International Core Journal of Engineering Volume 12 Issue 4, 2026
ISSN: 2414-1895 DOI: 10.6919/ICJE.202604_12(4).0001

Trustworthy Traceability for Logistics Chains Using Latent Fingerprints and Quality-Aware Score Fusion

Haonan Wu, Xinwei Liu*

Zhejiang Wanli University, Ningbo, Zhejiang 315100, China

*Corresponding author: xinwei_liu@yeah.net

Abstract

Modern logistics chains involve multiple handover stages, during which evidence can be easily lost or tampered with, making responsibility tracing difficult. To address this issue, this paper proposes a quality-aware trustworthy evidence preservation and provenance method based on latent fingerprints. The method constructs an event-driven evidence package for each logistics event and adopts a hybrid storage architecture: event metadata and evidence digests are recorded on-chain, while latent fingerprint data and auxiliary materials are encrypted and stored off-chain, thereby forming a verifiable evidence chain. In addition, a quality-aware mechanism fuses latent fingerprint quality indicators with matching scores to improve evidence usability. We treat latent fingerprint usability as part of the provenance record by storing a quality-fused credibility score to support dispute investigation. Experimental results show that the proposed quality-fusion strategy outperforms a matcher-only baseline in verification performance. In the overhead evaluation, the scheme achieves higher write efficiency and lower on-chain storage footprint under typical workloads, meeting the requirements for continuous event recording and rapid trace-back in logistics operations. Moreover, the proposed method can effectively detect tampering attacks, thereby ensuring evidence integrity and enabling trustworthy traceability in logistics scenarios. Overall, the proposed approach provides a technical path that balances usability, trustworthiness, and compliance for logistics dispute evidence collection and responsibility attribution.

Keywords

Latent Fingerprint; Blockchain; Traceability; Trustable Digital Evidence.

1. Introduction

As the scale of express logistics continues to expand, parcels circulate frequently across multiple stages-including pickup, in-transit handoffs, and last-mile delivery-involving a wide range of participants such as senders, couriers, service stations/sorting centers, and platforms. While multi-party participation, multi-stage operations, and high-frequency handovers substantially improve service efficiency, they also expose persistent issues: when incidents such as damage, loss, tampering/substitution, or delivery disputes occur, there is often no continuous, objective, and verifiable chain of evidence. Consequently, liability determination tends to rely on manual records, oral statements, or fragmented multimedia materials, which are prone to evidence gaps, ex post supplementation, tampering allegations, and limited traceability. Therefore, constructing a trustworthy evidence [1] chain for logistics processes that enables effective traceability and verification without imposing excessive operational overhead has become a critical requirement for dispute resolution and platform governance.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202604_12(4).0001

Among the various forms of evidence available for forensics, latent fingerprints [2] offer distinctive value. On the one hand, latent fingerprints encode contact relationships; fingerprint traces collected from key carriers such as outer packaging, sealing tapes, and waybills can provide auxiliary cues for abnormal contact, unauthorized opening, and other illicit behaviors, as shown in Figure 1. On the other hand, latent fingerprints are sensitive biometric data, and their acquisition, storage, and sharing must comply with privacy regulations. Moreover, latent fingerprints in logistics settings are frequently affected by substrate variability, background texture, contamination, abrasion, and partial impressions, leading to substantial quality fluctuations [3] and, consequently, unstable matching reliability [4]. These considerations indicate that merely writing data on-chain or logging process traces is insufficient to support the practical use of latent fingerprints in logistics forensics. It is necessary not only to ensure evidence integrity and tamper resistance at each stage of evidence recording and use, but also to address the uncertainty of latent fingerprint quality in real-world settings, so that the evidence chain is not only trustworthy but also usable. To evaluate usability-aware fusion of latent fingerprints in logistics scenarios, we conduct experiments on the Latent Fingerprint in the Wild (LFIW) database [5]. The database contains latent fingerprints deposited on diverse surfaces along with corresponding reference impressions, covering common conditions such as cluttered backgrounds and partial impressions, and can serve as a proxy for the quality uncertainty of latent fingerprint samples on logistics carriers such as tapes, waybills, and cartons.

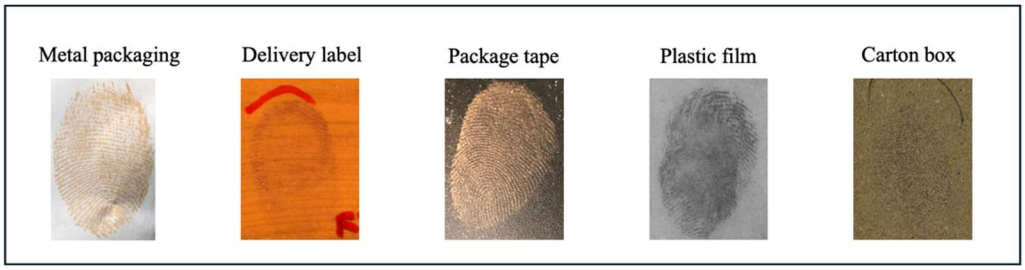

Figure 1. Example of Latent Fingerprint in Logistics (e.g., Metal packaging, Delivery label, Package tape, Plastic film, Carton box)

To address these challenges, we propose a quality-aware trustworthy evidence preservation and provenance method for latent fingerprints in logistics chains. The method abstracts pickup, in-transit handoffs, and delivery as event nodes, and constructs an evidence package for each node to bind the latent fingerprint with the corresponding event information. A hybrid storage architecture is adopted: event metadata and encrypted digests of evidence packages are recorded on-chain, while the original evidence is encrypted and stored off-chain, thereby forming a trustworthy evidence chain. In addition, a quality-aware mechanism is introduced to fuse fingerprint quality indicators with matching scores, effectively improving the usability of latent fingerprints. Experimental results show that the proposed quality-aware fusion strategy yields measurable improvements. Moreover, under a lightweight on-chain recording setting, the evidence preservation and provenance procedures can be performed in a timely manner with feasible overhead. The method can also effectively detect common attacks such as off-chain tampering and missing evidence, which verifies its practicality and security in logistics scenarios.

Overall, we propose an event-based provenance framework for latent fingerprints in logistics. Metadata and evidence digests are recorded on-chain, while encrypted evidence packages are stored off-chain. Dispute investigation is supported through event-chain replay, hash-link validation, and digest recomputation. A quality-aware score fusion module is further incorporated to assess evidence integrity and usability. Experimental results confirm the method's effectiveness, overhead feasibility, and robustness against common tampering behaviors.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202604_12(4).0001

2. Related Work

Trustworthy provenance studies in logistics and supply chains [6] typically model the process as a sequence of events and record key information, such as order status updates, handover logs, and exception handling, to improve transparency and support liability tracing. Existing solutions generally fall into two categories. One line relies on fully on-chain recording of end-to-end states [7], using blockchain immutability to provide tamper-evident logging. The other line adopts a hybrid on-/off-chain design [8], storing digests or indices on-chain while keeping large-volume business data off-chain to reduce on-chain storage overhead and improve throughput. At the application level, provenance systems are mainly used for authenticity verification, responsibility attribution, and auditing. However, the use of biometric evidence in logistics [9] dispute forensics is still uncommon, and end-to-end designs that explicitly account for evidence usability remain limited.

In multi-party logistics systems involving senders, carriers, service stations, platforms, regulators, and arbitration bodies, data sharing must simultaneously satisfy least-privilege access, auditability, and privacy compliance. Prior studies generally employ identity authentication and authorization mechanisms, implementing access management for sensitive data through workflows such as registration, authorization, verification, and auditing. These mechanisms are often combined with encrypted storage, on-chain digest anchoring, key escrow, or policy-based controls to prevent direct exposure of sensitive information. In cross-organization settings, contract-based authorization logic [10] can further encode access conditions into executable rules, making evidence retrieval traceable and enforceable in terms of accountability. Nevertheless, most existing work focuses on whether access is permitted, while paying insufficient attention to questions that are crucial for real dispute arbitration-namely, whether the evidence is worth retrieving, whether retrieved evidence is credible, and how the intrinsic quality of evidence should be characterized.

Biometric information [9] is intrinsically more privacy-sensitive due to its irreplaceability and strong linkage to individuals. To enable secure biometric sharing, the literature commonly adopts template-based representations, encrypted storage, digest-based integrity verification, contract-mediated authorization [10] , and audit trails to ensure controllability and accountability throughout the sharing process. Compared with actively captured modalities such as face or iris, latent fingerprints are passively deposited and collected in situ, making them well-suited for dispute forensics where contact relationships are of interest. Accordingly, latent fingerprints have practical potential on carriers such as logistics sealing tapes and package surfaces. However, latent fingerprints are highly susceptible to substrate properties, background texture, contamination/abrasion, partial impressions, and imaging conditions, leading to substantial uncertainty in usability; therefore, mere preservation does not guarantee their effectiveness in subsequent verification.

Latent fingerprint quality assessment [11] aims to characterize sample comparability and information completeness, and is often used to support operational decisions (e.g., whether to enter automated matching, whether enhancement or re-capture is required). In recent years, beyond single quality metrics, an increasing body of work has explored combining quality scores with matching scores and using learning-based fusion models [12] to output more reliable confidence estimates, thereby improving performance under complex backgrounds and low-quality conditions [13]. This work is particularly relevant to logistics. By recording fused credibility scores as part of the provenance metadata, a provenance system can convey not only where evidence comes from and whether it has been altered, but also how usable the evidence is for subsequent verification. However, most studies on quality assessment and score fusion are developed primarily to improve matching performance in forensic pipelines. They are seldom designed together with logistics-specific requirements, such as event-chain evidence preservation, retrieval decisions, and mechanisms for detecting off-chain tampering.

Prior studies have laid the groundwork for logistics provenance, access control, biometric data protection, and latent fingerprint quality modeling, but their integration into logistics dispute forensics remains limited [14]. Most provenance systems focus on tamper-evident process logs, while

ISSN: 2414-1895 DOI: 10.6919/ICJE.202604_12(4).0001

evidence-package modeling and evidence usability are often missing. Access-control mechanisms are mainly designed to determine whether evidence can be accessed. Quality-aware fusion is typically studied in isolation for recognition performance and is rarely combined with event-chain preservation and tamper detection. To address these issues, we store the outputs of quality fusion as provenance metadata and build an event-based preservation and verification workflow, which we validate through evaluations of effectiveness, overhead, and security.

3. Method

3.1 Process Quality-Aware Score Fusion Framework for Latent Fingerprints

Latent fingerprints collected in logistics scenarios are often affected by contamination, frictional abrasion, pose variations, and differences in substrate materials, which makes the scores produced by the same matcher exhibit pronounced instability across samples of varying quality. To enhance the usability and interpretability of latent fingerprint evidence in subsequent dispute verification, we introduce a quality-aware score fusion module at the evidence level, jointly modeling matching similarity and sample quality to yield a more robust credibility estimate. The overall workflow is illustrated in Figure 2.

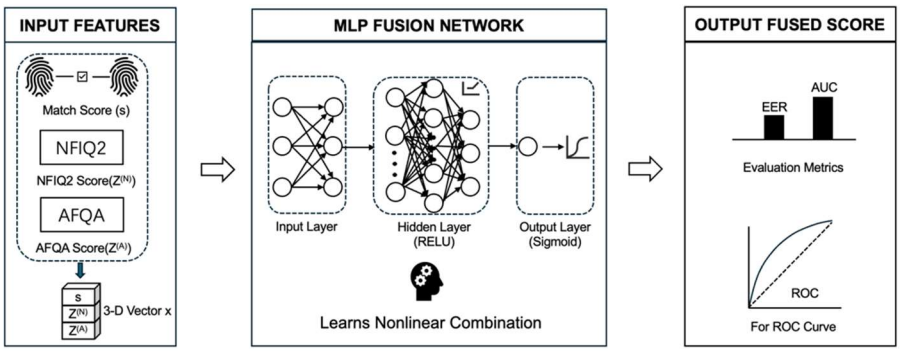

Figure 2. Quality-Aware MLP Fusion Framework

Specifically, given a latent fingerprint comparison pair, a fingerprint matcher first outputs the raw matching score s. We use the open-source Mindtct+Bozorth3 pipeline as the baseline matcher, which produces a real-valued similarity score. Meanwhile, quality-related indicators are extracted from the latent fingerprint sample, the NFIQ2 quality score $Z^{(N)}$ and the AFQA quality score $Z^{(A)}$. These three signals are concatenated to form a fused feature vector $\mathbf{x} = [s, Z^{(N)}, Z^{(A)}]$, which captures the joint status of similarity strength and information completeness. For evaluation, we divided the LFIW dataset into training set, validation set and test set, with the proportions of 60%/20%/20% respectively.

In each division, we generated pairs of real samples and forged samples. Compared with the baseline decision that relies solely on s, this feature construction explicitly helps distinguish cases where a low score arises from a true non-match from those where a low score is caused by poor quality and limited comparability, thereby improving robustness on low-quality samples.

For the fusion model, we employ a lightweight multilayer perceptron (MLP) to learn a nonlinear mapping from $\mathbf{x}$ to credibility. The network consists of an input layer, a hidden layer with ReLU activation, and a Sigmoid output layer, producing a probabilistic fused score $\hat{y} \in (0,1)$ that represents the confidence that the comparison pair is genuine. During training, genuine/impostor labels are used as supervision, and model parameters are optimized by minimizing the binary cross-entropy loss; the best model is selected on a validation set to mitigate overfitting. This learning process enables the model to capture the coupling between matching scores and quality indicators and to adaptively adjust the effective weight assigned to the matcher score under different quality conditions, leading to more stable decision outputs.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202604_12(4).0001

3.2 Evidence Package Modeling Design

Let the delivery process of an order o consist of K events, denoted by $\{e_i\}_{i=1}^{K}$. Each event e_i corresponds to an actual handoff or state transition (e.g., pickup, in-transit handoff, delivery, or exception handling). When e_i occurs, it triggers the generation of an evidence package ,producing an event-bound off-chain evidence package EP_i. To ensure that latent fingerprint evidence is both interpretable and traceable, the evidence package includes not only the latent fingerprint artifact itself, but also event-specific contextual information and auxiliary evidence that are strongly associated with the corresponding logistics operation. Accordingly, we abstract the evidence package as:

$$EP_i = \langle F_i,\ \mathcal{A}_i,\ \mathcal{C}_i,\ \pi_i \rangle.$$

The specific meanings of each field are shown in Table 1.The evidence packages are stored off-chain as encrypted objects; in our experiments, we simulate such "encrypted evidence packages" using local binary files. This design keeps the on-chain footprint at the metadata level while avoiding the privacy risks and irreversibility concerns that would arise from placing latent fingerprint data directly on-chain.

Table 1. Evidence package field definitions

Field	Description	Example	Sensitivity Level
F_i	Latent fingerprint information	Latent fingerprint image / features / mask	High
$\mathcal{A}_i$	Auxiliary evidence	Seal photos, exception notes	Medium
$\mathcal{C}_i$	Event context	OrderID, event type, timestamp, site	Medium
π_i	Privacy and access policy	Encryption / key ID	Low-Medium

3.3 On-chain Record

On-chain records are stored on a consortium blockchain and jointly maintained by logistics stakeholders such as platforms, carriers, and hubs, which avoids unnecessary public exposure of logistics metadata while meeting throughput and access requirements. For evaluation, we use a single-node deployment and benchmark record submission and verification to isolate the overhead of processing, hash-linking, and pointer-based off-chain verification.

To make the off-chain evidence verifiable, a cryptographic digest is computed for each evidence package EP_i:

$$H_i = \mathrm{SHA256}(EP_i)$$

We then write the event metadata, the digest, and the off-chain index pointer on-chain to form an evidence-preservation record, which can be abstracted as:

$$R_i = \langle \mathcal{M}_i,\ Prev_i,\ H_i,\ P_i \rangle$$

Here, $\mathcal{M}_i$ denotes the event metadata (at minimum including $\{OrderID, idx, type, ts, actor\}$); P_i is the off-chain object reference (e.g., an object-storage key or a controlled file path); and H_i is the digest of the evidence package. To ensure the temporal consistency of the event chain and to defend against reordering, insertion, and deletion attacks, we introduce a predecessor-hash linkage field:

ISSN: 2414-1895 DOI: 10.6919/ICJE.202604_12(4).0001

$$Prev_i = \begin{cases} \text{"GENESIS"}, & i = 1, \\ H_{i-1}, & i > 1. \end{cases}$$

This linkage forms a verifiable hash chain on-chain for each order: any modification to the ordering of records or to the linkage fields breaks chain consistency and can therefore be detected during provenance verification.

3.4 Traceback Playback and Verification

When a dispute is triggered (e.g., customer complaints, internal risk-control alerts, or arbitration intervention), the system retrieves the on-chain record sequence $\{R_i\}_{i=1}^{K}$ for the corresponding order indexed by the order identifier, and executes a closed-loop workflow of replay-verification-interpretation.

Firstly, the system performs event-chain replay. It outputs $\mathcal{M}_i$ in chronological order, linking pickup, in-transit handoffs, delivery, and exception events into a traceable event chain, thereby mitigating the "incomplete linkage" issue caused by fragmented evidence in conventional practices. Secondly, the system conducts linkage consistency verification by checking whether the on-chain records satisfy $Prev_i \stackrel{?}{=} H_{i-1}, \quad i = 2, \ldots, K$, If the condition does not hold, it indicates that the on-chain linkage has been corrupted or that records have been reordered/inserted. The system then reports a linkage verification failure and pinpoints the index at which the chain breaks. Finally, the system performs off-chain integrity verification. For each event, it retrieves the off-chain evidence package $\widehat{EP}_i$ according to P_i, computes $\widehat{H}_i = \mathrm{SHA256}(\widehat{EP}_i)$, and compares H_i against the on-chain digest $\widehat{H}_i$. If the off-chain file is missing or $\widehat{H}_i \neq H_i$, the evidence is deemed deleted or tampered with, and the system can localize the issue to the corresponding event node. With this mechanism, latent fingerprint evidence and auxiliary materials remain verifiable even when stored off-chain: digest consistency provides tamper-evident assurance against substitution in dispute scenarios, thereby strengthening non-repudiation.

At the interpretation stage, subject to authorization, the system can present the latent fingerprint evidence F_i and auxiliary evidence $\mathcal{A}_i$ contained in EP_i , and explain the provenance of the evidence by combining the event context $\mathcal{C}_i$ (i.e., at which stage the latent fingerprint was produced and by which node it was collected/packaged). Notably, latent fingerprint matching and discrimination are performed off-chain rather than on-chain, providing technical support for evidential usability in subsequent arbitration.

4. Results

4.1 Effectiveness of Latent Fingerprint Identification

In logistics environments, latent fingerprints may be degraded by contamination, friction, and pose variations. Relying solely on matcher scores can therefore lead to unstable decisions, particularly for low-quality samples. To assess the *usability* of latent fingerprints as logistics evidence, we design a latent fingerprint verification experiment comparing two decision strategies: a baseline that uses only the matcher score, and a quality-aware strategy that incorporates quality assessment information by feeding the matcher score together with quality-related features into a learned model to produce a more robust decision output. Performance is evaluated using ROC curves and AUC to quantify overall discriminative capability, while EER is additionally reported to characterize performance under the equal-error operating point.

As shown in Figure 3, the quality-aware strategy consistently outperforms the baseline, yielding an improved ROC curve with higher AUC and reduced EER. These results indicate that, even under complex noise and pronounced quality fluctuations typical of logistics scenarios, latent fingerprints retain sufficient discriminative value to support dispute forensics. This finding also establishes a prerequisite for the subsequent preservation-and-tracing mechanism: incorporating latent fingerprints

ISSN: 2414-1895 DOI: 10.6919/ICJE.202604_12(4).0001

into evidence packages is practically meaningful only when the underlying biometric evidence is demonstrably usable.

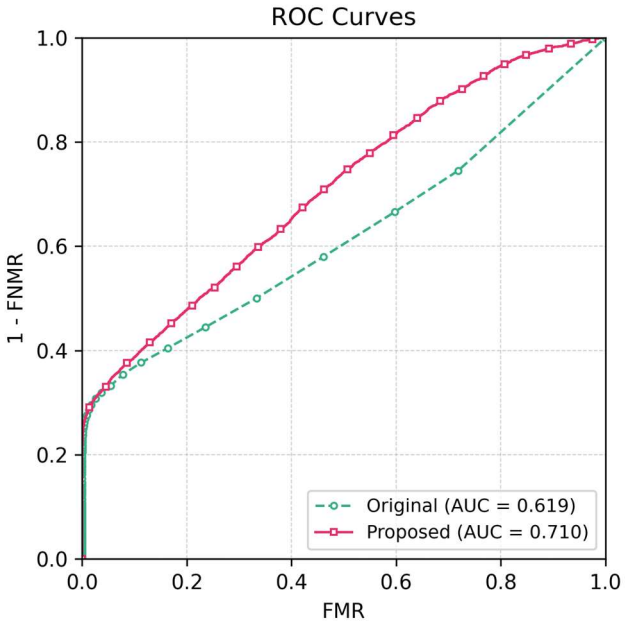

Figure 3. ROC curves on the LFIW test set comparing the baseline matcher score and the proposed quality-aware MLP fusion.

4.2 Timeliness of Evidence Preservation and Provenance

To assess the feasibility of the proposed latent-fingerprint-enabled trusted preservation and tracing method in logistics scenarios, we evaluate the timeliness of evidence writing, trace replay, and the consistency and integrity verification procedures. Evidence packages are generated in an event-driven manner: only event metadata, cryptographic digests, and off-chain pointers are recorded on-chain, while latent fingerprints and their auxiliary evidence are stored off-chain as encrypted objects. In addition, an order-level batch commit strategy is adopted to align with the batch-oriented write workflows commonly used in practical deployments.

As summarized in Table 2, the proposed hybrid storage design sustains a high writing throughput while keeping the end-to-end per-event preservation overhead within the millisecond range. The throughput drops as the thread count increases because record commits are serialized on a single-node write path, and higher concurrency mainly introduces lock contention and context-switch overhead rather than parallel speedup. As concurrency increases, the observed throughput–latency trade-off follows the expected behavior under single-node write contention, yet the overall performance remains sufficient for high-frequency logistics event recording. During tracing, the system retrieves the on-chain event sequence by order identifier to replay the event chain, and performs linkage consistency checks with low overhead, enabling effective detection of record reordering or corrupted linkage fields. Off-chain evidence is further validated by recomputing and comparing cryptographic digests, which can also be completed efficiently, thereby supporting a rapid replay–verify loop when disputes are triggered. Meanwhile, by storing only digests and pointers on-chain, the on-chain storage footprint is maintained at the scale of hundreds of bytes per event, substantially reducing on-chain burden compared with full on-chain storage and improving scalability. Overall, the proposed method achieves a favorable balance between timeliness and overhead, providing practical support for deploying latent fingerprint evidence in logistics dispute forensics and responsibility attribution.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202604_12(4).0001

Table 2. Timeliness evaluation of evidence preservation and tracing

Threads	Throughput(EP/s)	Avg. Write Latency (ms/EP)	Avg. Off-chain Verification (ms/order)
8	1078.22	6.94	0.815
16	882.21	15.64	0.912
32	896.23	29.26	0.915

4.3 Effectiveness of Traceability

To validate tracing effectiveness in dispute scenarios, we assess the tracing workflow from three perspectives-replayability, verifiability, and localizability-and the results are summarized in Table 3. Once a dispute is triggered, the system retrieves the on-chain sequence of event records by OrderID. It first replays the event chain by linking pickup, in-transit handover, delivery, and exception nodes in chronological order to form a traceable event stream. It then performs linkage consistency verification by checking the predecessor-digest association, thereby detecting record reordering, insertion, or corruption of linkage fields on-chain. Finally, it conducts off-chain integrity verification by loading the off-chain evidence packages via on-chain pointers, recomputing their cryptographic digests, and comparing them with the on-chain digests to determine whether the off-chain evidence is missing, substituted, or tampered with. The experimental results indicate that the proposed mechanism maintains event-chain replayability while effectively detecting typical tampering behaviors and localizing the compromised event node or evidence object, providing actionable technical support for responsibility attribution and arbitration verification. Overall, the method enables rapid event-chain replay after dispute initiation and offers verifiable evidence for logistics dispute resolution, thereby improving accountability-oriented tracing effectiveness in logistics environments.

Table 3. Tracing Effectiveness Test Results

Category	Test Item	Description	Result
Replay capability	Event-chain replay	Replay events by OrderID	Pass
Consistency verification	On-chain hash-chain validation	Validate Prev linkage	Pass
Integrity verification	Off-chain digest consistency	Verify digest match	Pass
Tamper detection	Off-chain deletion detection	Detect missing evidence	Pass

5. Conclusion

In this paper, we propose a quality-aware evidence preservation and provenance framework for latent fingerprints in logistics. The logistics process is modeled as an event sequence such as pickup, in-transit handoff, delivery, and exception handling, and each event generates an evidence package that binds the latent fingerprint with its corresponding context and auxiliary materials. A hybrid storage design is adopted: only event metadata, cryptographic digests, and off-chain references are recorded on-chain, while the original biometric and auxiliary evidence is encrypted and stored off-chain. To improve the usefulness of fingerprint evidence in dispute handling, we further fuse fingerprint quality measures with matcher scores and store the resulting credibility score as part of the provenance metadata.

Experiments show that the proposed fusion strategy improves latent fingerprint verification compared with a matcher-only baseline, especially under noisy and quality-varying conditions. The overhead results indicate that the hybrid design supports efficient evidence writing and verification with limited on-chain storage. Traceability tests further demonstrate reliable event-chain replay and the detection/localization of common attacks, including off-chain modification, missing evidence, and linkage manipulation. Future work will implement the system on a consortium blockchain with

ISSN: 2414-1895 DOI: 10.6919/ICJE.202604_12(4).0001

contract-based access control, improve key management and secure storage, and evaluate the framework at larger scale using operational data and diverse carriers.

References

[1] Vazquez Melendez, Elena Isabel, Paul Bergey, and Brett Smith. :Blockchain technology for supply chain provenance: increasing supply chain efficiency and consumer trust. Supply chain management: An international journal (2024) 706-730.

[2] Cao, Kai, and Anil K. Jain. :Automated latent fingerprint recognition. IEEE transactions on pattern analysis and machine intelligence (2018) 788-800.

[3] Yoon, Soweon, Eryun Liu, and Anil K. Jain. :On latent fingerprint image quality. International Workshop on Computational Forensics. Cham: Springer International Publishing, (2012) 67-82.

[4] Jain, Anil K., and Jianjiang Feng. :Latent fingerprint matching. IEEE Transactions on pattern analysis and machine intelligence (2010) 88-100.

[5] Liu, Xinwei, et al. :A latent fingerprint in the wild database. IEEE Transactions on Information Forensics and Security (2024) 3703-3718.

[6] Vazquez Melendez E I, Bergey P, Smith B. :Blockchain technology for supply chain provenance: increasing supply chain efficiency and consumer trust. Supply chain management: An international journal, (2024) 706-730.

[7] Vanin, Fausto Neri da Silva, et al. :A blockchain-based end-to-end data protection model for personal health records sharing: a fully homomorphic encryption approach. (2022).

[8] Lin, Qi, Binbin Gu, and Faisal Nawab. :RollStore: hybrid onchain-offchain data indexing for blockchain applications. IEEE Transactions on Knowledge and Data Engineering (2024).

[9] Xu, Bing, Tobechukwu Agbele, and Richard Jiang. :Biometric blockchain: A better solution for the security and trust of food logistics. IOP Conference Series: Materials Science and Engineering. (2019).

[10] Putra, Guntur Dharma, et al. :Trust-based blockchain authorization for IoT. IEEE Transactions on Network and Service Management (2021): 1646-1658.

[11] Sankaran, Anush, Mayank Vatsa, and Richa Singh. :Automated clarity and quality assessment for latent fingerprints. 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). (2013).

[12] Grosz, Steven A., and Anil K. Jain. :Latent fingerprint recognition: Fusion of local and global embeddings. IEEE Transactions on Information Forensics and Security (2023) 5691-5705.

[13] Ezeobiejesi, Jude, and Bir Bhanu. :Latent fingerprint image quality assessment using deep learning. Proceedings of the IEEE conference on computer vision and pattern recognition workshops. (2018).

[14] Zuev, Sergey, and Dmitry Bakhteev. :Digital Forensic Logistics: The Basics of Scientific Theory. International Journal of Law and Society (2021) 83-88.