VISUAL ADUIT FRAMEWORK FOR PREVENTING E-COMMERCE DELIVERY AND RETURN FRAUD

Ms. P PREETHI ,
Assistant Professor, Computer Science and Engineering,
St. Joseph College of Engineering,Chennai-602117, Tamil Nadu,
Email Id – ppreethi@stjoseph.ac.in

Ms. SHERLINE SWEETY S,
Student, Computer Science and Engineering,
St. Joseph College of Engineering ,Chennai-602117, Tamil Nadu,
Email Id – sherlinesusai@gmail.com

Ms. MALATHI K,
Student, Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id – kmalathikumaresan@gmail.com

ABSTRACT

Product delivery and return fraud is a growing issue in e-commerce, where products are replaced, tampered with, or returned with missing components. These incidents create disputes between customers and sellers and result in financial loss, mistrust, and poor customer experience. Most current delivery and return processes do not maintain reliable visual proof of the product across its lifecycle. There is no proper way to confirm what was packed, what was actually delivered to the customer, and what was later returned. Manual verification is time-consuming, prone to human error, and often fails to clearly identify where fraud or tampering occurred. To address this problem, this project introduces a visual verification framework that continuously records and analyzes three key checkpoints in the product lifecycle: the packing video, the delivery video, and the return video. Each video acts as digital proof of the product's condition, contents, and authenticity at different stages of the logistics process. The system applies YOLOv9 to detect and verify all visible items such as the main product and its accessories at each stage. A Siamese Network is then used to compare the product across these videos and confirm whether it is the same item throughout its journey. This deep-learning model is capable of handling variations in camera angle, lighting, and orientation, while still identifying subtle differences caused by product substitution or tampering. By performing pairwise comparisons—packing vs delivery, delivery vs return, and packing vs return—the system can accurately detect missing accessories, swapped items, or fraudulent return attempts. More importantly, it can pinpoint the exact stage where the discrepancy occurred, whether at the seller’s end, during courier handling, or by the customer. the proposed approach reduces disputes, protects both customers and sellers, and creates a transparent audit trail throughout the delivery and return process. It improves accountability, enhances fraud detection accuracy, and helps resolve product return claims fairly.

KEYWORDS

E-Commerce Fraud, Delivery Fraud, Return Fraud, Computer Vision, Image Verification, Visual Audit, Machine Learning, Risk Scoring, Fraud Detection.

I.INTRODUCTION

The rapid growth of e-commerce platforms such as Amazon, Flipkart, and Meesho has significantly transformed the retail industry by enabling convenient online shopping, doorstep delivery, and easy return policies. While these advancements have improved customer experience, they have also led to an increase in fraudulent activities related to product delivery and returns. Fraud cases such as false delivery claims, empty box returns, product swapping, and intentional damage reporting have become major concerns for e-commerce companies, causing substantial financial losses and operational challenges. Traditional verification methods such as OTP confirmation, delivery acknowledgements, and manual warehouse inspection are often insufficient to detect visual manipulation or product tampering.

These systems lack reliable visual proof and mainly depend on trust-based confirmation mechanisms. To address these issues, the PoP (Proof of

Package) Visual Audit Framework is proposed as an AI-powered solution that integrates Computer Vision and machine learning techniques to capture, analyse, and compare package images during dispatch, delivery, and return processes. By generating fraud risk scores and providing automated visual verification, the system enhances transparency, strengthens fraud prevention, and improves trust between customers and e-commerce platforms.

II. BACKGROUND AND MOTIVATION

E-commerce delivery and return fraud has emerged as a significant challenge in the digital retail ecosystem due to increasing transaction volumes and flexible return policies. Existing fraud detection mechanisms primarily rely on manual inspection, transaction history analysis, and complaint-based investigation, which are reactive rather than preventive in nature. These traditional systems do not provide strong visual evidence to verify the authenticity of returned products or the integrity of delivered packages. With the advancement of Artificial Intelligence and Deep Learning, particularly in Computer Vision, it has become possible to analyse product images, detect packaging tampering, identify object mismatches, and automatically detect anomalies with high accuracy. Motivated by the need for a proactive and automated fraud prevention system, the PoP framework aims to leverage visual auditing techniques to reduce dependency on manual verification and minimize fraudulent claims. By capturing real-time visual proof at different stages of the supply chain and applying AI-based comparison models, the proposed system ensures better accountability, reduces financial losses, and enhances operational efficiency in modern e-commerce environments.

III. SYSTEM ARCHITECTURE

The system consists of multiple integrated modules that ensure fraud detection during both delivery and return processes.

Components of System Architecture

1. Image Capture Layer

Captures package images or short videos:

- At warehouse dispatch
- At delivery point
- During return pickup

2. Preprocessing Layer

- Image resizing
- Noise removal
- Background normalization
- Image enhancement

3. Feature Extraction Layer

Extracts:

- Product shape and dimensions
- Packaging seal status
- Barcode/QR verification
- Object features using CNN models

4. Fraud Detection Module (AI Model)

Uses:

- Convolutional Neural Networks (CNN)
- Image similarity algorithms
- Anomaly detection techniques

It compares original and return images and detects mismatches.

5. Risk Scoring Engine

Generates fraud probability score based on:

- Visual mismatch percentage
- Seal damage detection
- Weight inconsistency
- Customer fraud history

6. Audit & Dashboard Module

Displays:

- Fraud alert
- Risk score
- Visual comparison results
- Recommendation (Approve / Manual Check / Reject)

IV.ARCHITECTURE FLOW

Visual Audit Framework for Preventing E-Commerce Delivery and Return Fraud follows a structured and sequential architecture to ensure accurate fraud detection during product dispatch, delivery, and return stages. The system integrates Computer Vision, Machine Learning, and risk analytics to provide automated visual verification.

Below is the detailed step-by-step architecture flow:

Step 1: Order Confirmation and Package Initialization

The process begins when a customer places an order on an e-commerce platform such as Amazon or Flipkart. Once the order is confirmed, a unique Order ID and Tracking ID are generated. The system initializes a digital audit record for that specific order in the central database. This record will store all visual and transactional data related to the package throughout its lifecycle.

Step 2: Warehouse Image Capture (Dispatch Verification)

Before the product is sealed and dispatched from the warehouse, high-resolution images (or short video clips) of the product and packaging are captured.

This includes:

- Product inside the box
- Packaging condition
- Barcode/QR code
- Tamper-proof seal status

These images are tagged with:

- Timestamp
- Location ID
- Order ID

The captured images act as the **original visual proof (baseline reference)** for future comparison.

Step 3: Image Preprocessing

The captured images undergo preprocessing to ensure consistency and improve model accuracy. This stage includes:

- Image resizing to uniform resolution
- Noise removal
- Background normalization
- Lighting correction
- Format standardization

This ensures that images captured in different environments (warehouse, doorstep, return pickup) can be fairly compared by the AI model.

Step 4: Feature Extraction Using Computer Vision

After preprocessing, important visual features are extracted using deep learning models such as Convolutional Neural Networks (CNN).

Extracted features include:

- Product shape and dimensions
- Color patterns
- Logo and branding details
- Barcode/QR code validation
- Seal and packaging structure
- Texture features

These extracted features are converted into numerical vectors and stored in the system database for comparison.

Step 5: Delivery Stage Image Capture (Proof of Delivery)

At the time of doorstep delivery, the delivery agent captures images of:

- Delivered package
- Packaging seal condition
- Customer confirmation

These images are uploaded to the central system and linked with the original warehouse images.

The system verifies:

- Whether the seal is intact
- Whether the package appears tampered
- Whether the correct package is delivered

This creates strong proof in case of future disputes like “Item Not Delivered” fraud.

Step 6: Return Initiation and Return Pickup Image Capture

If the customer initiates a return, the system activates the return audit workflow. During return pickup, the delivery agent captures:

- Image of returned product
- Packaging condition
- Product inside box
- Visible damage (if claimed)

These images are uploaded and stored under the same Order ID for comparison with the original dispatch images.

Step 7: AI-Based Image Comparison and Anomaly Detection

This is the core fraud detection stage.

The system compares:

- Original warehouse image
- Delivery stage image
- Return stage image

Using:

- Image similarity algorithms
- CNN-based object detection
- Structural Similarity Index (SSIM)
- Anomaly detection models

The system checks for:

- Product mismatch

- Missing items
- Damaged packaging
- Seal tampering
- Object replacement

If visual differences exceed a predefined threshold, the system flags the case as suspicious.

Step 8: Risk Scoring Engine

After comparison, a fraud risk score is generated based on multiple parameters:

- Image mismatch percentage
- Seal integrity status
- Weight discrepancy (if integrated with smart weighing system)
- Customer return history
- Past fraud records

The risk score is categorized as:

- Low Risk (Safe Return)
- Medium Risk (Manual Review Required)
- High Risk (Fraud Suspected)

Step 9: Explainable AI (XAI) Output

To improve transparency, the system provides an explanation for the decision. Instead of only marking “Fraud” or “Safe,” it highlights:

- Area of visual mismatch
- Seal damage detected
- Product replacement identified

- Missing accessory detected

This helps logistics teams understand the exact reason for fraud detection.

Step 10: Admin Dashboard and Alert System

The final results are displayed on an admin dashboard that includes:

- Order ID
- Visual comparison results
- Risk score
- Fraud probability percentage
- Recommended action

If high-risk fraud is detected:

- Alert notification is sent
- Return approval is paused
- Manual investigation is triggered

Step 11: Data Storage and Audit Trail Maintenance

All visual records and fraud decisions are securely stored in cloud storage. This ensures:

- Tamper-proof audit trail
- Legal evidence support
- Historical fraud analytics
- Model retraining dataset

V. Module Description

1. Warehouse Verification Module

Captures product image before sealing and dispatch.

2. Delivery Verification Module

Captures proof of delivery with customer presence.

3. Return Verification Module

Captures returned product image before acceptance.

4. Image Comparison Module

Uses CNN and image hashing techniques to compare:

- Product identity
- Packaging condition
- Seal integrity

5. Fraud Detection Module

Classifies:

- Genuine Return
- Suspicious Return
- Fraudulent Return

6. Reporting Module

Provides:

- Fraud analytics
- Customer risk profile
- Monthly fraud trends

VI. IMPLEMENTATION METHODOLOGY

The implementation of **Visual Audit Framework for Preventing E-Commerce Delivery and Return Fraud** follows a structured approach to ensure accurate visual verification and fraud detection.

Step1: Data Collection

Product images are collected at different stages such as warehouse dispatch, delivery, and return pickup. Sample datasets of genuine and fraudulent return cases are also gathered for training the model.

Step2: Image Processing

Captured images are resized, cleaned, and normalized to maintain uniform resolution and quality. Noise removal and lighting correction are applied to improve image consistency.

Step3: Feature Extraction

Important visual features such as product shape, packaging seal status, barcode details, and texture patterns are extracted using Convolutional Neural Networks (CNN). These features are converted into numerical format for analysis.

Step4: Model Training

Machine Learning and Deep Learning models are trained using labelled datasets to identify product mismatches, packaging tampering, and anomalies. The system learns patterns of genuine and fraudulent returns.

Step5: Image Comparison and Fraud Detection

The trained model compares dispatch images with delivery and return images using similarity and anomaly detection techniques. If inconsistencies are detected beyond a threshold, the system flags the case as suspicious.

Step6: Risk Scoring and Decision MakingA fraud risk score is generated based on visual mismatch, seal condition, and customer history. The system categorizes the return as low, medium, or high risk.

VII. RECENT ADVANCEMENTS IN VISUAL AI FOR FRAUD PREVENTION

1. Advanced Object Detection Models (e.g., YOLOv8, Faster R-CNN, SSD)

Modern object detection architectures are capable of identifying multiple objects, shapes, and patterns in an image instantly:

- Detect precise product boundaries, labels, and packaging parts.
- Recognize barcodes, logos, and text even under poor lighting.
- Distinguish between genuine and tampered packaging using learned features.

These models provide higher accuracy and faster inference time compared to traditional techniques.

2. Image Similarity and Feature Embeddings

State-of-the-art similarity metrics use deep feature embeddings rather than simple pixel comparison:

- Models like **Siamese Networks** and **Triplet Networks** learn meaningful visual representations.
- They detect subtle differences between original and return images even when the object is rotated or partially obscured.
- This increases fraud detection accuracy compared to basic hashing or pixel-by-pixel comparison.

3. Anomaly Detection Using Deep Learning

Anomaly detection models are trained to recognize normal (genuine) image patterns so that deviations can be flagged as suspicious:

- **Autoencoders** and **Variational Autoencoders (VAEs)** reconstruct input images and detect differences.

- **Generative Adversarial Networks (GANs)** help model what normal packaging should look like and expose unnatural alterations.
- Helps catch rare fraud cases that the system has never seen before.

4. Explainable AI (XAI) for Transparent Decisioning

Instead of opaque black-box results, modern systems use **Explainable AI** techniques that show *why* a return was flagged:

- Heatmaps show areas where visual mismatch occurs.
- Saliency maps highlight the exact pixels influencing the fraud decision.
- Decision explanations enhance trust and assist auditors in rapid review.

This improves human understanding and reduces false positives.

5. Edge AI Deployment on Mobile Devices

Rather than sending every image to a cloud server for processing:

- Lightweight visual AI models can run **directly on delivery agent smartphones** or handheld scanners.
- This reduces latency and improves real-time verification at the source.
- It also helps conserve bandwidth and enables offline processing in low-connectivity environments.

6. Real-Time Video Analysis

Instead of only static images, recent systems can analyse **short video clips** from delivery moments:

- Capture customer interactions, packaging openings, and product orientation changes.
- Video provides richer context than single images.
- Models extract temporal patterns and motion cues to improve fraud detection.

7. 3D Vision and Depth-Based Verification

With consumer-grade depth sensors and stereo cameras:

- Systems capture 3D shape information of products.
- This is useful for detecting subtle product swaps and internal manipulations.
- Techniques like **3D reconstruction** provide deeper insights beyond flat images.

8. Blockchain for Secure Visual Audit Trails

Emerging fraud prevention systems use blockchain to:

- Store package images and audit records immutably.
- Prove that visual evidence has not been tampered with after capture.
- Enable secure cross-organization verification between sellers, logistics providers, and buyers.

This ensures strong security and non-repudiation.

9. Multi-Modal AI Systems

Modern frameworks don’t just rely on visual data — they combine it with other signals:

- **Text recognition (OCR)** for invoices and labels
- **Sensor data** from smart scales
- **Location metadata** from delivery apps
- **Behavioral signals** like delivery time patterns

Multi-modal fusion increases fraud detection accuracy and resilience.

10. Continual Learning and Self-Learning Models

Instead of static models, newer systems continuously retrain with fresh data:

- They adapt to new fraud patterns.
- Reduce model degradation over time.
- Automatically improve detection based on feedback loops from real incidents.

This improves robustness and scalability in evolving fraud landscapes.

VIII.ADVANCEMENTS IN E-COMMERCE FRAUD DETECTION

1. AI and Machine Learning-Based Fraud Detection

Traditional rule-based systems are being replaced by AI-driven models that learn patterns from large volumes of transaction and customer data. Machine Learning algorithms such as Random Forest, Gradient Boosting, and Neural Networks can automatically detect unusual behaviors, abnormal transaction patterns, and suspicious return activities.

Key Benefits:

- Detects new and unknown fraud patterns
- Reduces dependency on static rules
- Continuously improves through retraining

2. Deep Learning for Behavioural Analysis

Deep Learning models analyze complex customer behavior patterns such as:

- Purchase frequency
- Return rate
- Location changes
- Device usage patterns

Recurrent Neural Networks (RNN) and LSTM models can detect hidden patterns in sequential data, helping identify repeat offenders and coordinated fraud networks.

Impact:

- Higher fraud detection accuracy
- Reduced false positives
- Early detection of suspicious customers

3. Computer Vision for Visual Verification

One of the most important recent advancements is the use of Computer Vision in fraud detection. AI models can now:

- Compare product images before dispatch and after return
- Detect packaging tampering
- Identify product swapping
- Detect empty box returns

Convolutional Neural Networks (CNN) and object detection models such as YOLO are widely used for visual fraud detection.

Advantages:

- Provides strong visual proof
- Reduces manual inspection errors
- Detects return fraud effectively

4. Real-Time Fraud Detection Systems

Modern e-commerce systems operate in real time. Fraud detection engines analyze transactions instantly before approval.

Technologies used include:

- Real-time risk scoring engines
- API-based fraud detection systems
- Automated alert generation

Benefits:

- Prevents fraud before completion
- Minimizes financial loss
- Enhances customer security

5. Multi-Layered Fraud Detection Frameworks

Instead of relying on a single detection method, companies now use multi-layered systems combining:

- Transaction analysis
- Device fingerprinting
- IP tracking
- Visual verification
- Customer behaviour scoring

This layered approach improves detection accuracy and reduces system vulnerability.

6. Explainable AI (XAI) for Transparent Decisions

Modern fraud detection systems integrate Explainable AI to provide reasons behind fraud alerts. Instead of simply flagging a transaction as fraudulent, the system explains:

- High return frequency
- Packaging mismatch
- Suspicious location change
- Product image difference

Importance:

- Improves trust in AI decisions

- Helps fraud analysts understand alerts
- Supports legal and audit requirements

7. Blockchain for Secure Audit Trails

Blockchain technology is being explored to store transaction and return records in a tamper-proof manner. This ensures that visual evidence and delivery records cannot be altered.

Advantages:

- Immutable record keeping
- Improved transparency
- Strong dispute resolution support

8. Federated Learning for Privacy Protection

Federated Learning allows fraud detection models to be trained across multiple devices or warehouses without sharing raw data. This protects sensitive customer information while still improving model accuracy.

Benefits:

- Enhanced data privacy
- Compliance with data protection regulations
- Secure collaborative learning

9. Big Data and Predictive Analytics

E-commerce platforms process millions of transactions daily. Big Data technologies help analyse:

- Historical fraud patterns
- Seasonal fraud trends
- High-risk customer segments

Predictive analytics models forecast potential fraud risk before it occurs.

10. Automated Risk Scoring and Customer Profiling

Modern systems assign dynamic fraud scores to customers based on:

- Return ratio
- Past fraud cases
- Payment behaviour
- Account age

High-risk customers are monitored more strictly, reducing fraud attempts.

IX. CHALLENGES

1.Rapidly Evolving Fraud Techniques

Fraudsters continuously change their strategies to bypass detection systems. They use advanced methods such as professional resealing of packages, product swapping with identical-looking items, and coordinated fraud networks. As detection systems improve, attackers adapt quickly, making fraud prevention an ongoing challenge.

2. Difficulty in Detecting Visual Manipulation

In visual audit systems like PoP, image-based verification plays a major role. However, detecting subtle product swaps, minor packaging tampering, or high-quality fake replicas can be difficult. Fraudsters may carefully open and reseal packages without obvious damage, making visual detection challenging.

3. Variations in Image Quality and Environment

Images captured at warehouses, delivery points, and return pickups may vary due to:

- Lighting conditions
- Camera quality

- Angle differences
- Background noise

These variations can affect AI model accuracy and increase false positives or false negatives.

4. High False Positive Rate

Sometimes genuine customers may be wrongly flagged as fraudulent due to:

- Damaged packaging during transit
- Delivery handling errors
- Image misinterpretation by AI

High false positives can reduce customer trust and negatively impact brand reputation.

5. Large Data Storage and Processing Requirements

Visual audit systems generate a huge amount of image and video data daily. Storing, processing, and analysing this data in real time requires:

- High storage capacity
- Powerful cloud infrastructure
- Efficient data management systems

This increases operational costs.

6. Privacy and Data Security Concerns

Capturing images during delivery and returns may involve customer premises and personal information. Ensuring compliance with data protection regulations and preventing unauthorized access to stored images is a critical challenge.

7. Integration with Existing Logistics and IT Systems

Implementing a visual fraud detection system requires integration with:

- Order management systems
- Warehouse management systems
- Delivery tracking systems
- Customer support platforms

Compatibility issues, technical complexity, and training delivery personnel can slow down implementation.

X. CONCLUSION

The proposed **Visual Audit Framework for Preventing E-Commerce Delivery and Return Fraud** provides an advanced, technology-driven solution to address one of the most critical challenges in modern digital commerce. With the rapid growth of online marketplaces such as Amazon and Flipkart, delivery and return fraud have emerged as significant threats, leading to financial losses, operational inefficiencies, and reduced trust between customers and sellers. Traditional verification mechanisms such as OTP confirmation, manual inspection, and complaint-based investigation are often reactive and insufficient to detect sophisticated fraud techniques like product swapping, empty box returns, and packaging tampering.

The framework overcomes these limitations by integrating Computer Vision, Machine Learning, and automated risk scoring into a structured visual audit system. By capturing product images at multiple stages—warehouse dispatch, delivery confirmation, and return pickup—the system establishes reliable visual proof throughout the product lifecycle. Advanced image comparison and anomaly detection models analyse differences between original and returned items, enabling accurate identification of suspicious activities. The inclusion of a risk scoring engine further strengthens the decision-making process by categorizing returns based on fraud probability, while explainable outputs enhance transparency and accountability.

In addition to reducing fraudulent claims and financial losses, the proposed system improves operational efficiency by minimizing manual verification efforts and enabling real-time fraud detection. It also enhances trust among stakeholders by providing tamper-resistant audit trails and data-backed decisions. Although challenges such as image variability, data storage requirements, and system integration must be carefully managed, the PoP framework demonstrates strong potential as a scalable and intelligent solution for modern e-commerce ecosystems. Overall, the implementation of this visual audit framework represents a significant step toward secure, transparent, and technology-enabled fraud prevention in the evolving digital marketplace.

XI. REFERENCES

1. Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G., “Calibrating Probability with Undersampling for Unbalanced Classification,” *IEEE Symposium Series on Computational Intelligence*, 2015.

2. He, K., Zhang, X., Ren, S., & Sun, J., “Deep Residual Learning for Image Recognition,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016.

3. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A., “You Only Look Once: Unified, Real-Time Object Detection,” *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016.

4. Chalapathy, R., & Chawla, S., “Deep Learning for Anomaly Detection: A Survey,” *ACM Computing Surveys*, 2019.

5. Lundberg, S. M., & Lee, S. I., “A Unified Approach to Interpreting Model Predictions,” *Advances in Neural Information Processing Systems (NeurIPS)*, 2017.

6. Ribeiro, M. T., Singh, S., & Guestrin, C., “‘Why Should I Trust You?’ Explaining the Predictions of Any Classifier,” *ACM SIGKDD*

International Conference on Knowledge Discovery and Data Mining, 2016.

7. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X., "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature," *Decision Support Systems*, 2011.
8. Phua, C., Lee, V., Smith, K., & Gayler, R., "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," *Artificial Intelligence Review*, 2010.
9. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O., "Sequence Classification for Credit-Card Fraud Detection," *Expert Systems with Applications*, 2018.
10. Kaggle, "E-Commerce Fraud Detection Dataset," Available at: https://www.kaggle.com
11. Amazon Web Services (AWS), "Machine Learning for Fraud Detection in E-Commerce," Whitepaper, 2022. Amazon Web Services
12. Goodfellow, I., Bengio, Y., & Courville, A., *Deep Learning*, MIT Press, 2016.
13. Bishop, C. M., *Pattern Recognition and Machine Learning*, Springer, 2006.
14. Aggarwal, C. C., *Outlier Analysis*, Springer, 2017.
15. OpenAI, "Advances in Computer Vision and AI-Based Risk Analysis," Research Publications, 2023. OpenAI