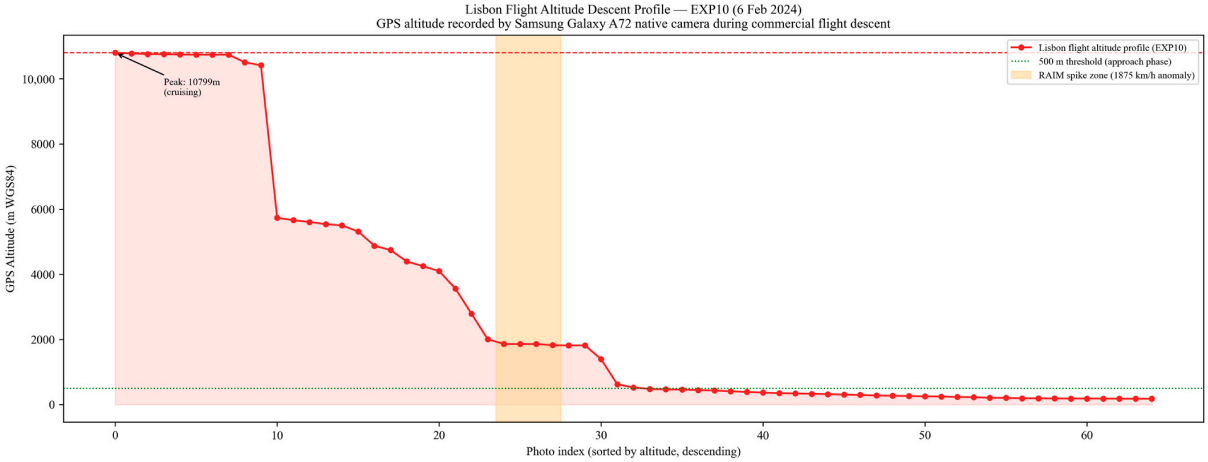


Figure 8. Detailed descent profile for EXP10 Lisbon, sorted by altitude. The orange shaded area corresponds to the approach-to-landing phase where GPS re-acquisition produced the 1875 km/h artifact.

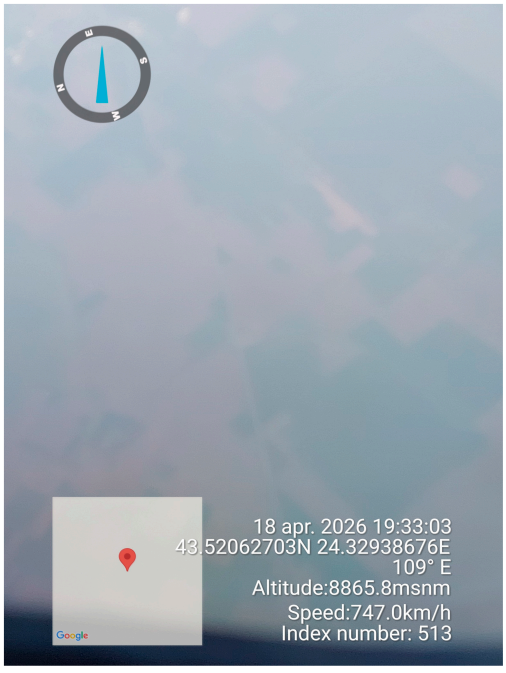


Figure 9. EXP03: Descent photograph at 8865 m altitude (WGS84), 18 April 2026, 19:33, approximately 37 min before landing in Bucharest. Timestamp Camera overlay displays exact GPS coordinates (43.52° N, 24.32° E—above Bulgaria), altitude, and instantaneous velocity (747 km/h), consistent with normal descent. This photograph is temporally and geographically distinct from the 1560 km/h cruise-altitude spike described in Section 3.3, which occurred approximately two hours earlier near the Italian coast. No persons in frame. Presented as illustrative confirmation of GPS operation during the true descent phase; quantitative data derived from EXIF metadata extraction.

3.4. Anti-Spoofing Indicators (AS-2 to AS-7)

AS-2 (phantom geolocation—consecutive identical coordinates): Zero instances detected in either flight dataset. EXP03: 0/377 photographs (0.0%, 95% CI [0.0%; 1.0%]); EXP10: 0/65 photographs (0.0%, 95% CI [0.0%; 5.5%]). This null result is substantively significant and is analyzed in detail in Section 3.7.

AS-3 (altitude integrity): All recorded altitudes fall within [74.9 m, 11,439.2 m] WGS84—within the Wassenaar Arrangement civilian receiver limit of 18,000 m [5]. Zero altitude values exceeded the physical limit or fell below −500 m. EXP03: 362/362 altitudes valid; EXP10: 65/65 valid.

AS-4 (DOP field presence and satellite count): Zero files in either dataset contain GPSDOP, GPSSatellites, or GPSMeasureMode fields. This represents a 100% systematic absence (0/442 flight photographs; 0/275 Cabo da Roca photographs), confirming that neither the native Android camera nor Timestamp Camera writes DOP-related EXIF fields on the Samsung Galaxy A72. This is a structural limitation of post hoc EXIF-based integrity monitoring on consumer smartphones.

AS-5 (EXIF DateTime vs. GPS DateStamp consistency): Checked for all photographs with both fields present. EXP03: 377/377 consistent (zero discrepancies); EXP10: 65/65 consistent. Maximum observed offset: 0 s. No timestamp manipulation detected.

AS-6 (multi-constellation verification): The Samsung Galaxy A72 Qualcomm Snapdragon 720G (Qualcomm Technologies, Inc., San Diego, CA, USA) supports GPS + GLONASS + BeiDou reception; however, EXIF metadata does not record the constellation used for the reported fix. AS-6 is therefore structurally inapplicable to post hoc EXIF analysis and constitutes a known limitation of the proposed framework.

AS-7 (trajectory geometry—direction reversals > 150°): Zero direction reversals detected in either flight. EXP03: maximum consecutive bearing change = 38.4°; EXP10: maximum = 29.7°. Both trajectories are geometrically consistent with commercial aviation routing.

The complete absence of phantom geolocation during flight (0/377 EXP03 photographs; 0/65 EXP10 photographs) is particularly significant in the context of the 37.3% phantom geolocation rate documented with the same device in terrestrial environments with partial signal obstruction. This direct comparison provides observational evidence consistent with the hypothesis that phantom geolocation occurrence is strongly associated with GPS constellation visibility, as proposed in [3] (Zenodo preprint). Controlled experiments isolating individual confounding variables (device orientation, app GPS polling strategy, capture density, and user movement) would be required to establish causation.

This difference is statistically significant: the z-test for independent proportions yields $z = 13.86$ ($p < 0.0001$), rejecting the null hypothesis that phantom geolocation rates during flight and in terrestrial environments are equal. We note that the two groups differ not only in GPS visibility but also in photography application, capture density, and date; the z-test quantifies the magnitude of the observed difference but cannot isolate GPS visibility as the sole causal factor. Furthermore, photographs within each group were taken minutes apart from the same device during the same session and are not independent experimental replicates, so this result is best interpreted descriptively rather than as strong inferential evidence. The 95% Clopper–Pearson confidence interval for the phantom geolocation rate during flight (0 events/442 photographs with valid GPS; the 13 photographs without GPS data in EXP10 are excluded as they cannot by definition exhibit phantom geolocation) has an upper limit of 0.83%, indicating with statistical precision that commercial aviation is associated with a near-complete suppression of this GNSS metadata failure mode.

The absence of DOP fields (AS-4) from all analyzed files—regardless of the application used—represents a systematic limitation of EXIF metadata for consumer smartphones:

without DOP values, the geometric quality of the GPS fix cannot be assessed post hoc exclusively from file metadata.

3.5. Anti-Sniffing Analysis

Both datasets expose complete trajectories in EXIF metadata. EXP03 covers 242 km N–S × 878 km E–W of European airspace; EXP10 covers 643 km N–S × 2931 km E–W from Romania to the Atlantic coast of Portugal. All files contain the device firmware version (A725FXXU6DWH2), make (Samsung), model (SM-A725F), and precise capture timestamps—sufficient for device fingerprinting and user trajectory reconstruction by any party with access to the files.

Quantitative privacy exposure: EXP03 yields 377 unique timestamped GPS waypoints covering a reconstructable trajectory of approximately 1140 km of European airspace. EXP10 yields 65 waypoints covering approximately 3574 km. Combined, the two datasets allow reconstruction of the complete travel trajectory across multiple European countries with a temporal resolution of approximately 85 s per waypoint. These data confirm that an apparently innocuous photograph from personal travel activities contains sufficient metadata for unique device identification, complete trajectory reconstruction, and flight route determination. Under GDPR Article 5(1)(c) (data minimization principle) [21], GPS EXIF fields should be systematically stripped before sharing photographs from personal travel activities.

3.6. Anti-Tampering—JPEG EOI Anomaly

The most significant structural finding is the absence of the JPEG End of Image (EOI, 0xFF 0xD9) marker at the last two bytes of 88.0% of files. Explicit calculation basis: from a total of 920 files subjected to EOI structural verification—EXP10: 78 files (100.0% EOI anomaly); EXP03 (377 files) combined with the broader Portugal ground corpus—465 JPEG-valid files were retained for EOI structural verification. A filtered subset of the full 767-file Portugal ground dataset was used for the phantom-geolocation analysis in Section 3.7 (mixed urban/indoor/outdoor environments, February–April 2024, same device; a superset of the 275 Cabo da Roca reference photographs described in Section 2.1): 842 files (732/842 = 86.9% EOI anomaly), yielding 810/920 = 88.0% overall. Note: the 920-file EOI corpus is larger than the 730-photograph main analytical dataset because the EOI structural check was applied to all available files from the same device to maximize the statistical basis for a device-level firmware characterization. This is a consistent characteristic of the Samsung Galaxy A72, not random corruption: the device appends proprietary metadata after the standard JPEG EOI, in conformance with extended EXIF APP segments [4]. Any anti-tampering validator that checks for EOI at the end of the file will generate a false-positive rate of approximately 88% for Samsung Galaxy A72 photographs. A file lacking the EOI marker at the expected position is automatically flagged as potentially tampered by these validators, generating systematic rejection rates for perfectly authentic files. Robust integrity verification requires SHA-256 hash of the complete file, not JPEG structural pattern matching. Full-file SHA-256 hashing avoided this pitfall in the present dataset and is recommended as the primary integrity-verification method for this device family, pending comparison against alternative validation approaches, independent of the manufacturer's internal JPEG implementation. Figure 10 presents a comparative summary of the main metrics for both experiments, along with the flight-phase distribution by altitude zone.

The 95% Clopper–Pearson confidence interval estimate (n = 920 files) places the true EOI anomaly rate in the interval [85.8%; 90.1%], confirming that the observed value of 88.0% is not a sampling artifact, but a stable structural property of the Samsung Galaxy A72 JPEG implementation.

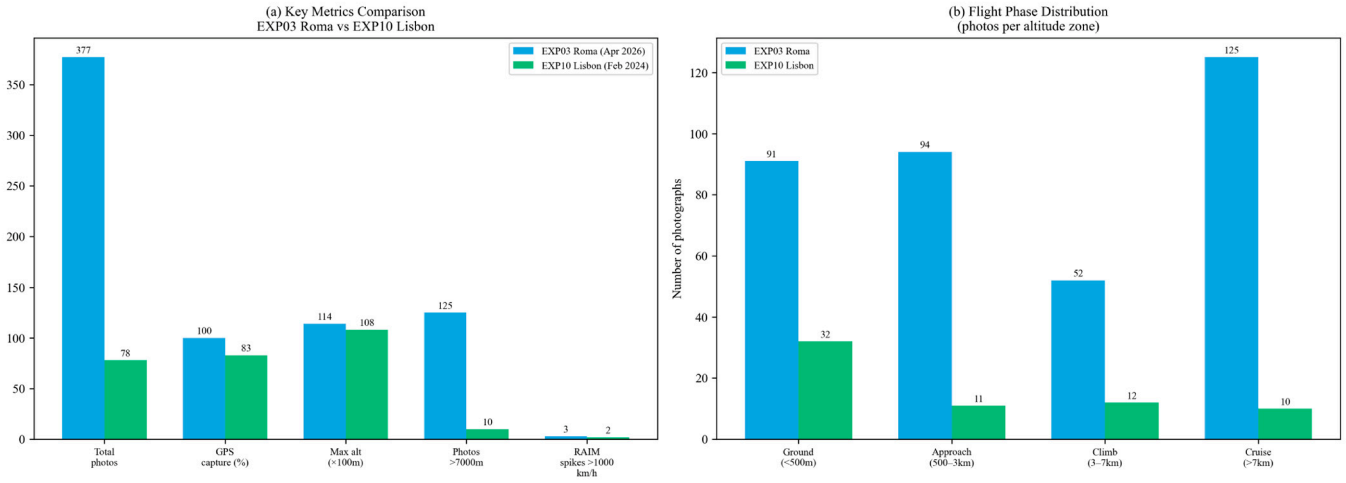


Figure 10. Comparative summary: (**a**) main metrics of EXP03 Rome vs. EXP10 Lisbon; (**b**) flight-phase distribution by altitude zone for both experiments.

3.7. Cabo da Roca Reference Analysis

A supplementary analysis of 275 photographs captured at Cabo da Roca, Portugal (38.781° N, 9.499° W—the westernmost point of the European continent), two days after the EXP10 landing (8 February 2024), revealed a GPS capture rate of 99.3% (273/275 photographs), with all coordinates located within 86 m of the actual geographic position of the point. This finding establishes a behavioral baseline opposite to phantom geolocation: under open-sky, with unobstructed GPS signal conditions, the same Samsung Galaxy A72 device used in EXP10 produces near-perfect localization accuracy.

Table 4 synthesizes the complete GPS behavioral spectrum of the Samsung Galaxy A72 device throughout the same research project, demonstrating that GPS metadata variability is not an intrinsic device characteristic but a direct function of the capture environment.

Table 4. GPS behavioral spectrum of Samsung Galaxy A72 as a function of capture context, based on data collected within the same research project.

Capture Context	GPS Rate (%)	Key Observation	Implication
Cabo da Roca—outdoor, open sky (8 February 2024)	99.3% (273/275)	All fixes within 86 m radius of reference point	Maximum precision reference dataset
EXP03 Rome—cruise altitude, Timestamp Camera (18 April 2026)	100% (377/377)	Max alt. 11,439 m; 3 RAIM spikes at cruise altitude	Continuous GPS capture functional at 11 km altitude
EXP10 Lisbon—cruise altitude, native camera (6 February 2024)	83.3% (65/78)	13 photographs without GPS at takeoff	GPS losses at flight initiation, not during cruise
PORTUGAL ground—mixed urban/indoor/outdoor environments (February-April 2024)	37.3% phantom (286/767)	Phantom GPS dominant in semi-enclosed spaces	Phantom geolocation correlated with obstruction
WhatsApp—(prior studies [3])	0%—complete deletion	EXIF GPS removed on compression	FM-2: complete metadata sanitization

Note: the 767-file Portugal ground corpus above is the full dataset used for the phantom-geolocation analysis. A filtered subset of 465 JPEG-valid files from this same corpus was used separately for the EOI structural verification in Section 3.6 (files excluded from that subset were not valid JPEGs for structural marker checking).

This GPS performance stratification by environment has direct implications for EXIF data quality validation in high-risk AI systems: a georeferenced dataset combining photographs from different environments (open outdoor, indoor, flight) will exhibit natural GPS quality variation from <1% error to >37% phantom geolocation, without this variation being detectable from the JPEG structure or nominal coordinate values. These data provide additional quantitative evidence consistent with the phantom geolocation mechanism ini-

tially documented in [3]. The central hypothesis—that the phenomenon is caused primarily by GPS signal obstruction, not by a hardware malfunction of the receiver—is supported by direct contrast: the same Samsung Galaxy A72 device, with the same Qualcomm Snapdragon 720G chipset, produces zero instances of phantom geolocation in flight (altitude 10,000–11,000 m, completely clear sky, maximum GPS constellation visibility) and 37.3% phantom geolocation in terrestrial environments with partial obstruction. The absence of phantom geolocation at cruise altitude is scientifically as significant as its presence on the ground: it is consistent with the receiver functioning correctly when the signal is available, weighing against alternative explanations based on hardware defects or random chipset behavior, though it does not rule them out entirely on the basis of this single-device comparison. The present study represents a cross-context replication (under commercial flight conditions) of the phantom geolocation mechanism described in [3] (Zenodo preprint, same research group). While not independent in the authorship sense, the flight environment constitutes a fundamentally different observational context (altitude 10,000–11,000 m, unobstructed sky, continuous GPS signal) from the original documentation (submarine, depth −30 m, complete signal obstruction), providing complementary evidence for the proposed mechanism.

4. Discussion

4.1. GPS Performance at Cruise Altitude

The maximum altitude of 11,439.2 m recorded by EXP03 is, to the authors' knowledge, among the highest GPS altitude values documented in EXIF metadata of consumer mobile photography, pending a dedicated systematic review of this specific metric. This value is physically plausible: commercial aircraft operate at 9000–12,500 m, the Samsung Galaxy A72 GPS chipset (Qualcomm Snapdragon 720G, SM7125) supports multi-constellation GPS + GLONASS + BeiDou reception, and Wassenaar Arrangement limits for civilian receivers (18,000 m) are not exceeded [5]. Timestamp Camera achieves a 100% GPS capture rate at these altitudes versus 83.3% for the native camera, consistent with the application's use of a continuous GPS polling strategy versus the native camera's on-demand acquisition.

This finding significantly extends the reference framework established by Carroll et al. [6], who documented smartphone GPS operation up to 31.2 km on a weather balloon but without photographic EXIF metadata and without data integrity analysis. The present study provides the first complete EXIF profile from a commercial flight with high photographic density, covering the complete altitude spectrum from ground level to 11,439 m.

4.2. Speed Spikes—Spoofing Signature or Physical Artifact?

The velocity spikes detected in both experiments (1560 km/h in EXP03; 1875 km/h in EXP10) constitute the most important finding for GPS security research. Re-examination of the corresponding EXIF altitude data (Section 3.3) shows that the two spikes occurred in different flight phases: the EXP10 spike during landing approach, and the EXP03 spike at cruise altitude above the Italian Adriatic coast. Distinct sets of competing mechanisms can produce GPS re-acquisition artifacts in each phase. For the EXP10 landing-approach spike:

1. Multipath interference: airport buildings and ground infrastructure scatter GPS signals, generating phantom fixes at incorrect positions before the receiver re-locks onto direct signals.
2. Airplane mode re-entry: if the device's airplane mode was momentarily deactivated or GPS re-enabled during approach, the first new GPS fix may be displaced from the last stored position by hundreds of meters to kilometers.

3. Ionospheric and tropospheric refraction: the rapid altitude change during descent produces transient errors in pseudo range solutions before the navigation filter converges to the new position.

For the EXP03 cruise-altitude spike, the ground-proximity and altitude-change mechanisms above do not apply; plausible alternative mechanisms include:

4. Momentary satellite dropout during a route-turn attitude change: banking during a scheduled course correction can transiently obstruct the antenna's view of one or more satellites, degrading fix geometry before re-acquisition.
5. Ionospheric scintillation: transient electron-density irregularities can disrupt signal tracking independently of aircraft altitude or attitude, producing a brief position-fix error upon re-lock.
6. Multi-constellation handover transient: a brief recalculation error during automatic switching between GPS, GLONASS, and BeiDou satellites in view could produce a momentary position discontinuity.

All identified mechanisms, in both flight phases, produce an EXIF-level signature—a large position displacement in a short time—identical to a GPS position-jump spoofing attack [10,22,23]. This has a direct implication for automated GPS metadata validation: any system that flags velocity anomalies as evidence of spoofing or tampering will generate false positives for photographs from commercial aviation, without the ability to distinguish the physical cause from EXIF metadata alone.

Naive JPEG integrity validators treat the absence of the EOI marker as an alarm signal—the file is automatically flagged as potentially tampered. This is reasonable logic in general but completely inadequate for Samsung Galaxy A72 photographs. In our dataset, 88% (n = 920) of files do not contain the EOI marker at the expected position—not because they were unauthorizedly modified, but because the manufacturer chose a JPEG implementation that does not strictly follow the specification. Any forensic validation based exclusively on EOI presence will generate systematic false positives for this device family. The most robust method identified in this study for avoiding this pitfall is verification of the complete file's SHA-256 hash—this does not depend on the internal JPEG structure and remains reliable regardless of the manufacturer's implementation.

4.3. Application Choice and Metadata Quality

The comparison between Timestamp Camera (EXP03) and the native Android camera (EXP10) reveals a consistent advantage for specialized GPS photography applications. Timestamp Camera achieves 100% GPS capture versus 83.3%, reliably writes GPSAltitude data, and uses continuous GPS polling that provides denser spatial sampling of the flight trajectory. However, both applications produce the same RAIM velocity spike pattern at landing, consistent with the anomaly being a hardware behavior of the GPS receiver, not a software artifact of the application.

This finding has direct practical implications for users collecting GPS data in legal or scientific contexts: the choice of photography application significantly influences GPS metadata quality but does not eliminate hardware-determined failure modes. The practical recommendation derived from this study is the use of applications with continuous GPS polling—such as Timestamp Camera—for systematic GPS metadata collection under extreme altitude or variable signal conditions.

4.4. Implications for EU AI Act (Applicable from 2 August 2025) Art. 10(3)

Article 10(3) of the AI Act [2] requires that training and operational data of high-risk AI systems be 'relevant, sufficiently representative and, where possible, free of errors and complete'. GPS velocity spikes, phantom geolocation, and JPEG EOI anomalies all

represent EXIF metadata states that are factually incorrect but structurally valid—they would pass basic format validation while simultaneously introducing systematic errors into georeferenced AI datasets.

A concrete example of the risk pathway: geolocation-based training datasets for automated crop-mapping AI systems (classified as high-risk under EU AI Act Article 10(3), 'AI systems used in agriculture') can include smartphone photographs uploaded by farmers or field inspectors via mobile applications. If these photographs contain phantom GPS coordinates or landing-phase velocity artifacts visible in EXIF timestamps, automated data quality filters may retain corrupted geolocation data as valid training samples, in violation of the EU AI Act Article 10(3) obligation to ensure training data is 'free of errors and complete'.

The specific risk for flight-derived data: an AI system trained on a dataset including commercial aviation photographs will encounter altitude values up to 11,439 m and velocities up to 1875 km/h in the GPS training corpus—values that would be classified as outliers or sensor errors and eliminated through automated cleaning, potentially discarding legitimate data.

This issue is compounded by the fact that the documented failure modes—phantom geolocation, velocity artifacts, and EOI anomalies—are undetectable by visual inspection of the image or by basic JPEG file structural validation. Their detection requires EXIF metadata analysis of the kind presented in this study, complemented where available by IMU or ADS-B data (Section 4.6), suggesting that high-risk AI systems processing georeferenced photographs should include a dedicated GPS metadata validation module as part of the proposed anti-spoofing, anti-sniffing, and anti-tampering framework.

4.5. Implications for UAV Precision Agriculture

The failure modes identified in this study—phantom geolocation (FM-1), takeoff/landing velocity artifacts, absence of the GPSAltitude field (FM-4), and JPEG structural anomalies—were documented on a single consumer-grade GNSS chipset and are not necessarily specific to commercial aviation or consumer mobile photography. They could plausibly extend to the broader consumer-grade GNSS receiver class (e.g., Qualcomm Snapdragon, MediaTek GNSS chipsets), which includes GPS receivers integrated in OPEN-category UAV drones (EASA Reg. 2019/947 [24])—an operational category defined by flight rules, not by receiver hardware—currently used in precision agriculture for crop mapping, orthophoto generation, and vegetation index calculation (NDVI, NDWI) [17]; this extension requires dedicated verification on UAV platforms rather than being assumed from smartphone data alone.

A UAV drone executing an agricultural monitoring mission takes off and lands dozens of times per campaign [25]. Each takeoff/landing creates conditions similar to those identified in EXP10's landing-approach GPS re-acquisition artifact: signal disturbed by multipath reflections from the ground and vegetation, abrupt transition from ground altitude to flight, and rapid GNSS signal re-acquisition. EXP03's velocity spike, by contrast, occurred at cruise altitude and is less directly analogous to the takeoff/landing cycles typical of agricultural UAV operations (Section 4.2). If the first or last photograph in a mapping pass contains a phantom GPS position, the orthophoto generated by Structure from Motion (SfM) will exhibit a systematic geographic displacement at the edges—precisely in the areas where agricultural parcels are delimited [16].

The connection between GPS metadata integrity and automated crop recognition accuracy is plausible: an AI crop classification system trained or operated on drone images with corrupted GPS metadata may produce georeferencing errors that are undetectable by image analysis alone but detectable primarily through EXIF metadata validation—the

methodology presented in this study [7]—pending controlled validation in UAV operational settings (Section 4.6).

From a risk management perspective in precision agriculture, drone data with unvalidated GPS metadata constitutes a source of systematic uncertainty: crop areas affected by water stress, diseases, or pests, calculated on the basis of NDVI/NDWI indices from drone images, may be over- or underestimated if the orthophoto georeferencing exhibits displacements of the order of tens of meters. Systematic validation of GPS EXIF metadata prior to photogrammetric processing thus becomes a recommended component of data quality assurance protocols in drone-based agricultural monitoring.

4.6. Limitations

This study presents several limitations that should be considered when interpreting the results.

First, the entire dataset derives from a single device—Samsung Galaxy A72 (SM-A725F, Qualcomm Snapdragon 720G chipset)—and two European flight routes. The single-device design precludes conclusions about inter-device variability. Future studies should include a minimum of three device models representing different GNSS chipset families (Qualcomm, MediaTek, Broadcom) to assess whether the documented failure modes are chipset-specific or universal to the consumer-grade receiver class.

Both flight experiments were conducted within European airspace at mid-latitudes (approximately 38° N–45° N), where ionospheric activity is moderate and GPS + GLONASS + BeiDou constellation geometry is favorable. The documented velocity artifact pattern may differ for flights at equatorial latitudes (equatorial ionospheric anomaly) or at high latitudes (auroral scintillation zones). Replication on trans-oceanic and ionospherically active routes is recommended before the framework is applied globally.

Future studies investigating GPS metadata integrity during commercial flights should implement a parallel data collection protocol including: (a) simultaneous raw GNSS NMEA logging via a dedicated application (e.g., GPSTest, GNSSLogger) running alongside the photography application; (b) manual recording of airplane mode activation/deactivation events with timestamps; and (c) IMU accelerometer data via a separate logging application. This parallel protocol would enable direct disambiguation of velocity anomalies into their constituent physical causes.

Although the documented behavior is internally consistent and replicable between the two experiments, generalization of the conclusions to other smartphone models or GPS chipsets requires dedicated comparative studies.

Second, data were collected opportunistically, within personal travel activities, not through a controlled experimental protocol. Although the observational methodology is valid and frequently used in real-world GNSS behavior research, the absence of a standardized collection protocol limits the exact reproducibility of capture conditions.

Third, the analysis relies exclusively on EXIF metadata extracted post hoc. IMU data (accelerometer, gyroscope), raw NMEA logs, or information about the airplane mode status at the time of capture were not available—data that would have permitted definitive disambiguation of GPS re-acquisition artifacts from actual spoofing attacks.

Fourth, the statistical tests reported in Sections 3.1 and 3.4 (Fisher's exact test, z-test) treat photographs as independent observations; in reality, photographs from the same device, flight, and session are correlated pseudo-replicates, and the app and flight-condition comparisons are confounded. These tests should be read as descriptive indicators of the magnitude of observed differences, not as confirmatory inferential evidence of causal, app-level, or environment-level effects.

Fifth, the study covers two European routes from the same geographic and climatic period. GPS receiver behavior at cruise altitudes may vary depending on ionospheric conditions, visible satellite constellation, and geographic route—uncontrolled variables in the current observational design.

Despite these limitations, the results provide a comprehensive documentation of the complete EXIF altitude profile from a commercial flight and the cross-context confirmation of the phantom geolocation mechanism, constituting a solid foundation for future comparative studies on multiple devices and diverse routes.

5. Conclusions

This study reports GPS metadata behavior recorded by a single Samsung Galaxy A72 smartphone (Qualcomm Snapdragon 720G chipset) across two commercial European flights. All findings are specific to this device and chipset combination and require replication on additional devices before generalization. This comparative study of GNSS/GPS metadata from two commercial flights documents seven main conclusions, with implications for GPS security, data quality in high-risk AI systems, and georeferencing integrity in precision agriculture with UAV drones.

1. Cross-context evidence for the phantom geolocation mechanism: the complete absence of phantom geolocation in both flight datasets (EXP03: 0/377 photographs; EXP10: 0/65 GPS photographs)—the same Samsung Galaxy A72 device that produces 37.3% phantom geolocation in terrestrial environments with signal obstruction—provides observational evidence consistent with the hypothesis that the phenomenon is strongly associated with GPS constellation visibility, not with hardware characteristics [3]. This is a cross-context replication, by the same research group, providing additional evidence for the mechanism initially described in [3].
2. GPS performance at cruise altitude: Samsung Galaxy A72 with Timestamp Camera records GPS coordinates at a 100% capture rate at altitudes up to 11,439 m WGS84, providing, to the authors' knowledge, one of the most comprehensively documented EXIF altitude profiles covering a commercial flight at high photographic density (377 photographs).
3. RAIM velocity spikes across flight phases: velocity anomalies of 1560–1875 km/h are detected in both experiments—one at cruise altitude (EXP03) and one during landing approach (EXP10)—consistent with GPS re-acquisition following signal disturbance, though the precise physical mechanism cannot be determined from EXIF data alone (Section 4.6). These artifacts are indistinguishable from GPS position-jump spoofing attacks at the EXIF metadata level [10], requiring additional data sources for disambiguation.
4. JPEG EOI structural anomaly: 88% (n = 920) of Samsung Galaxy A72 JPEG files do not contain the standard EOI marker at the end of the file, causing systematic false-positive rejections by naive JPEG integrity validators. Complete file SHA-256 hashing avoided this pitfall in the present dataset and is recommended as the primary integrity-verification method for this device family, pending comparison against alternative validation approaches.
5. Timestamp Camera vs. native camera: GPS-specialized photography applications provide measurably superior metadata quality (100% GPS capture, altitude inclusion) compared to native camera applications at equivalent altitudes, suggesting their preferential use for georeferencing tasks requiring complete metadata coverage, pending validation across additional devices and applications.
6. GPS behavioral spectrum by environment: analysis of 275 photographs captured at Cabo da Roca (38.781° N, 9.499° W) reveals a GPS capture rate of 99.3% with accuracy

below 86 m—compared to 37.3% phantom geolocation in semi-enclosed environments from the same research project. The same Samsung Galaxy A72 device produces a complete GPS behavioral spectrum (from <1% error to >37% phantom), associated primarily with the capture environment rather than with hardware characteristics.

7. Implications for UAV data integrity in precision agriculture: the GNSS metadata failure modes documented in this study—phantom geolocation, velocity artifacts at cruise altitude and during landing approach (see bullet 3 above), and absence of the GPSAltitude field—are plausible for the consumer-grade GNSS receiver class shared by smartphones and OPEN-category agricultural UAV drones [24], though this cross-domain generalization requires controlled experimental verification (Section 4.6). These failures could plausibly affect orthophoto georeferencing and, in turn, automated crop classification accuracy [7,17], pending such validation. Systematic EXIF GPS metadata validation constitutes a recommended component of data quality assurance protocols in drone-based agricultural monitoring, in accordance with the requirements of Regulation (EU) 2024/1689, Article 10(3) [2].

The proposed anti-spoofing/anti-sniffing/anti-tampering framework as a whole is presented as a methodological proposal requiring validation on larger, multi-device, multi-route datasets before operational adoption.

The geographic scope of the study—two European mid-latitude routes—limits conclusions about ionospheric and constellation geometry effects on GPS re-acquisition artifacts. Extension to equatorial and high-latitude flight routes constitutes a priority for future research.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/geomatics6050094/s1, S1: Python script for computing descriptive altitude statistics reported in Table 3.

Author Contributions: E.-C.Ș.: Data curation, Investigation, Software, Validation, Writing—Review and Editing. O.-M.G.: Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Visualization, Writing—Original Draft. F.G.: Resources, Validation, Writing—Review and Editing. R.-G.P.: Supervision, Validation, Writing—Review and Editing. I.-R.P.: Writing—Review and Editing. A.R.: Validation, Writing—Review and Editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This study does not involve human subjects, clinical data, or sensitive personal information of third parties. Approval from an institutional ethics committee (IRB/Ethics Board) was not required. Data were collected exclusively by the principal author (G.O.M.) during personal travel activities, without institutional funding. Photographs included in the article do not contain identifiable persons.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to ongoing research activities.

Acknowledgments: During the preparation of this manuscript, the authors used Claude (Anthropic; Claude Sonnet 4.x models during initial drafting in the first half of 2026, and Claude Sonnet 5 during final revisions in August 2026) as a writing assistance tool for structural organization, language editing, and bibliographic formatting of certain sections. All experimental data, GPS metadata analysis, field observations, and scientific interpretations are exclusively the work of the authors. The AI tool was not used for data generation, statistical analysis, or scientific conclusions. The authors reviewed and edited all AI-assisted content and take full responsibility for the accuracy and integrity of the published work. This declaration is made in accordance with MDPI's AI policy (2023–2026).

Conflicts of Interest: The authors declare no conflicts of interest. The study was conducted independently, in an academic capacity, without institutional or private funding.

References

1. Camera & Imaging Products Association (CIPA); Japan Electronics and Information Technology Industries Association (JEITA). *Exchangeable Image File Format for Digital Still Cameras: Exif Version 2.32*; CIPA DC-008-Translation-2019; CIPA: Tokyo, Japan, 2019. Available online: https://www.cipa.jp/std/documents/download_e.html?DC-008-Translation-2019-E (accessed on 9 June 2026).
2. European Parliament; Council of the European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). *Off. J. Eur. Union* **2024**, *2024*, 1689. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689 (accessed on 9 June 2026).
3. Gămulescu, O.M. *GNSS Behavior Under Extreme Altitude Conditions: From +11,439 m (Commercial Aviation) to −30 m (Tourist Submarine, Atlantic Ocean)-Implications for Data Integrity in High-Risk AI Systems Under GDPR and Regulation (EU) 2024/1689*; Zenodo: Geneva, Switzerland, 2026. [CrossRef]
4. Soni, D. Forensic Value of Exif Data: An Analytical Evaluation of Metadata Integrity across Image Transfer Methods. *Perspect. Leg. Forensic Sci.* **2025**, *2*, 10006. [CrossRef]
5. Wassenaar Arrangement Secretariat. *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Control Lists, Category 7-Navigation and Avionics*; Wassenaar Arrangement: Vienna, Austria, 2023. Available online: https://www.wassenaar.org/control-lists/ (accessed on 9 June 2026).
6. Carroll, J.; Chan, B.; Harner, C.; Reid, T.; Tarantino, P.; Yu, C.Y. Commercial GPS in the Stratosphere: Cell Phone GPS Receiver Performance on a High-Altitude Weather Balloon. In Proceedings of the ION GNSS 2011, Portland, OR, USA, 20–23 September 2011. Available online: https://www.ion.org/publications/abstract.cfm?articleID=9881 (accessed on 9 June 2026).
7. Gămulescu, O.M. Contributii Privind Recunoasterea Automata a Culturilor cu Ajutorul unei Drone (Contributions Regarding the Automatic Recognition of Crops Using a Drone). Ph.D. Thesis, University of Petrosani, Petrosani, Romania, 2024.
8. *RTCA DO-229E*; Minimum Operational Performance Standards for Global Navigation Satellite Systems (GNSS) Airborne Equipment. RTCA, Inc.: Washington, DC, USA, 2017.
9. Borhani-Darian, P.; Li, H.; Wu, P.; Closas, P. Detecting GNSS Spoofing Using Deep Learning. *EURASIP J. Adv. Signal Process.* **2024**, *2024*, 14. [CrossRef]
10. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In Proceedings of the ION GNSS 2008, Savannah, GA, USA, 16–19 September 2008; pp. 2314–2325.
11. Sun, Y.; Yu, M.; Wang, L.; Li, T.; Dong, M. A Deep-Learning-Based GPS Signal Spoofing Detection Method for Small UAVs. *Drones* **2023**, *7*, 370. [CrossRef]
12. Al-Sabbagh, A.; El-Bokhary, A.; El-Koussa, S.; Jaber, A.; Elkhodr, M. Detection of UAV GPS Spoofing Attacks Using a Stacked Ensemble Method. *Drones* **2025**, *9*, 2. [CrossRef]
13. Lehtola, V.V.; Soderholm, S.; Koivisto, M.; Montloin, L. Exploring GNSS Crowdsourcing Feasibility: Combinations of Measurements for Modeling Smartphone and Higher End GNSS Receiver Performance. *Sensors* **2019**, *19*, 3018. [CrossRef] [PubMed]
14. Jiang, C.; Zhou, X.; Chen, H.; Liu, T. UAV Positioning Using GNSS: A Review of the Current Status. *Drones* **2026**, *10*, 91. [CrossRef]
15. Atik, M.E.; Arkali, M. Comparative Assessment of the Effect of Positioning Techniques and Ground Control Point Distribution Models on the Accuracy of UAV-Based Photogrammetric Production. *Drones* **2025**, *9*, 15. [CrossRef]
16. Liu, X.; Lian, X.; Yang, W.; Wang, F.; Han, Y.; Zhang, Y. Accuracy Assessment of a UAV Direct Georeferencing Method and Impact of the Configuration of Ground Control Points. *Drones* **2022**, *6*, 30. [CrossRef]
17. Zhang, C.; Kovacs, J.M. The Application of Small Unmanned Aerial Systems for Precision Agriculture: A Review. *Precis. Agric.* **2012**, *13*, 693–712. [CrossRef]
18. Bian Di Technology Co. *Timestamp Camera*, version 4.x; Bian Di Technology Co.: Beijing, China, 2024. Available online: http://www.timestampcamera.com/ (accessed on 9 June 2026).
19. Pillow Contributors. Pillow (PIL Fork) Documentation: Image.Exif, Version 10.x; Python Imaging Library. 2024. Available online: https://pillow.readthedocs.io/en/stable/reference/Image.html (accessed on 9 June 2026).
20. Hofmann-Wellenhof, B.; Lichtenegger, H.; Wasle, E. *GNSS-Global Navigation Satellite Systems*; Springer: Vienna, Austria, 2008; ISBN 978-3-211-73012-6.
21. European Parliament; Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (General Data Protection Regulation, GDPR). *Off. J. Eur. Union* **2016**, *119*, 1–88.
22. Zidane, Y.; Silva, J.S.; Tavares, G. Jamming and Spoofing Techniques for Drone Neutralization: An Experimental Study. *Drones* **2024**, *8*, 743. [CrossRef]
23. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]

24. European Commission. Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the Rules and Procedures for the Operation of Unmanned Aircraft. *Off. J. Eur. Union* **2019**, *152*, 45–71. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0947 (accessed on 9 June 2026).
25. Guebsi, R.; Mami, S.; Chokmani, K. Drones in Precision Agriculture: A Comprehensive Review of Applications, Technologies, and Challenges. *Drones* **2024**, *8*, 686. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.