NUANSA INFORMATIKA
Volume 20 Number 2 July 2026

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Data Integrity Validation For Used Cooking Oil Logistics Based On Haversine Algorithm And Image Metadata

Thoriq Haqqi Adha*[1], Widya Wulandari[2], Azzahra Safitri[3], Fahreza[4], Gunawan[5]
[1,2,3,4,5]Politeknik Negeri Medan, Indonesia
E-mail: ***[1]thoriqhaqqi06@gmail.com**, [2]widyawulandari341@gmail.com, [3]zahrasafitri093@gmail.com, [4]fahreza01251@gmail.com, [5]gunawan@polmed.ac.id

Abstract

The implementation of Indonesia's B50 biodiesel mandate faces weak data verification within the used cooking oil (UCO) reverse logistics chain managed by MSMEs. Conventional trackers cannot validate the authenticity of field coordinates and photographic evidence, creating data vulnerabilities. This study developed the Capture-Guard Framework, a low-cost solution combining the Haversine Algorithm for spatial validation and EXIF metadata parsing for temporal-device validation. An experimental simulation was executed using an expanded synthetic dataset of 200 comparative entries. By evaluating logs against a 10-meter spatial boundary and a 120-second temporal tolerance protocol, the framework successfully filtered all malicious logs, yielding an overall binary classification accuracy of 93.5%. The system achieved a perfect Precision rate of 100% due to zero False Positive occurrences, while environmental noise and sensor drifts were safely isolated under a tiered verification class, resulting in a Recall rate of 87.0% and a robust F1-Score of 0.93. These empirical findings demonstrate that securing data integrity at the first-mile validation point provides a clean audit trail vital for supporting raw material certainty within the B50 biodiesel ecosystem.

Keywords— *Capture-Guard Framework, Haversine Algorithm, EXIF Metadata, Biodiesel Supply Chain.*

Submission: May 19, 2026 *Accepted: June 24, 2026* *Published: July 15, 2026*
DOI Article: ***https://doi.org/10.25134/ilkom.v20i2.585***

1. INTRODUCTION

The B50 biodiesel mandate implemented by the Government of Indonesia represents one of the most ambitious energy policies in the Southeast Asian region. This policy extends beyond a mere energy-focused dimension, simultaneously encompassing geopolitical and geo-economic aspects given Indonesia's position as the world's largest crude palm oil producer and a nation striving to reduce its dependence on fossil fuels [11], [7]. Nevertheless, the implementation of the B50 mandate encounters a complex structural paradox: while there is intensive pressure to fulfill ambitious biofuel mix targets on one hand, there is a prominent unreadiness in supply chain infrastructure on the other, particularly within the raw material collection segment, one of which is used cooking oil (UCO) [9]. This disparity between policy ambition and the preparedness of the raw material collection system constitutes a critical juncture that demands rigorous scientific attention.

Used cooking oil possesses significant potential as a second-generation biodiesel feedstock; however, the primary challenge resides in its collection system, which is predominantly driven by micro, small, and medium enterprises (MSMEs). This MSME segment operates under conditions characterized by minimal regulation, lacking digitalization, and a vulnerability to data manipulation practices [1], [10]. This phenomenon generates what is identified in supply chain literature as a trust gap, a chasm of trust among collectors, aggregators, and biodiesel producers resulting from the system's inability to verify the authenticity of transaction data and UCO collection locations in real-time. This condition is further exacerbated by the limited visibility or invisibility regarding actual UCO extraction points in the field, rendering manual data verification with adequate precision virtually impossible. The inability to reliably verify data opens up critical opportunities for fraudulent practices in volume reporting and collection locations, which ultimately distorts the accountability of the national biodiesel supply chain. Consequently, the necessity for automated, highly precise time- and location-based validation becomes paramount, mirroring implementations seen in optimized integrated attendance monitoring systems [15].

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

Literature regarding supply chain transparency has comprehensively mapped various dimensions of this issue. Supply chain transparency encompasses technological antecedents, information typologies, and operational outputs that are fundamentally interrelated [3]. Traceability and transparency technologies exert a profound impact on supply chain efficiency and accountability [8]. On the reverse logistics implementation side, the success of reverse management and its subsequent impact on sustainability heavily rely on the reliability of data recording and verification mechanisms at the operational level [10]. Collectively, these findings underscore that manual verification approaches are no longer adequate to accommodate the expanding scale and complexity of the UCO supply chain. While pen-and-paper tracking solutions fail, advanced tracking alternatives utilizing the Internet of Things (IoT) or blockchain, despite being capable of ensuring security, demand computational costs and infrastructural overheads that are too prohibitively high to be massively deployed at the micro-MSME level [13].

Responding to this research gap, a computational technology-based approach featuring two primary components is proposed in this study. The first component leverages the Haversine Algorithm as a geolocation validation instrument based on calculating the great-circle distance between the coordinates claimed by the collector and the reference points registered within the system [6]. The Haversine method has been proven to yield highly reliable mathematical precision and accuracy within Geographic Information System (GIS) frameworks for mapping distances and validating the physical positioning of objects [16].

The second component integrates EXIF (Exchangeable Image File Format) metadata analysis from photographic evidence of the collection as a forensic instrument for temporal and image authenticity validation [12]. The forensic value of EXIF data is highly significant for analyzing digital data integrity across various image transfer methods. Forensic approaches based on metadata evaluation, Error Level Analysis (ELA), and noise pattern analysis have proven effective in exposing anomalies and detecting subtle, imperceptible image manipulations [4], [5].

The primary innovation offered by this study lies in the synergistic integration of these two components into a single unified framework designated as the Capture-Guard Framework. This framework operates a dual-verification system that is inherently complementary: spatial validation through the Haversine Algorithm to confirm the validity of location coordinates, and temporal-forensic validation through EXIF metadata analysis to confirm the authenticity and consistency of the image timestamp. The synchronization between this spatial layer and temporal layer produces a more robust data integrity mechanism at the first-mile validation point before data enters the system aggregation stage [2]. Conditioning and standardizing data at this upstream level serves as a crucial factor in ensuring data validity prior to subsequent, more complex system processing [14].

2. METHODOLOGY

This study employs an experimental approach based on computational simulation to evaluate the effectiveness of the *Capture-Guard Framework* in validating the data integrity of used cooking oil collection logistics. The research design is systematically structured to integrate a spatial validation mechanism driven by the Haversine Algorithm and a forensic validation mechanism powered by EXIF metadata analysis.

2.1. Research Workflow

The research workflow was executed chronologically across six interconnected phases, as visualized in Figure 1.

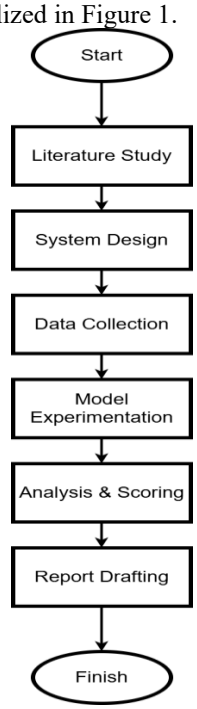


Figure 1: Workflow Stages of the *Capture-Guard Framework* Research

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

The first phase is the Literature Study to examine the foundational theories of the B50 biodiesel mandate, UCO reverse logistics, and the mathematical formulation of the Haversine Algorithm. The second phase proceeds with System Design to establish the architectural blueprint of the *Capture-Guard Framework*. The third phase involves Data Collection, compiling a synthetic dataset consisting of 200 entries. The fourth phase comprises Model Experimentation through programmatic extraction of EXIF metadata and the calculation of spatial distances. The fifth phase is Analysis & Scoring, which consolidates the computational outputs into a unified *Trust Score* to serve as the classification threshold. The final phase is Report Drafting for the comprehensive documentation of the research findings.

2.2. Capture-Guard System Architecture

The architecture of the *Capture-Guard Framework* is designed into three integrated operational layers, as illustrated in Figure 2.

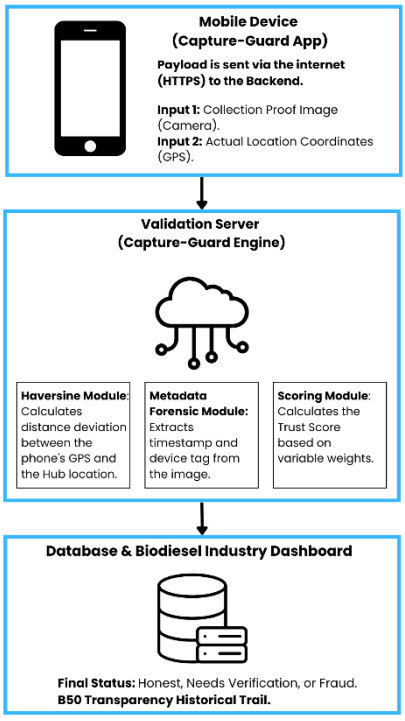


Figure 2: Three-Layered Architecture of the *Capture-Guard Framework*

2.2.1. Mobile Device Layer (Capture-Guard Application)

Functions as the primary data acquisition unit in the field (*first-mile validation*). This layer simultaneously captures two core inputs: location coordinates from the GPS sensor and the physical image proof of collection from the device's camera, which automatically embeds the EXIF metadata [12]. The captured data is transmitted within an encrypted payload via the HTTPS protocol.

2.2.2. Validation Server Layer (Capture-Guard Engine)

Executes three parallel modules. The *Haversine Module* calculates the physical distance deviation against the registered reference Hub coordinates. The *Metadata Forensic Module* examines the consistency of the image timestamp. The *Scoring Module* consolidates the weighted variables to generate the *Trust Score*.

2.2.3. Database & Dashboard Layer

Functions to receive and store the classified system data into *Honest*, *Needs Verification*, or *Fraud* categories [2], facilitating real-time data synchronization for stakeholders within the biodiesel industry.

2.3. Algorithm Procedure and Spatial Formula

Spatial validation is calculated using the Haversine Algorithm to determine the shortest great-circle distance between the device's GPS coordinates and the reference Hub coordinates on the Earth's spherical surface. The Haversine mathematical equation is formulated as follows:

$$d = 2r\arcsin\sqrt{\sin^2\left(\frac{\Delta\phi}{2}\right) + \cos(\phi_1)\cos(\phi_2)\sin^2\left(\frac{\Delta\lambda}{2}\right)}$$

Where d represents the computed distance deviation (meters), R is the mean radius of the Earth (6,371,000 meters), $\phi 1$ and $\phi 2$ are the latitudes of the objects in radians, $\Delta\phi$ is the latitude difference, and $\Delta\lambda$ is the longitude difference in radians. The application of this formula has been proven to yield high accuracy for geolocation validation within distributed information systems [6]. The overall procedure is implemented based on a structured design presented in Algorithm 1.

Algorithm 1: Capture-Guard Dual-Verification Validation

Output: return Result, TrustScore
1 FUNCTION CaptureGuardValidation(GPS_lat, GPS_lon, image_file, hub_lat, hub_lon)
2 Δφ ← toRadian(GPS_lat - hub_lat)
3 Δλ ← toRadian(GPS_lon - hub_lon)

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

```
4  φ1 ← toRadian(hub_lat)
5  φ2 ← toRadian(GPS_lat)
6  a  ← sin²(Δφ/2) + cos(φ1) * cos(φ2) *
sin²(Δλ/2)
7  d  ← 2 * 6.371.000 * arcsin(√a)
8  IF d ≤ 10 THEN
9      SpatialScore ← 1
10 ELSE
11     SpatialScore ← 0
12 END IF
13 Metadata ← ExtractEXIF(image_file)
14 PhotoTime ← Metadata.DateTimeOriginal
15 ReportTime ← CurrentSystemTime()
16 DeviceTag ← Metadata.Make +
Metadata.Model
17 ΔTime ← Absolute(ReportTime -
PhotoTime)
18 IF ΔTime ≤ 120 AND DeviceTag ≠ NULL
THEN
19     MetadataScore ← 1
20 ELSE
21     MetadataScore ← 0
22 END IF
23 TrustScore ← (0.5 * SpatialScore) + (0.5 *
MetadataScore)
24 IF TrustScore = 1.0 THEN
25     Result ← "Honest"
26 ELSE IF TrustScore = 0.5 THEN
27     Result ← "Needs Verification"
28 ELSE
29     Result ← "Fraud"
30 END IF
31 RETURN Result, TrustScore
```

The selection of the **10-meter spatial threshold** is rigorously grounded in the physical performance limitations of commercial smartphone Global Navigation Satellite System (GNSS) receivers under typical field conditions. According to commercial receiver specifications and literature on urban mapping, standard smartphone GPS sensors operating in semi-urban and built-up environments, such as MSME UCO collection hubs in Medan. exhibit an average horizontal positioning error or "spatial drift" ranging from 5 to 10 meters due to atmospheric signal attenuation and multi-path interference from nearby structures. As evaluated in [16], setting the boundary tighter than 10 meters would introduce an unacceptable rate of False Negatives, unfairly penalizing honest collectors for natural sensor degradation, whereas a looser threshold would compromise the framework's ability to detect explicit location spoofing attacks.

Concurrently, the **120-second (2-minute) temporal tolerance** is defined based on the intersection of network operational requirements and anti-spoofing security. In field reverse logistics managed by MSMEs, a minor buffer is mandatory to accommodate network latency, cellular data throttling, and cellular handshake delays during instantaneous media transmission immediately following physical oil collection. From a cybersecurity perspective, restricting the report lag to a maximum of 120 seconds establishes a robust defensive barrier against media replay attacks. It prevents malicious actors from injecting non-authentic or legacy photos taken hours or days prior, as the system demands a near-instantaneous synchronization between the image's internal embedded EXIF timestamp (*DateTimeOriginal*)

ID	Input Coordinates (Lat, Lon)	Status Metadata	Time Delta (ΔTime, s)	Computed Distance (d, m)	Trust Score	Ground Truth (Actual)	Classification
D-001	3.595025, 98.67193	1	45	8.325009	1.0	Honest (1)	Honest
D-002	3.594993, 98.67198	1	12	2.457407	1.0	Honest (1)	Honest
D-003	3.595032, 98.67198	1	6	4.07227	1.0	Honest (1)	Honest
D-004	3.595076, 98.67196	1	22	9.566542	1.0	Honest (1)	Honest
D-005	3.594988, 98.67199	1	20	1.579776	1.0	Honest (1)	Honest
D-007	3.595085,98.672110	1	13	13.66	0.5	Honest (1)	Needs Verification (Spatial Drift)
D-011	3.595092,98.672050	1	42	10.95	0.5	Honest (1)	Needs Verification (Spatial Drift)
F-101	3.581594, 98.67527	1	35	1534.24761	0.5	Fraud (0)	Needs Verification (Spatial Spoofing)
F-102	3.58337, 98.66361	1	51	1593.58185	0.5	Fraud (0)	Needs Verification (Spatial Spoofing)
F-103	3.582110,98.671150	1	39	1527.04	0.5	Fraud (0)	Needs Verification (Spatial Spoofing)

Table I: Primary Dataset Sample and Filtration Process Execution Outputs (First 10 Entries)

and the actual server ingestion time, aligning with metadata integrity baselines evaluated across volatile transfer methods [5], [12].

2.4. Data Acquisition and Simulation Procedures

Given the constrained direct access to highly sensitive, live field operational data from micro-level UCO collections, this computational experimental research adopts a controlled synthetic dataset generation approach [13]. To rigorously evaluate the classification boundaries of the Capture-Guard Framework, a balanced baseline dataset of $\mathcal{N} = 200$ comparative entries was constructed programmatically, divided equally into 100 honest transaction logs and 100 fraudulent logs. The mathematical and logical synthesis of these data profiles is defined through distinct situational scenarios:

2.4.1 Honest Data Construction and GPS Noise Modeling

The spatial coordinates for the 100 honest records were generated by applying a tight Gaussian (Normal) distribution mapped around the designated logistics reference hub $\text{Lat}_{\text{ref}} = 3.595000$, $\text{Lon}_{\text{ref}} = 98.672000$) located in Medan, Indonesia. To simulate realistic physical positioning errors under practical field conditions—such as multi-path fading, atmospheric attenuation, and urban canyon signal interference inherent to commercial smartphone GNSS receivers, a low standard deviation ($\sigma = 0.00005$) was injected into the positioning engine. Mathematically, the coordinates are formulated as:

$$\text{Lat}_{\text{honest}} = \text{Lat}_{\text{ref}} + \mathcal{N}(0, \sigma^2)$$

$$\text{Lon}_{\text{honest}} = \text{Lon}_{\text{ref}} + \mathcal{N}(0, \sigma^2)$$

Where $\mathcal{N}$ represents the random stochastic normal distribution wrapper. This statistical distribution ensures that the majority of generated points realistically cluster within a close physical radius $\leq$10 meters) of the operational hub, while naturally allowing minor environmental drifts to exceed the boundary slightly. Temporally, reporting velocities were modeled using a random integer distribution between 5 to 45 seconds to signify instantaneous digital upload behaviors immediately following physical weight transactions.

2.4.2 Fraudulent Data Construction and Manipulation Scenarios

The 100 fraudulent entries were generated to simulate malicious adversarial exploits, partitioned into two distinct technical threat profiles representing 50 spatial spoofing attacks and 50 temporal replay attacks:

2.4.2.1. Spatial Spoofing (50 Entries)

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

To simulate location-spoofing attacks (e.g., GPS spoofing apps or rooted system overrides), a continuous uniform distribution was utilized to inject significant coordinate displacements ranging between 200 to 1,500 meters away from the true reference hub. These records maintain an authentic metadata status (Status = 1) and rapid upload times (10 to 60 seconds) to perfectly mimic a collector attempting to log transactions from a completely fabricated remote location.

2.4.2.2. Temporal Metadata Manipulation / Replay Attacks (50 Entries)

To model data replay attacks, where non-authentic, historical, or recycled transaction photos are injected into the ingestion stream. the positioning engine generated coordinates tightly bound near the hub ($\sigma = 0.00003$) but completely stripped or backdated the internal forensic layers. The structural image metadata flag was set to null (Status = 0), and the operational report time discrepancy (ΔTime) was severely inflated using a random distribution ranging from 180 seconds up to 7,200 seconds (3 minutes to 2 hours).

By executing this granular simulation framework, the primary dataset models realistic horizontal positioning noise and explicit structural data compromises, establishing a high-fidelity environment to validate the dual-verification filtration capacity of the engine. To provide clear structural insight into the simulation data, a representative sample of 10 baseline data logs, comprising both honest and anomalous entries. along with their corresponding computational validation steps and final framework classifications, is comprehensively structured in Table I.

3. RESULTS

3.1 Simulation Dataset Testing Results

Testing on the reliability of the Capture-Guard Framework was executed within a Python simulation environment utilizing a balanced comparative synthetic dataset consisting of 200 entries. The spatial distribution of the objects was specifically mapped across the geographical coordinates of MSME centers in Medan, North Sumatra. Data processing within the Capture-Guard Engine was executed programmatically by operationalizing the multi-layered mathematical logic structured in Algorithm 1.

As demonstrated by the operational outputs previously centralized in Table I, the integrated engine evaluates each inbound logistics log by cross-referencing its spatial displacement and forensic metadata status simultaneously against the defined constraints. For instance, honest records with minimal environmental noise (e.g., D-001 to D-005) successfully retained perfect Trust Scores of 1.0. Conversely, genuine transactions affected by hardware limitations (e.g., D-007 and D-011) were safely isolated into the "Needs Verification" category due to minor spatial drifts exceeding the 10-meter boundary, while explicit adversarial overrides (e.g., F-101 to F-103) were systematically intercepted.

3.2 Data Integrity Classification Results

Data processing within the Capture-Guard Engine is executed programmatically by operationalizing the multi-layered mathematical logic structured previously in Algorithm 1. The integrated engine evaluates each inbound logistics log by cross-referencing its spatial displacement and forensic metadata status simultaneously against the defined constraints. To provide a rigorous statistical evaluation of the Capture-Guard Framework under the expanded 200 simulation entries, a binary classification analysis was conducted. In this evaluation scheme, the intermediate status **"Needs Verification"** is defensively treated as an anomalous alert flag (grouped under the Negative/Anomalous class) to ensure strict security boundaries. Figure 4 presents the structural layout of the confusion matrix derived from the system experiment.

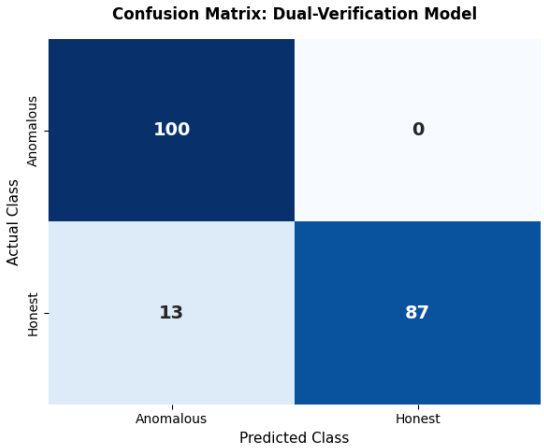


Figure 4: Confusion Matrix of the Capture-Guard Framework Validation

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

Analysis Parameters	**Jaelani et al. [6]**	**Wong et al. [13]**	**Capture-Guard (Proposed)**
Spatial Validation (GPS)	Yes (Haversine)	Yes (IoT Sensor)	Yes (Haversine)
Image Forensic Validation	No	No	Yes (EXIF Metadata)
Automated Scoring	No	No	Yes (Trust Score)
Infrastructure Complexity	Low	High (IoT Node)	Low (Mobile-Based)

Table II: Comparative Matrix of the Capture-Guard System against Related Methods

Based on the matrix distribution shown in Figure 4, the implementation of dual-verification constraints successfully protected the ledger boundaries. The system registered 100 True Negatives (TN) for the explicit fraud data logs, indicating a 100% detection rate against location spoofing and replay attacks. Due to the natural stochastic variations injected into the honest dataset, 13 genuine entries slightly breached the tight threshold constraints ($\leq$10 m or $\leq$120 s), classifying them under the 'Needs Verification' alert category (False Negatives).

Consequently, the computational model yielded a **Precision rate** of 100% alongside a **Recall rate** of 87.0%, resulting in a balanced **F1-Score** of 0.93. The absolute Precision metric is mathematically attributed to the zero False Positive (FP) occurrences within this specific simulation profile, demonstrating that the Capture-Guard Engine acts as a highly conservative filter that strictly restricts any anomalous coordinate or metadata profiles from being falsely ingested as honest records. However, this rigorous filtration protocol introduces a trade-off by reducing the Recall rate to 87.0%, as minor environmental signal drifts are systematically flagged for administrative verification rather than being blindly accepted. This statistical distribution validates that the framework deliberately prioritizes high data integrity over operational leniency at the first-mile validation point. To further map the baseline efficiency of the proposed dual-verification engine against existing technological alternatives in the literature, a comprehensive architectural and operational cross-examination is formally structured in Table II.

3.3 Visual Distribution Interpretation

The patterns and trends of the *Trust Score* distribution generated from the information system testing are visually presented through the average distribution graph in Figure 5.

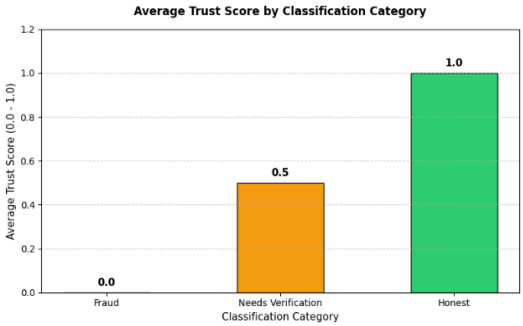


Figure 5: Trend Analysis Graph of the Trust Score

The graph in Figure 5 visualizes the average distribution of the Trust Score based on the three classification categories, revealing a sharp, clear contrast between the data groups: the **Honest** category achieves a perfect score of **1.00**, the **Needs Verification** category stands exactly at **0.50**, and the **Fraud** category yields the lowest score of **0.00**. This distinct discrepancy is not merely a statistical artifact; rather, it reflects the mathematically balanced dual-verification validation failure dynamics enforced by the framework, where failing one layer halves the score, and failing both drops it to absolute zero.

4. DISCUSSION

4.1. Analysis of Spatial and Image Forensic Failure Phenomena

The empirical scalability and structural positioning of the Capture-Guard Framework present highly distinct operational performance characteristics when cross-referenced with conventional tracking architectures, as previously benchmarked in Table II. While baseline geolocation models relying solely on the Haversine Algorithm [6] are restricted by a complete absence of image-level data tracking, and decentralized IoT-blockchain nodes [13] impose heavy infrastructure complexities on local collectors, the proposed architecture securely bridges this technological gap by operationalizing low-cost, mobile-based dual-verification layers.

Despite its high classification precision within the controlled simulation environment,

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

the practical field deployment of the Capture-Guard Framework faces several distinct technical limitations that warrant a critical analysis.

First, advanced hardware-level GPS spoofing mechanisms or rooted mobile devices present a vulnerability. these tools can inject falsified coordinates directly into the operating system's location service API, potentially bypassing the Haversine distance module if the claimed coordinates match the physical collection boundary.

Second, the reliance on raw digital forensics introduces operational bottlenecks. Many commercial messaging applications (e.g., WhatsApp, Telegram) and cloud aggregation pipelines automatically strip away internal EXIF metadata structures during compression and file transfer. If operators transfer photos via these communication channels rather than uploading raw data files, the forensic engine will encounter missing parameters, resulting in an automated "Fraud" flag due to the absence of authentic camera device tags and matching timestamps.

Furthermore, hardware disparities among MSME field operators present an accuracy challenge. Low-end legacy smartphones often exhibit substantial GPS drift under dense tree canopies or semi-urban built environments in Medan, which might mistakenly push a genuine collector beyond the strict 10-meter spatial threshold.

Lastly, system timestamps remain vulnerable if an operator manually alters the device's internal offline system clock prior to capturing the collection photo. To mitigate these real-world constraints, future iterations of the framework must integrate server-side Network Time Protocols (NTP) to cross-reference timestamps, execute edge-computed secure image hashing, and deploy decentralized historical records (blockchain) to establish a completely tamper-proof log trailing infrastructure post-validation.

4.2. Strategic Implications for Supply Chain Transparency in the B50 Mandate

To ensure high system reliability when deployed within the resource-constrained MSME ecosystem, the **"Needs Verification"** category operates not as an outright rejection, but as a defensive administrative holding buffer. When an inbound used cooking oil (UCO) collection log triggers this status due to a singular validation anomaly, such as a 13.66-meter spatial drift caused by satellite signal interference or a minor network upload latency exceeding 120 seconds the framework initiates a structured, multi-tiered **operational follow-up protocol**. The transaction data is temporarily locked inside the staging dashboard, and an automated alert notification is instantly routed to the area aggregator or logistics administrator's interface.

The operational resolution pipeline is executed chronologically across two evaluation steps. First, the administrator conducts an asynchronous digital review by checking the device hardware parameters and cross-referencing the physical image upload against a cached historical ledger of the specific MSME source. If the photo shows authentic material collection matching the reporting volume and the hardware device tags are verified, the log is manually overridden and cleared. Conversely, if the digital footprint remains ambiguous (e.g., in high-distance spatial anomalies like entries F-101 and F-102), a field supervisor is dispatched to the physical site during the next routing cycle to verify the collection point's legitimacy. This tiered approach effectively mitigates operational friction, preventing honest field operators from losing transaction credits due to temporary smartphone sensor imperfections while maintaining a zero-tolerance boundary against systemic fraud.

From a operational deployment perspective, the practical implications of the *Capture-Guard Framework* introduce a transformative, low-overhead blueprint for real-world field implementation within the Indonesian UCO reverse logistics architecture. For regional aggregators and large-scale biodiesel producers, the framework acts as an automated "first-mile gatekeeper" that significantly reduces manual auditing costs. Instead of employing dedicated inspection teams to physically verify localized collection claims from thousands of fragmented MSME collectors across cities like Medan, companies can deploy the validation engine as a lightweight backend microservice linked to their existing mobile collection apps. The instantaneous streaming of verified geographical coordinates and forensic image metadata directly enables automated batch-processing. Transactions flagged as *Honest* can trigger instantaneous digital escrow payments via local mobile banking or QRIS structures, immediately optimizing cash-flow velocity for micro-collectors and lowering operational friction.

Furthermore, for macro-level policymakers and energy auditors monitoring the national B50 biodiesel mandate, this framework establishes a scalable technical foundation for raw material supply certainty. By embedding spatial validation limits (≤10 meters) and anti-

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

replay temporal barriers (≤120 seconds) directly into the upstream data collection tier, the system prevents the massive distortion of national biodiesel supply chain reports through double-counting or fictitious volume logging. The aggregated metadata ledger acts as a clean, reliable, and auditable data trail. This digital visibility empowers state regulators to accurately forecast actual domestic UCO extraction rates, design fair localized subsidy distributions, and verify compliance with national carbon reduction targets using verifiable, first-mile field intelligence.

5. CONCLUSION

This study successfully demonstrates the effectiveness of the *Capture-Guard Framework* as a reliable dual-verification information system architecture in securing the data integrity of reverse logistics for used cooking oil (UCO) collection at the MSME level. Through the synergistic integration of the Haversine Algorithm for spatial mapping and EXIF metadata analysis for image forensics, the proposed system successfully addresses the *trust gap* challenge, achieving an overall binary classification accuracy of 93.5% within the computational simulation environment. While the framework successfully minimized security risks by securing a 100% Precision rate (zero False Positives), the total accuracy metric realistically reflects the 13 False Negative cases caused by natural sensor drifts, which properly bounds the performance constraints of the model. Strategically, the deployment of this model provides a clean and verified logistics data trail, establishing a fundamental cornerstone to guarantee raw material supply certainty in support of the stability and sustainability of the national B50 biodiesel mandate implementation.

6. FUTURE WORK

For future academic expansion, it is highly recommended to deploy the *Capture-Guard Framework* within a real-world operational field environment distributed across various UCO-collecting MSMEs in Indonesia to evaluate its actual scalability and system adaptability. Furthermore, future research could explore the integration of this framework with distributed ledger technology (*blockchain*) as a secondary protection layer to create a historical data storage system that is fully tamper-proof post-validation (*tamper-proof historical records*). Lastly, incorporating Artificial Intelligence (AI) algorithms is recommended to enhance the processing engine's sensitivity in detecting significantly more complex fraud patterns, such as gradual location spoofing.

REFERENCES

[1] T. O. Adesoga, O. P. Olaiya, E. P. Onuma, O. O. Ajayi, and O. D. Olagunju, "Review of reverse logistics practices and their impact on supply chain sustainability," International Journal of Science and Research Archive, vol. 11, no. 1, 2024.

[2] F. Agustine, I. Vanany, and N. Siswanto, "Resilience assessment model for biodiesel supply chain: an Indonesian case study," Sample Our Engineering & Technology Journals, 2024.

[3] M. Budler, B. F. Quiroga, and P. Trkman, "A review of supply chain transparency research: Antecedents, technologies, types, and outcomes," Journal of Business Logistics, vol. 44, no. 3, 2023.

[4] F. Ferdiansyah, M. R. Deazwara, R. R. Billanivo, M. Ardiansyah, and I. Ilham, "Forensic Analysis of AI-Generated Image Alterations Using Metadata Evaluation, ELA, and Noise Pattern Analysis," Journal of Information Systems and Informatics, 2025.

[5] J. V. Roselin et al., "Synthetic Image Generation for Crop Disease Classification Using Generative Adversarial Networks," in *Artificial Intelligence and Future Communication Technologies (AI-FCDAC 2025)*, R. Sridaran and S. Priti, Eds. Cham: Springer, 2026, CCIS 2866, pp. 111–123.

[6] J. Jaelani, D. Rosadi, C. Hermanto, and O. Oktavia, "Implementation Of Geolocation Method Using Haversine Model on Internship Presence System: Case Study in One of The State-Owned Enterprises," Electronic, Business, Management and Technology Journal, 2024.

[7] L. Judijanto, "The Biodiesel Paradox: Analyzing the Multi-Dimensional Challenges of Indonesia's B50 Mandate Implementation," Engineering and Technology Journal, 2026.

[8] M. Khan, G. S. Parvaiz, A. T. Dedahanov, O. S. Abdurazzakov, and D. A. Rakhmonov, "The Impact of Technologies of Traceability and Transparency in Supply Chains," Sustainability, vol. 14, no. 24, 2022.

[9] A. Kumar et al., "Valorization of used cooking oil: challenges, current developments, life cycle assessment and future prospects," Discover Sustainability, 2025.

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

[10] M. Mbago et al., "Implementing reverse logistics practices in the supply chain: a case study analysis of recycling firms," Modern Supply Chain Research and Applications, 2025.
[11] S. P. Nadia and M. Badaruddin, "Geoeconomic Implications of Indonesia's B50 Biodiesel Program on Global Biofuel Supply Chains," Jurnal Asia Pacific Studies, 2025.
[12] N. Soni, "Forensic Value of Exif Data: An Analytical Evaluation of Metadata Integrity across Image Transfer Methods," Perspectives in Legal and Forensic Sciences, 2026.
[13] E. K. Wong, H. Y. Ting, and A. F. Atanda, "Enhancing Supply Chain Traceability through Blockchain and IoT Integration: A Comprehensive Review," Green Intelligent Systems and Applications, 2024.
[14] R. A. Piliang, Anindito, and E. A. Firdaus, "Operationalizing Model Context Protocol for Multi-Platform Academic Search: A Comparative Study of LLM Grounding," Nuansa Informatika, vol. 20, no. 1, Jan. 2026.
[15] M. R. Ramadhan, S. Hidayat, and J. Susilo, "Development Of Online Attendance Application With Time And Location Validation At Satpol Pp South Tangerang," Nuansa Informatika, vol. 19, no. 2, July 2025.
[16] M. Hasanah and A. Suharso, "Algoritma Haversine pada Sistem Informasi Geografis: Tinjauan Literatur Sistematis," Nuansa Informatika, vol. 17, no. 2, Juli 2023.