APPLIED INFORMATION TECHNOLOGY AND COMPUTER SCIENCE
e-ISSN: 2773-5141

AITCS

Vol. 7 No. 1 (2026) p. 1250-1269
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

Dashcam Footage Analysis Tool for Timestamp and License Plate Evidence Extraction

Abdullahi Ubandoma Abubakar[1], Nurul Azma Abdullah[1*]

[1] *Fakulti Sains Komputer dan Teknologi Maklumat,*
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

*Corresponding Author: azma@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2026.07.01.067

Article Info

Received: 7 June 2026
Accepted: 23 June 2026
Available online: 30 June 2026

Keywords

Dashcam analysis, digital forensics, evidence extraction, license plate detection, tamper detection, timestamp extraction.

Abstract

Dashcam footage has become an important source of digital evidence in traffic accident analysis and criminal investigations. However, manual examination of dashcam videos is time-consuming, prone to human error, and often lacks systematic verification of evidence integrity. Existing tools provide limited automation and insufficient forensic validation, which may compromise the reliability and admissibility of extracted evidence. This project presents the development of a Dashcam Footage Analysis Tool for Evidence Extraction that automates key forensic processes and enhances evidence reliability. The system focuses on video upload, time-stamp extraction, tamper detection, license plate detection, and automated forensic report generation. The tool is developed using the Prototyping Model to allow iterative refinement based on user feedback. It is implemented using Python and Flask, with OpenCV and Tesseract OCR for video frame analysis and timestamp extraction. At the same time, SHA-256 cryptographic hashing is employed to ensure evidence of integrity through tamper detection. Experimental testing demonstrates that the system can accurately extract timestamps, identify video modifications through hash comparison, and generate structured forensic reports suitable for investigative purposes. The developed tool provides a practical and user-friendly solution for dashcam video forensics, improving investigation efficiency and increasing confidence in the authenticity of digital evidence.

1. Introduction

Dashcam footage has become a crucial source of evidence in police investigations [1]. It helps officers understand what happened during road accidents or crime scenes by recording real-time video inside vehicles. This footage captures key details such as time, GPS location, vehicle movement, and license plates, which are critical for reports or solving cases [2]. However, analyzing dashcam videos is still mostly done manually. Officers often watch lengthy videos to find important details, which takes time and can slow down investigations. Poor video quality and unclear frames further complicate the process. Many existing tools are also too expensive or complex for everyday use by local law enforcement [3].

The Malaysian case of Zayn Rayyan demonstrated how dashcam footage aided police in locating valuable hints. Through quicker and more precise video analysis, this case emphasizes the value of having technologies that help both crime scene and traffic accident investigations. To address these challenges, this project proposes the development of a Dashcam Footage Analysis Tool that automates evidence extraction tasks, including timestamp

reading, license plate detection, and tamper verification [4]. The tool aims to make digital evidence analysis faster, affordable, and user-friendly for forensic and police use. The objectives of this project are:

1. To develop a tool that extracts timestamps and license plates from dashcam videos.
2. To create a simple system with detection, tamper verification, and report features.
3. To support digital forensic investigations in accident and crime cases.

This project focuses on developing a Dashcam Footage Analysis Tool to assist investigators in analyzing digital evidence from dashcam videos. The system includes five main modules: video upload, timestamp extraction, license plate detection, tamper detection, and report generation. The tool supports pre-recorded dashcam videos in standard formats such as MP4 and AVI. However, it does not handle real-time streaming, audio evidence, cloud-based analysis, or AI-based tamper detection. The tool is also intended for single-user access only.

License plate detection is implemented using Optical Character Recognition (OCR) techniques for text extraction from video frames. Timestamp extraction retrieves visible timestamps from video frames, while tamper detection identifies possible alterations through metadata and hash comparison. The report generation module produces structured and printable reports from all extracted data. Each module plays a critical role in supporting digital forensic processes by simplifying video analysis, ensuring data authenticity, and improving the efficiency of police investigations.

This project presents a significant contribution to the field of digital forensics by addressing key challenges associated with the manual analysis of dashcam footage. The proposed Dashcam Footage Analysis Tool bridges the gap between conventional video review methods and modern forensic requirements by automating essential evidence extraction processes such as timestamp detection, metadata analysis, and license plate recognition. This automation reduces investigative workload and accelerates the overall analysis process, allowing investigators to focus on interpretation and decision-making rather than repetitive video inspection.

The system also enhances the credibility and reliability of digital evidence through the integration of tamper detection and cryptographic hashing techniques. By verifying the integrity of dashcam recordings and identifying potential alterations, the tool strengthens the evidential value of video footage used in legal proceedings. This capability supports accurate case reconstruction and increases confidence in the authenticity of digital evidence presented in court.

Furthermore, the study promotes accessibility and inclusiveness in digital forensic practice by providing a cost-effective and user-friendly analysis platform. Unlike complex and expensive commercial forensic tools, the proposed system is designed for ease of use by officers with limited technical expertise. This enables smaller police departments and investigative units, particularly in developing regions, to adopt digital forensic technologies more effectively. Overall, the project contributes to a more efficient, trustworthy, and technology-driven approach to modern law enforcement and digital evidence handling.

2. Related Work

This section will analyze current dashcam analysis tools, highlight their limitations, and introduce the Dashcam Footage Analysis Tool as a simplified and efficient solution for digital forensic investigations.

2.1 Dashcam Technology and Analysis Platforms

The proposed Dashcam Footage Analysis Tool is a desktop-based system designed to support police officers and digital forensic analysts in handling dashcam evidence efficiently [5]. The system integrates key forensic functions such as automated timestamp extraction, metadata analysis, license plate recognition, video enhancement, and tamper verification using cryptographic hashing techniques.

In terms of dashcam technology, the platform is designed to process video data captured from standard dashcam devices that embed visual overlays and metadata, including date, time, GPS location, and vehicle speed [6]. By analyzing both video frames and embedded metadata, the system ensures comprehensive evidence extraction and contextual accuracy during investigations.

From an analysis platform perspective, the tool emphasizes simplicity, usability, and affordability, making it suitable for users with limited technical expertise. Automated evidence extraction reduces reliance on manual video review, minimizes human error, and significantly improves investigation efficiency [7]. Additionally, the system supports structured forensic report generation, ensuring that extracted evidence is clearly documented, verifiable, and legally admissible for court proceedings [8].

2.2 Analysis of Existing Systems

This section reviews three existing tools commonly used in dashcam footage and forensic video analysis: Amped FIVE, OpenALPR, and Dashcam Viewer Pro [9]. These systems were selected for their relevance to evidence extraction and digital investigation tasks. Each offers unique capabilities but also presents limitations

that justify the development of the proposed Dashcam Footage Analysis Tool for Timestamp and License Plate Evidence Extraction.

Amped FIVE is a professional forensic video enhancement software widely adopted in law enforcement. It provides tools for video restoration, clarification, and annotation, enabling investigators to enhance footage quality and prepare it for court presentation [10]. However, it is costly, requires technical expertise, and is not ideal for fast on-field analysis. OpenALPR is an open-source automatic license plate recognition system that uses computer vision and OCR to detect and read vehicle registration numbers from images or videos. While effective for plate extraction, it lacks integrated timestamp extraction and forensic verification features. Dashcam Viewer Pro is commercial software designed for viewing and mapping dashcam recordings with GPS and speed data [11]. Despite its ease of use, it focuses primarily on playback rather than forensic evidence validation.

Amped FIVE is a widely recognized forensic video enhancement and analysis software used by law enforcement and forensic laboratories in over 100 countries. According to its official site (https://ampedsoftware.com/five)(10), the system provides a complete solution for analysing, clarifying, and restoring both video and image evidence. It includes more than 140 filters for tasks such as noise reduction, frame stabilization, timestamp enhancement, and metadata analysis [12].

Several of Amped FIVE's functions align with the goals of the proposed Dashcam Footage Analysis Tool for Timestamp and License Plate Evidence Extraction. Its timestamp clarification, video enhancement, and metadata inspection capabilities are particularly useful for improving the quality of dashcam footage and extracting relevant forensic details [13]. These functions help investigators uncover hidden or unclear evidence from low-quality or compressed recordings.

While Amped FIVE demonstrates the potential of advanced forensic tools, its complexity and high cost make it less accessible for smaller police departments or agencies in developing regions. Therefore, the proposed tool aims to integrate similar essential features, such as timestamp extraction and video integrity verification, but in a simpler, more affordable, and user-friendly format tailored for local forensic needs [14].

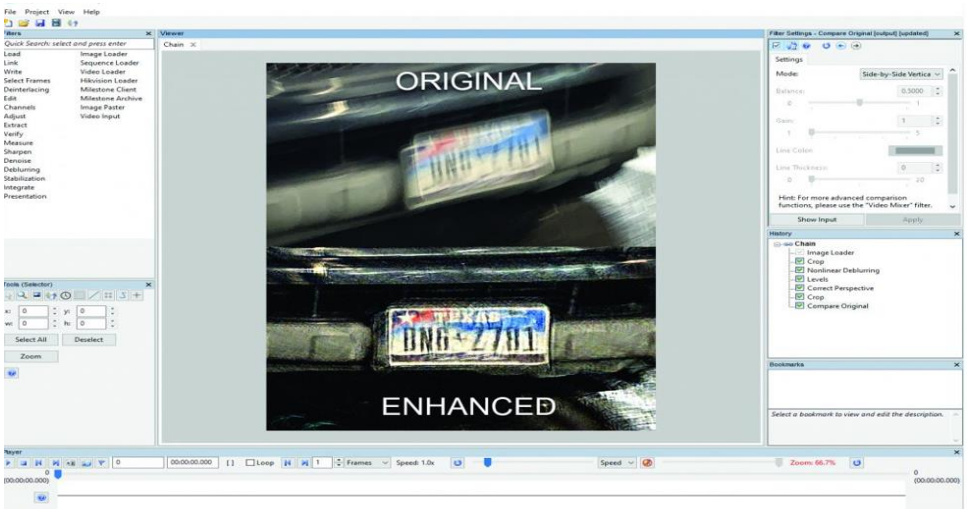


Fig.1 *Amped FIVE*

Fig. 1 shows a side-by-side comparison of a dashcam video frame before and after enhancement using Amped FIVE. The enhanced version on the right offers improved visibility of important forensic details such as timestamps, vehicle features, and scene context, which can significantly aid in evidence analysis.

OpenALPR (Automatic License Plate Recognition) is an open-source system that uses computer vision and OCR techniques to detect and recognize vehicle license plates from images and video streams. It supports multiple regions and plate formats, making it useful for traffic monitoring and forensic applications.

*A*lthough OpenALPR offers high accuracy in license plate recognition, it lacks integrated timestamp extraction, tamper detection, and forensic reporting features [15]. Additionally, enterprise-level features require paid licensing and higher system resources. The proposed tool adopts a lightweight OCR-based approach optimized for offline forensic use.

Fig.2 *OpenALPR*

Fig. 2 shows how OpenALPR automatically detects and reads a vehicle's license plate from dashcam footage. The recognized plate number is displayed in text format, helping investigators quickly identify vehicles involved in incidents without manually reviewing each video frame.

Dashcam Viewer Pro is a commercial software tool designed for visualizing and analyzing dashcam recordings. It is available at https://dashcamviewer.com(11). The tool supports various dashcam brands and video formats, enabling users to play back recordings while overlaying metadata such as GPS coordinates, speed, and g-force [16]. Additional features include route maps, video trimming, zooming, and data exporOne of the key features relevant to the proposed Dashcam Footage Analysis Tool is the synchronized display of video footage and metadata. This functionality allows investigators to accurately track vehicle movement and event timing. Although Dashcam Viewer Pro offers an intuitive interface and is well-suited for managing and viewing dashcam data, it lacks critical forensic functions such as tamper detection, structured evidence reporting, or timestamp extraction.While the software provides an intuitive interface and effective data visualization, it lacks forensic-specific features such as tamper detection, automated timestamp extraction, and structured report generation[17]. Insights from its interface design are useful for improving usability in the proposed tool.

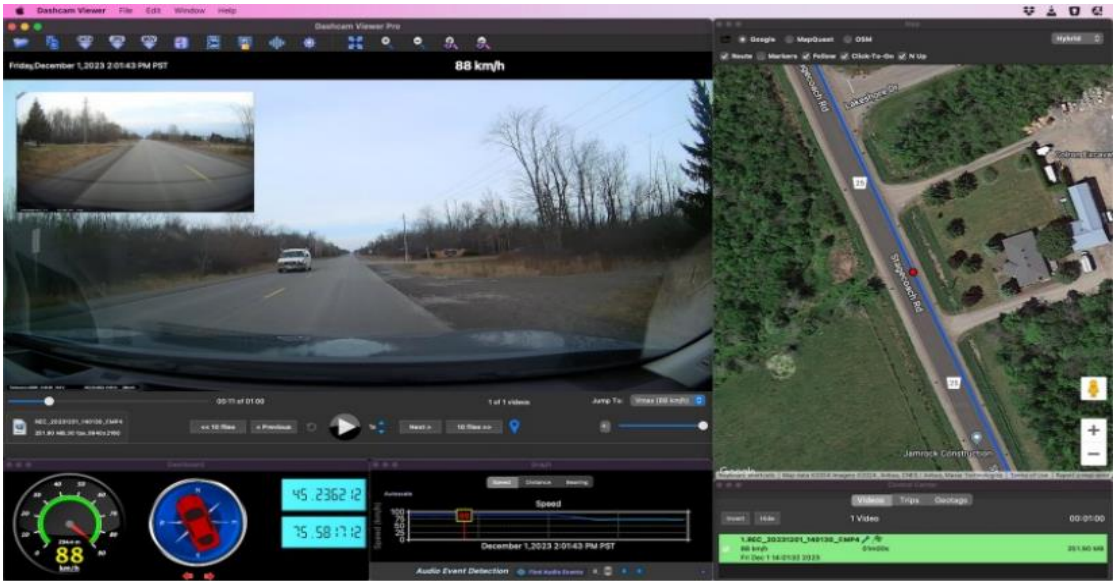


Fig.3 *Dashcam Viewer Pro*

Fig. 3 shows the Dashcam Viewer Pro interface, where recorded video footage is synchronized with GPS location and speed data. This visualization helps investigators trace vehicle movement in real time. Although the tool is useful for playback and data display, it lacks advanced forensic features like tamper detection or structured report generation (18).

Table 1 *Comparison of the existing system with the proposed Tool*

Features	Amped FIVE	OpenALPR	Dashcam Viewer Pro	Proposed Tool
Login Authentication	Yes	No	Yes	Yes
Video Enhancement	Yes	No	Yes	Yes
Metadata Extraction	Yes	Yes	Yes	Yes
Tamper Detection (Hashing)	Yes	Yes	No	Yes
License Plate Detection	Yes	No	No	Yes
Report Generation	Yes	No	No	Yes
Ease of Use for Police Users	No	Yes	Yes	Yes
Cost-Effective	No (High)	Yes (Free)	Yes	Yes

The comparison between the existing and proposed Tool is shown in Table 1. Existing tools such as Amped FIVE, OpenALPR, and Dashcam Viewer Pro offer useful features but lack a complete and integrated solution for dashcam forensic analysis, often being costly or limited in key functions. The proposed Dashcam Footage Analysis Tool addresses these gaps by combining automated evidence extraction, tamper detection, and reporting into a single, affordable, and user-friendly system suitable for digital forensic investigations.

3. Methodology

The development of the Dashcam Footage Analysis Tool adopts the Prototyping Model, carefully selected to support accurate evidence extraction, user-center design, and system reliability. This model is suitable for forensic applications as it allows continuous refinement of features such as timestamp extraction, tamper detection, and license plate recognition through iterative testing and feedback.

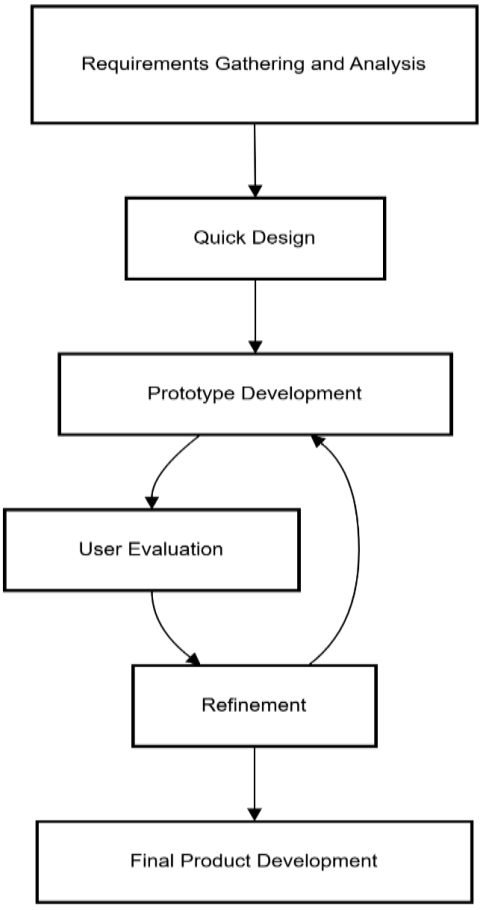


Fig.4 *Prototyping Model*

Applied Information Technology and Computer Science Vol. 7 No. 1 (2026) p. 1250-1269

Fig. 4 illustrates the iterative process of the Prototyping Model used in this project. It begins with requirements gathering, followed by quick design and prototype development. The prototype is then evaluated, refined based on feedback, and improved iteratively until the final system is produced, ensuring user requirements are consistently incorporated.

Table 2 *Software Development Activities and Their Tasks (for Dashcam Footage Analysis Tool)*

Phase	Task	Output
Requirements Gathering	Identify dashcam-specific features: video upload (MP4/AVI), timestamp extraction from frame regions, SHA-256 tamper detection, license plate detection using OCR	List of functional/non-functional requirements for dashcam forensic tool. List
Quick Design	Design UI for video playback, frame navigation, license plate highlighting, and report generation page	Wireframes showing dashcam analysis dashboard
Prototype Development	Build prototype with: Flask backend, OpenCV for frame extraction, Tesseract OCR for timestamps + plates, SHA-256 hashing for integrity	Working prototype that can process dashcam footage
User Evaluation	Test with real dashcam footage; evaluate timestamp accuracy, plate detection rate, tamper verification success	Feedback report on forensic accuracy and usability
Refinement	Improve OCR accuracy for low-light dashcam frames, optimize video processing speed, enhance report formatting.	Updated prototype
Final Product Development	Integrate all features into a stable version of the tool	Final tool ready for real use

The development of the Dashcam Footage Analysis Tool followed the Prototyping Model through six key phases. It started with gathering requirements based on real forensic needs. A quick design phase followed to sketch the tool's layout. A working prototype was then developed using Python and tested by users. Based on their feedback, the tool was refined to improve performance and usability. Finally, all features were integrated into a complete version of the tool. Each phase built upon the previous one to ensure the system was functional, user-friendly, and met its objectives

4. System Analysis and Design

The system analysis phase identifies the functional requirements and workflow needed to support reliable dashcam evidence extraction for digital forensic investigations. The proposed Dashcam Footage Analysis Tool is designed to assist investigators in efficiently extracting timestamps, detecting license plates, verifying video integrity, and generating structured forensic reports.

From a design perspective, the system follows modular architecture to ensure simplicity, scalability, and ease of maintenance. The core modules include user authentication, video upload, timestamp extraction, license plate detection, tamper detection, and report generation. Each module operates independently while sharing a centralized data flow to maintain forensic consistency. This design ensures that the system provides an efficient, user-friendly, and forensically sound solution suitable for police officers and digital forensic analysts handling dashcam evidence.

4.1 System Architecture Design

Fig. 5 is the architecture diagram that represents the sequential flow of the tool. Users begin by uploading dashcam footage, followed by timestamp extraction using OCR. The system then performs license plate detection, tamper analysis through SHA-256, and metadata verification, and finally reports generation in PDF format. If the evidence is valid and clear, it is forwarded to the police; otherwise, it is flagged for further manual review. This structured process supports reliable and efficient forensic analysis.

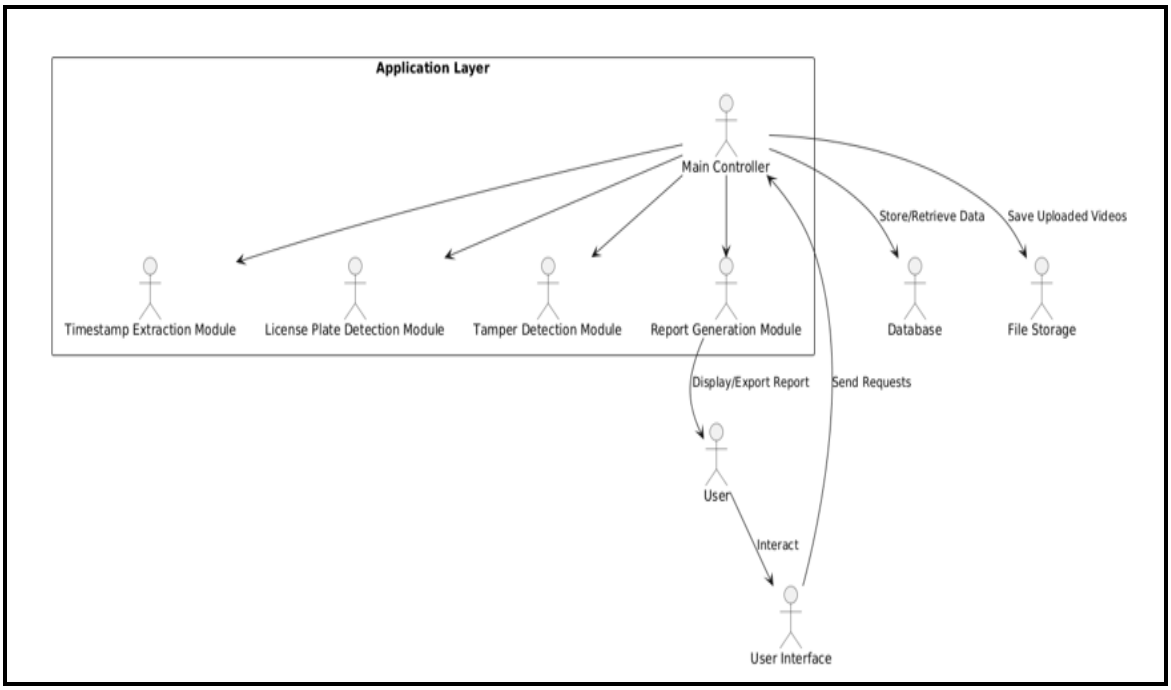


Fig. 5 *System Architecture Diagram for Dashcam Footage Analysis Tool*

4.2 Use Case Diagram

The Use Case Diagram for the Dashcam Footage Analysis Tool illustrates the interaction between the primary user, the digital forensic officer, and the system. It highlights the main functions provided by the tool, including user login, video upload, timestamp extraction, license plate detection, tamper verification, and report generation. Each use case represents a core operation that supports digital evidence extraction in forensic workflows. This diagram helps visualize how investigators interact with the system during accident or crime scene analysis. The following sections provide an overview of each use case, covering their purpose, actors involved, preconditions, flow of events, and expected outcomes.

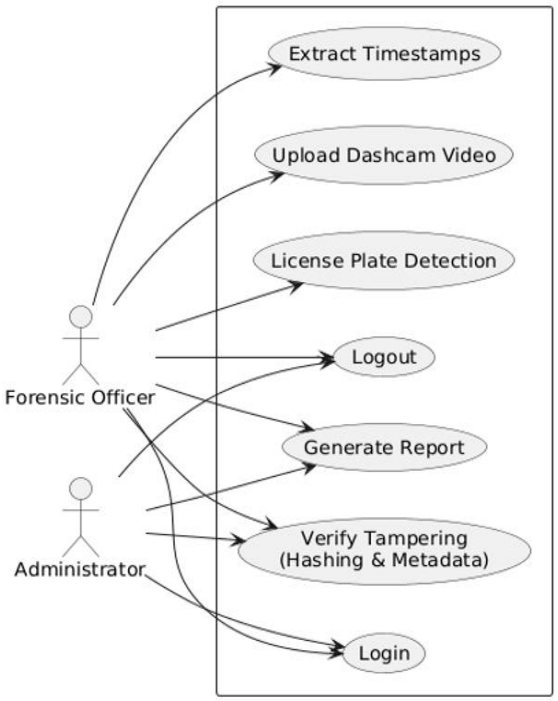


Fig. 6 *Use Case Diagram*

Fig. 6 shows the case diagram which outlines the interaction between the user (e.g., investigator or officer) and the system. The user can perform essential actions such as logging in, uploading dashcam footage, extracting timestamps, verifying video authenticity, and generating reports. It helps visualize the main functionalities offered by the system.

4.3 Class Diagram

A class diagram is a Unified Modeling Language (UML) diagram that represents the static structure of a system. It illustrates the classes, their attributes, methods, and the relationships among them. This diagram helps developers understand the structure and behavior of the system before implementation. For the Dashcam Footage Analysis Tool, the class diagram shows how different modules interact, including user authentication, video upload, timestamp extraction, tamper detection, license plate detection, and report generation [18]. Each class performs a specific role, promoting modularity and ease of maintenance.

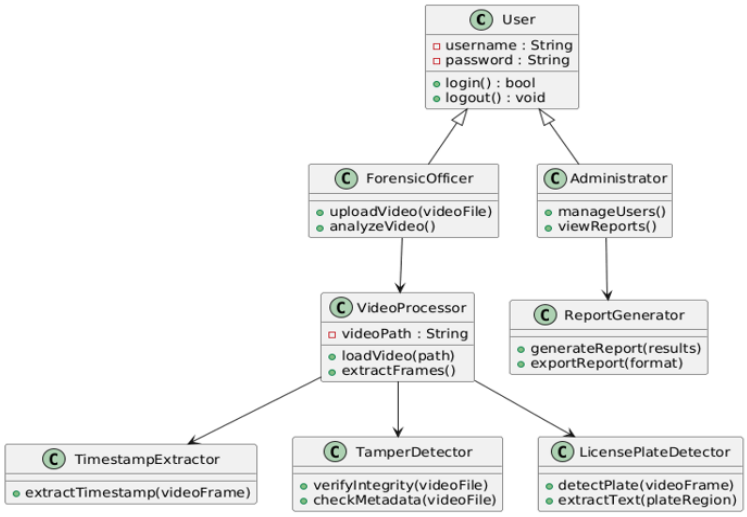


Fig. 7 *Class Diagram for the Dashcam Footage Analysis Tool*

Fig. 7 shows the class diagram that depicts the main classes of the Dashcam Footage Analysis Tool User, Video Processor, Timestamp Extractor, Tamper Detector, License Plate Detector, and Report Generator. These classes collaborate to perform core forensic functions such as video analysis, integrity verification, and evidence reporting.

4.4 Activity Diagram

Fig. 8 represents the activity diagram for extracting timestamps. After video upload, the tool processes the frames, applies OCR to detect timestamps, and structures the data for display.

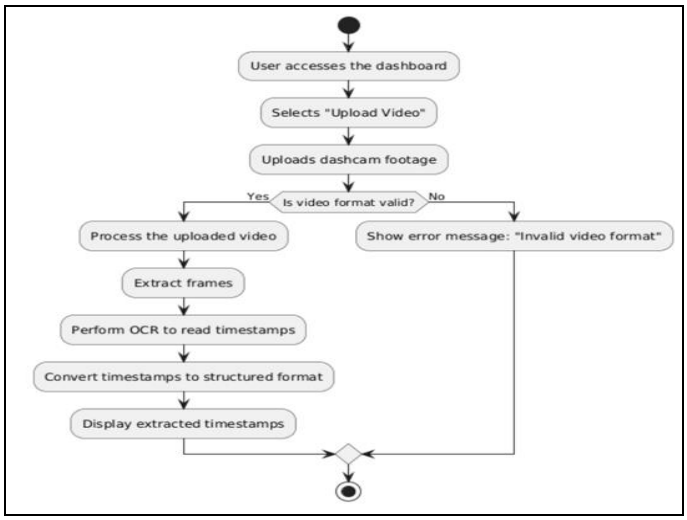


Fig. 8 *Activity Diagram for Timestamp Extraction*

Fig 9 shows the activity diagram for tamper detection begins when the user selects a video for integrity checking. The tool calculates the hash value, extracts metadata, and compares it with expected values to determine tampering.

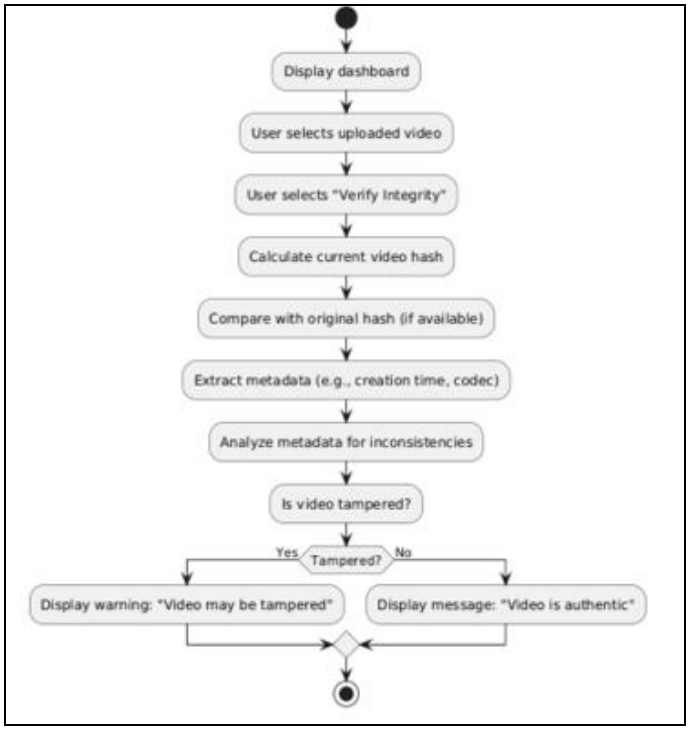


Fig. 2 *Activity Diagram for Tamper Detection*

Fig. 10 shows the activity diagram for license plate detection where the activity begins with the user selecting the license plate detection option. The system processes frames, locates the license plate, applies OCR, and displays the results. If no license plate is detected, the system notifies the user.

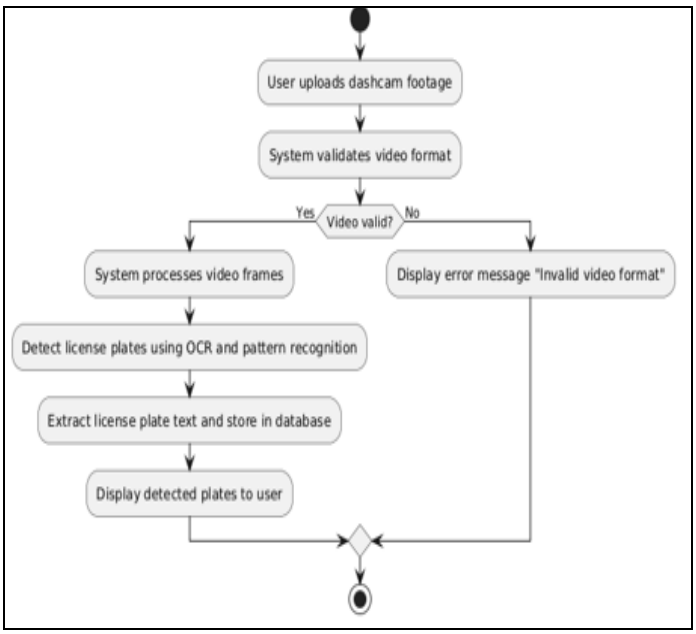


Fig. 10 *Activity Diagram for License Plate Detection*

4.5 Requirement Analysis

The Dashcam Footage Analysis Tool is designed to assist police officers and digital forensic investigators in efficiently analysing dashcam video recordings. The tool adopts an object-oriented approach that organizes its functionalities into distinct modules, each handling a specific forensic task. This modular structure ensures easier maintenance, scalability, and integration of future features.

The primary objective of the system is to automate key forensic processes, including video uploading, timestamp extraction, license plate recognition, tamper verification, and report generation for investigation purposes. Access to the tool is restricted to authorized users through a secure login interface to maintain the confidentiality and integrity of evidence. The system emphasizes user-friendliness, speed, and efficiency, particularly in real-world cases such as crime investigations or traffic accident analysis.

Table 3 *Functional Requirements*

Modules	Requirement
Login Module	• Allow authorized users to log in using a valid ID and password. • Restrict access to prevent unauthorized users from entering the system.
Video Upload Module	• Allow users to upload dashcam footage in formats such as MP4 and AVI. • Validate video type before allowing upload.
Time Extraction Module	• Detect and extract timestamps from video frames using OCR. • Convert extracted timestamps into structured data
Tamper Detection Module	• Use hashing algorithms (e.g., SHA-256) to verify the authenticity of video files. • Display metadata such as file size, format, and creation date.
License Plate Detection Module	• Automatically detect and recognize vehicle license plates from uploaded footage. • Extract plate numbers and store them in a structured form for reporting.
Report Generation Modul	• Compile all extracted data into a readable and printable report.

Table 4 *Non-functional Requirements*

Requirement	Description
Performance	The tool should be able to process and analyze uploaded footage efficiently.
Usability	The interface should be clean and easy to navigate, even for non-technical users.
Security	Only authenticated users should be able to access the tool.
Compatibility	The tool should support standard video formats and run on both Windows and Linux platforms.

4.6 Evidence Extraction Techniques and Algorithms

This section explains the core techniques and algorithms used in the Dashcam Footage Analysis Tool to extract digital forensic evidence reliably and systematically.

4.6.1 Timestamp Extraction Technique

The timestamp extraction process begins with frame sampling, where selected frames are extracted from the uploaded dashcam video at predefined intervals. A Region of Interest (ROI) is then identified to focus on the area where the timestamp is embedded in the video frame. Optical Character Recognition (OCR) using the Tesseract engine is applied to the ROI to recognize textual timestamp data. The extracted timestamp is validated to remove noise and formatting errors. Finally, the timestamp is structured into a standardized date–time format suitable for forensic reporting and evidence presentation.

4.6.2 License Plate Detection Technique

License plate extraction starts with frame selection to identify clear and stable frames suitable for analysis. Plate region detection is performed using image processing techniques to localize the vehicle license plate area within the frame. OCR is then applied to the detected plate region to recognize alphanumeric characters. A confidence score is assigned based on recognition, accuracy and character clarity. The recognized license plate number and confidence level are stored as evidential data for forensic examination.

4.6.3 Tamper Detection Algorithm

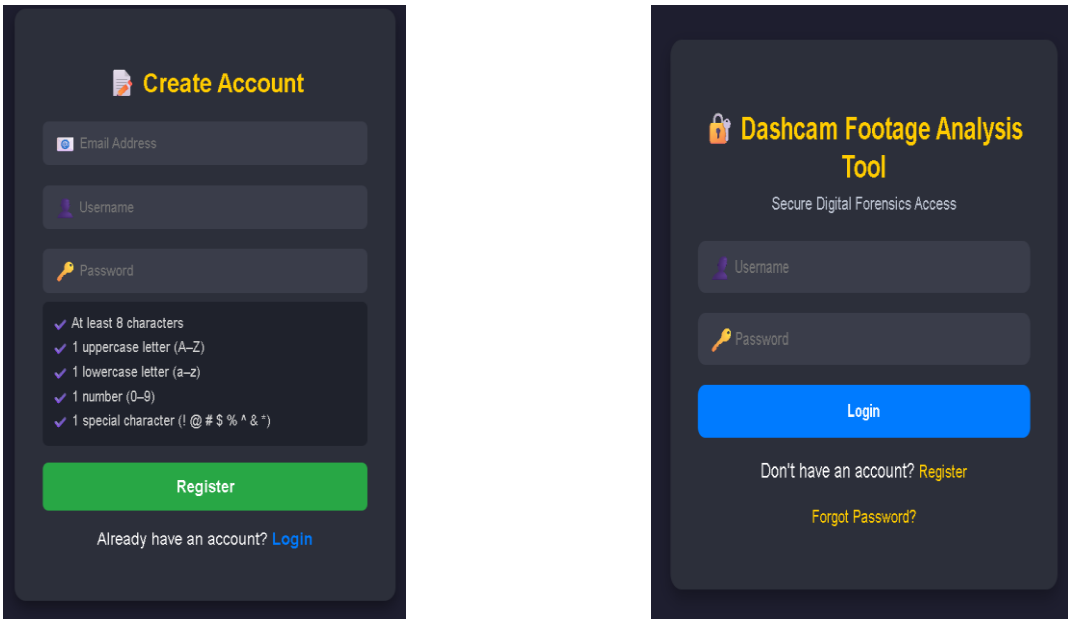
The tamper detection process begins by generating a SHA-256 hash value when the video file is first uploaded into the system. This original hash value is securely stored as a reference. During analysis or re-access of the video, the system recomputes the SHA-256 hash. The newly generated hash is compared with the original stored hash. If both hash values match, the video is flagged as Authentic; otherwise, it is flagged as Tampered, ensuring digital evidence integrity.

4.7 Implementation

The implementation phase translates the system design into a functional Dashcam Footage Analysis Tool prototype. This phase focuses on integrating the core modules, including user authentication, video upload, timestamp extraction, license plate recognition, tamper detection, and report generation, based on the design specifications presented earlier. The system was developed as a web-based application using Python and Flask for backend processing, with HTML, CSS, and JavaScript for the user interface. An iterative implementation approach was adopted to allow continuous testing and refinement of features, ensuring accuracy, usability, and reliability. This approach enables the system to effectively support digital forensic investigators in extracting and managing reliable dashcam evidence.

4.7.1 Registration and Login

The Registration and Login module as shown in Fig. 11 (a0-(b) allows users to securely create an account and access the Dashcam Footage Analysis Tool. User details are validated to ensure correct email format, unique credentials, and password compliance before being stored in the database. During login, the system verifies user credentials and restricts access to authorized users, ensuring secure and controlled system usage.



(a) (b)

Fig. 11 *Registration and Login*

4.7.2 Dashcam Footage Analysis Tool Main Interface

The Dashboard Module serves as the main interface of the Dashcam Footage Analysis Tool, providing users with centralized access to all forensic analysis functions after login. It allows investigators to navigate key modules such as video upload, time-tamp extraction, tamper detection, license plate detection, and report generation in a clear workflow sequence. The interface is designed for simplicity and clarity, ensuring efficient navigation and smooth progression through the forensic analysis process.

Fig 12 shows the main interface for the Dashcam Footage Analysis Tool, which also includes additional features such as logout functionality and quick module navigation. By providing a centralized and user-friendly interface, the Dashboard Module ensures that investigators can easily move from video upload to analysis and finally to report generation. It acts as the command center for the entire digital forensic workflow and keeps all core processes well-structured and easy to follow.

Applied Information Technology and Computer Science Vol. 7 No. 1 (2026) p. 1250-1269

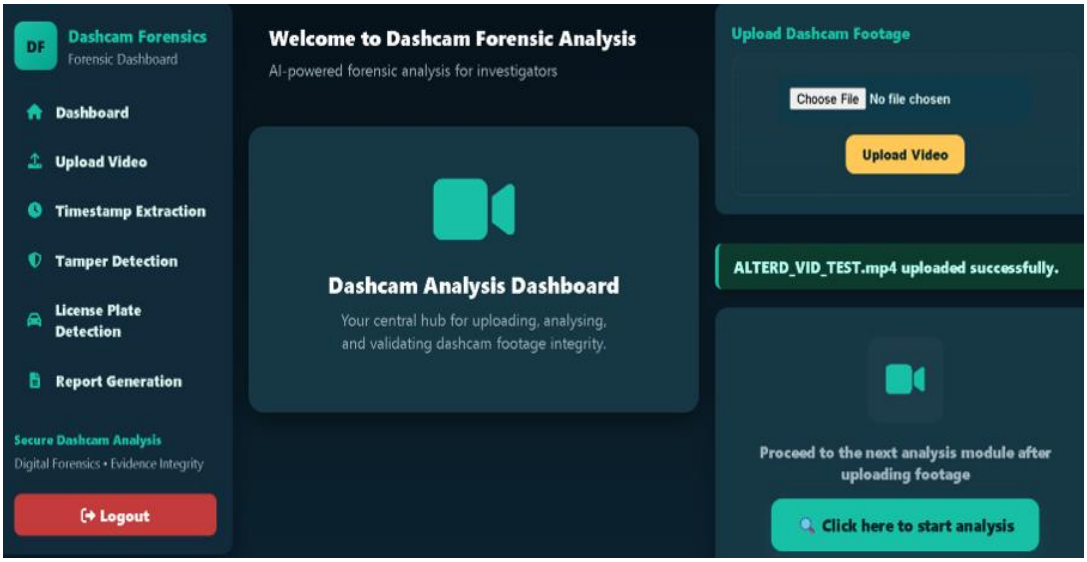


Fig. 12 *Dashcam Footage Analysis Tool main interface*

4.7.3 Video Upload

The Video Upload section in Fig 13 provides investigators with an interface to upload, manage, and organize dashcam video files for forensic analysis. This module ensures that video evidence is properly prepared and verified before proceeding to timestamp extraction and other forensic processes.

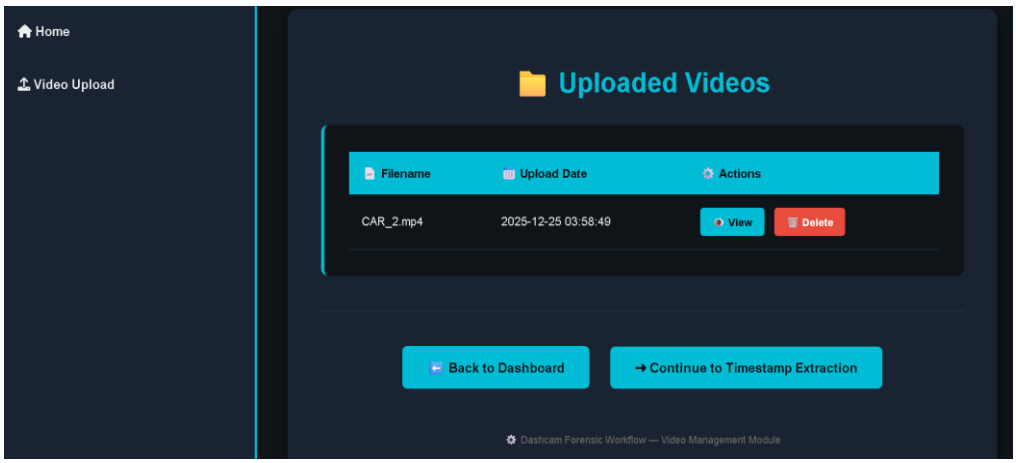


Fig. 13 *Video Upload Interface*

Fig. 12 shows the video upload interface, where users can upload new dashcam footage and view a list of previously uploaded videos along with their filenames and upload dates. The interface also provides actions to view or delete videos and includes a navigation option to proceed to the next stage of forensic analysis.

4.7.4 Video Viewing

The Video Viewing section allows users to preview uploaded dashcam footage directly within the system before conducting forensic analysis. This module helps investigators visually confirm the content, quality, and relevance of the selected video. Fig. 14 shows the video viewing interface, where the selected dashcam footage is displayed with standard playback controls. Navigation buttons are provided to return to the upload page or dashboard, ensuring smooth movement between forensic modules.

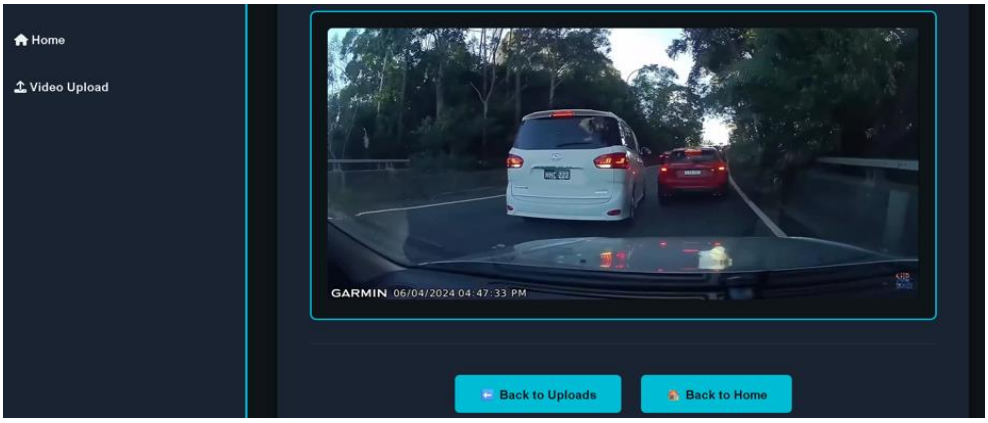


Fig. 14 *Video Viewing Interface*

4.7.5 Tamper Detection

The Tamper Detection section is designed to verify the integrity and authenticity of uploaded dashcam videos using cryptographic hashing techniques. This module ensures that digital evidence has not been altered after upload and remains legally reliable. Fig. 15 shows the tamper detection interface, which lists uploaded videos along with their integrity status. The system compares the current SHA-256 hash with the baseline hash to determine whether the video is authentic or tampered.

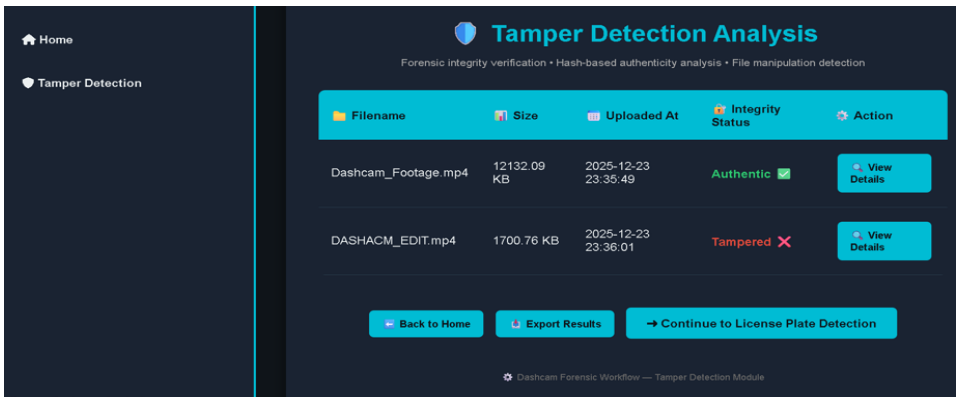


Fig. 15 *Tamper Detection Interface*

Fig. 16(a) shows an authentic verification result, confirming that the video maintains its original state and integrity. Fig. 16(b)-(e) shows a tampered verification result, where the system correctly detects modifications made to the original video file. They shows the detailed view interface, where hash comparison results are clearly presented together with the forensic method used. A navigation option allows investigators to return to the tamper detection list.

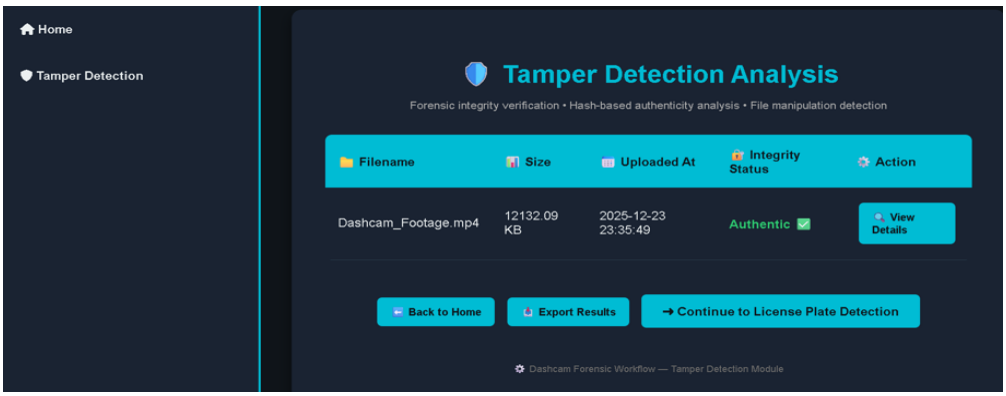
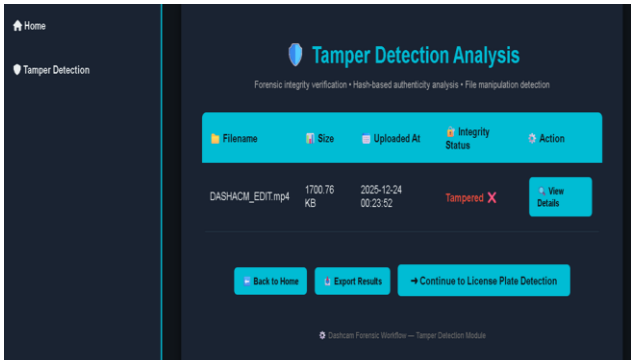
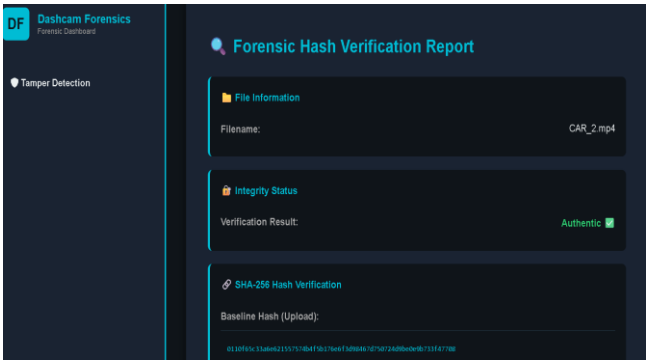


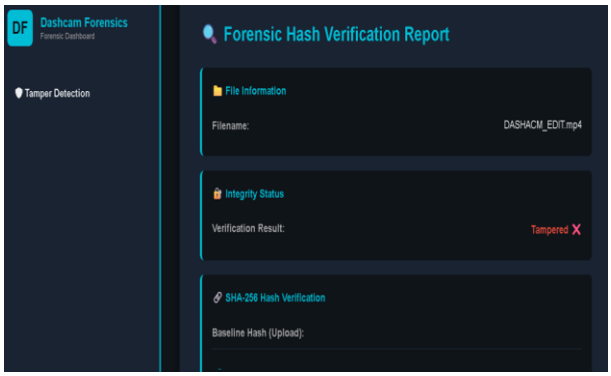
***Fig. 16 (a)**, Tamper Detection Authentic Result*



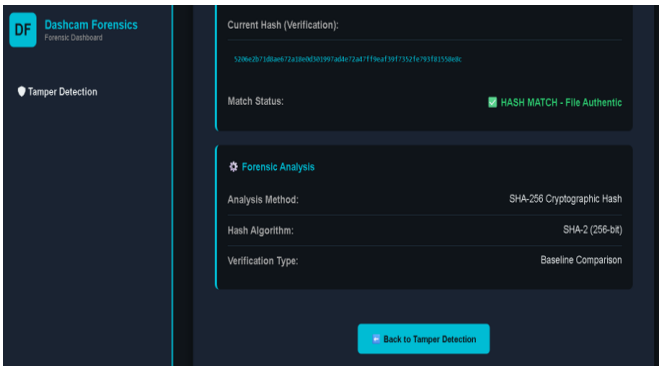
(b)



(c)



(d)

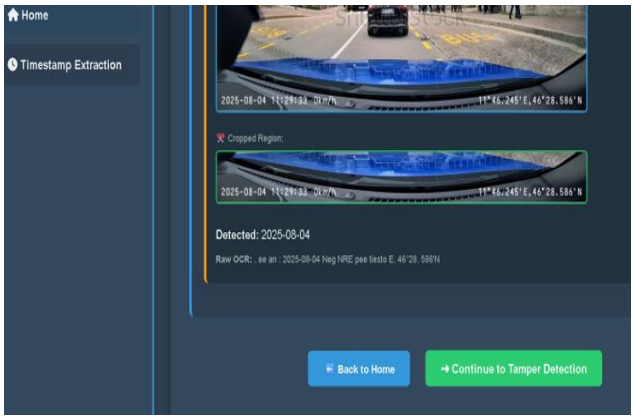


(e)

Fig. 16(b)-(e) *Tamper Detection Tampered Result*

4.7.6 Timestamp Extraction

This section will show that when accessing the Timestamp Extraction Module, the system automatically analyzes the uploaded dashcam video to identify and extract embedded timestamp information for forensic purposes. As shown in Fig. 17(a), the interface presents the results of the timestamp extraction process, including extracted dates, visual previews, and raw OCR outputs. Fig. 17(b) shows how to achieve accurate timestamp detection. The system scans several frames from the dashcam data



(a)

(b)

Fig. 17 *Timestamp Extraction Result*

4.8 License Plate Detection Results

The License Plate Detection Results Module displays all extracted license plate detections from the analyzed video. Multiple detections are shown to support evidence verification across different frames.

Fig.18 *License Plate Detection Results*

Fig. 18 shows the results interface, presenting cropped license plate images with confidence percentages in a gallery layout. Navigation options allow users to proceed to report generation or return to the dashboard.

4.9 Report Generation

The Report Generation Module compiles all forensic analysis results produced by the Dashcam Footage Analysis Tool into a single structured document. After completing timestamp extraction, license plate detection, and tamper verification, investigators can generate a comprehensive report through this module. As shown in Fig. 19, the generated report presents case details, extracted timestamps with cropped evidence, detected license plates, and hash-based integrity verification in a structured and forensically reliable format suitable for investigation and legal review

Fig. 19 *Report Generation interface*

4.10 Generated Forensic Report Document

The Generated Forensic Report Document represents the final output of the Dashcam Footage Analysis Tool in a professionally structured PDF format. The report consolidates all validated forensic findings, including timestamp evidence, license plate detection results, and integrity verification status. Fig. 20 illustrates the report generation interface, where users generate a final PDF that automatically compiles all extracted evidence, confidence values, and integrity results as the concluding stage of the forensic workflow.

Applied Information Technology and Computer Science Vol. 7 No. 1 (2026) p. 1250-1269

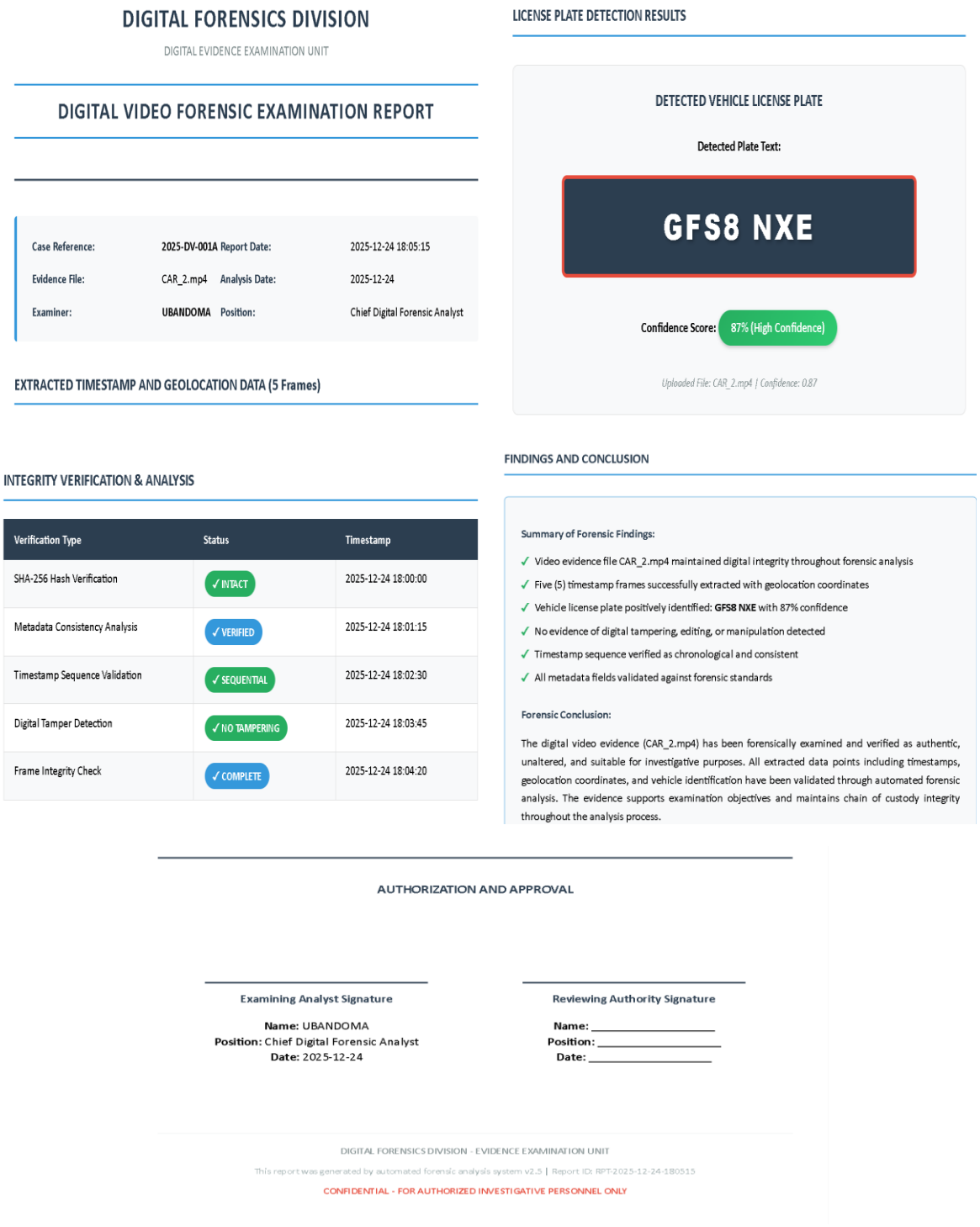


Fig. 20 *Report generation interface*

4.11 Review

The review phase was conducted to evaluate whether the Dashcam Footage Analysis Tool functioned according to the design specifications and forensic objectives. All core modules, including user authentication, video upload, timestamp extraction, license plate detection, tamper detection, and report generation, were reviewed to ensure correct functionality and smooth workflow progression. The system was verified to guide users logically from video upload through analysis and finally to report generation. From a forensic perspective, the review confirmed that the system produces clear and traceable evidence outputs, including cropped timestamp regions, license plate images with confidence scores, and hash-based integrity results. Minor interface and performance refinements were addressed during this phase, confirming that the prototype is stable, usable, and suitable for controlled forensic and academic use.

4.12 Testing

Testing is a critical phase in ensuring the accuracy, reliability, and forensic validity of the Dashcam Footage Analysis Tool. This phase focuses on verifying that all system modules function as intended and that extracted evidence remains accurate and legally admissible.

The Testing activities were conducted to validate core functionalities such as video upload, timestamp extraction, license plate detection, tamper verification, and report generation. These tests ensure the system produces consistent results and supports digital forensic investigation workflows.

4.12.1 Functional Testing

Functional testing was conducted to verify that each system module operates according to its intended purpose. This includes user authentication, video upload validation, timestamp extraction using OCR, license plate detection, tamper verification using hashing techniques, and automated report generation. The objective of this testing was to ensure that all features produce correct and consistent outputs when processing dashcam footage.

Table 5: *Test cases*

Functional Module	Test Case	Description	Expected Result	Test Result
Login	Valid login	User enters the correct username and password	User is authenticated and redirected to the dashboard	Pass
	Invalid username	User enters an unregistered username	The system displays an invalid username error	Pass
	Invalid password	User enters the correct username with the wrong password	The system displays an incorrect password error	Pass
	Empty fields	User submits the login form without credentials	System prompts user to fill required fields	Pass
Reset Password	Request reset (valid email)	User submits registered email	OTP is sent to the user's email	Pass
	Verify OTP	User enters correct OTP	System verifies OTP and allows password reset	Pass
	Invalid OTP	User enters incorrect OTP	The system displays an invalid OTP message	Pass
	Reset password	User enters and confirms new password	Password updated and redirected to login	Pass
	Unregistered email	User submits a non-existent email	The system displays an email not registered error	Pass
Video Upload	Upload a supported format	User uploads MP4/AVI file	Video uploaded successfully	Pass
	Unsupported format	User uploads an invalid file type	The system rejects the file and shows an error	Pass
	Large file upload	User uploads oversized video	The system rejects the file and shows an error	Pass
	No file selected	User clicks upload without a file	System prompts the user to select a file	Pass

Applied Information Technology and Computer Science Vol. 7 No. 1 (2026) p. 1250-1269

Table 5 *(cont.)*

Functional Module	Test Case	Description	Expected Result	Test Result
Timestamp Extraction	Extract timestamp	System processes video frames	Timestamp detected and displayed	Pass
	Display cropped timestamp	System highlights the timestamp region	Cropped timestamp image displayed	Pass
Tamper Detection	Authentic video	The system analyzes the original video	Video marked as Authentic	Pass
	Tampered video	System analyzing modified video	Video flagged as tampered	Pass
	No video selected	User runs detection without video	System prompts the user to upload a video	Pass
License Plate Detection	Detect plate	The system analyzes video	License plate detected and displayed	Pass
	Display the cropped plate	System highlights detected plate	Cropped plate image shown	Pass
	No visible plate	The video contains no plate	The system displays "No plate detected."	Pass
Report Generation	Generate report	The system compiles all extracted evidence	Forensic report generated successfully	Pass
	Download report	User downloads the generated report	PDF downloaded successfully	Pass

4.12.2 User Acceptance Testing

User Acceptance Testing (UAT) was conducted to evaluate the usability, functionality, and effectiveness of the Dashcam Footage Analysis Tool. A total of 16 respondents participated in the evaluation using a Google Form, consisting of students (81.3%), lecturers (6.3%), and IT/Digital Forensics practitioners (12.5%). The respondents included both users with prior experience in dashcam or video analysis tools (56.3%) and first-time users (43.8%), ensuring balanced and representative feedback.

The results indicate a high level of user satisfaction with the system. Most respondents rated system usability and effectiveness at scale 4 and 5, with 68.8% giving the highest usability rating and 75% awarding the highest score for system effectiveness. Core functions such as video upload, timestamp extraction, and license plate recognition were reported to perform reliably and were considered useful for digital forensic analysis.

Overall satisfaction was very strong, with 81.3% of users selecting the highest rating, and 100% of respondents confirming they would recommend the tool for digital forensic investigations. Minor suggestions for improvement included enhancing timestamp accuracy and refining detection performance for fast-moving vehicles, which provide direction for future enhancements.

The results demonstrate that the Dashcam Footage Analysis Tool achieved a high level of user acceptance across usability, functionality, and effectiveness metrics. The consistently positive ratings indicate that the system successfully supports timestamp and license plate evidence extraction in digital forensic contexts. While the feedback was overwhelmingly positive, minor improvements related to accuracy optimization and interface refinement can further enhance system performance. Overall, the findings confirm that the proposed tool is suitable for use as a digital forensic evidence support system.

5. Conclusion

This paper presented the development of a Dashcam Footage Analysis Tool for Timestamp and License Plate Evidence Extraction, designed to support digital forensic investigations through automated video analysis. By reviewing existing approaches and applying the Prototyping Model, the system was developed with a focus on accuracy, usability, and forensic reliability. The tool integrates key modules, including user login, video upload, timestamp extraction, license plate detection, tamper detection, and report generation. The use of Python-based technologies and iterative refinement ensured that the system meets investigative needs while remaining accessible to users with varying technical expertise. Future enhancements may include advanced object tracking, real-time analysis, and broader support for diverse dashcam formats. Overall, the proposed tool

contributes to improving the efficiency, credibility, and accessibility of dashcam evidence analysis in modern digital forensics.

Acknowledgement

The author would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM), for their guidance, facilities, and continuous support throughout this research.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design****: A.U. Abubakar, N. A. Abdullah;* ***data collection****: A.U. Abubakar, N. A. Abdullah;* ***analysis and interpretation of results****: A.U. Abubakar, N. A. Abdullah;* ***draft manuscript preparation****: A.U. Abubakar, N. A. Abdullah; All authors reviewed the results and approved the final version of the manuscript*.

References

[1] H. S. Lallie, "Dashcam forensic investigation guidelines," *Forensic Science International: Digital Investigation*, vol. 45, Jul. 2023, doi: 10.1016/j.fsidi.2023.301558.

[2] D. L. Carter, "• • • Law Enforcement Intelligence OperationS An Overview of Concepts, Issues and Terms Researched and Written By," 1990.

[3] B. L. Turner, E. M. Caruso, M. A. Dilich, and N. J. Roese, "Body camera footage leads to lower judgments of intent than dash camera footage," *Proc Natl Acad Sci U S A*, vol. 116, no. 4, pp. 1201–1206, Jan. 2019, doi: 10.1073/pnas.. 1805928116.

[4] J. Han and S. Lee, "A Study on the Processing of Timestamps in the Creation of Multimedia Files on Mobile Devices," *Journal of Information Processing Systems*, vol. 18, no. 3, pp. 402–410, Jun. 2022, doi: 10.3745/JIPS.04.0245.

[5] M. Branion-Calles *et al.*, "Underreporting and selection bias of serious road traffic injuries in auto insurance claims and police reports in British Columbia, Canada," *Transp Res Interdiscip Perspect*, vol. 30, Mar. 2025, doi: 10.1016/j.trip.2025.101375.

[6] E. Verolme and A. Mieremet, "Application of forensic image analysis in accident investigations," Sep. 01, 2017, *Elsevier Ireland Ltd*. doi: 10.1016/j.forsciint.2017.06.039.

[7] C. N. E. Anagnostopoulos, I. E. Anagnostopoulos, I. D. Psoroulas, V. Loumos, and E. Kayafas, "License plate recognition from still images and video sequences: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 9, no. 3, pp. 377–391, Sep. 2008, doi: 10.1109/TITS.2008.922938.

[8] B. Prasetiyo, Alamsyah, M. A. Muslim, Subhan, and N. Baroroh, "Automatic geotagging using GPS EXIF metadata of smartphone digital photos in tree planting location mapping," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Jun. 2021. doi: 10.1088/1742-6596/1918/4/042001.

[9] *Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI ' '17) : Boston, MA, USA, March 27 - 29, 2017*. USENIX Association, 2017.

[10] Z. Al-Ameen and C. Al-Atroshi, "Modern Visibility Enhancement and Tampering Detection Tools of Digital Image Forensics," *TECHART: Journal of Arts and Imaging Science*, vol. 4, no. 1, p. 32, Feb. 2017, doi: 10.15323/techart.. 2017.2.4.1.32.

[11] A. Jiménez-Meza, J. Arámburo-Lizárraga, and E. de la Fuente, "Framework for Estimating Travel Time, Distance, Speed, and Street Segment Level of Service (LOS), based on GPS Data," *Procedia Technology*, vol. 7, pp. 61–70, 2013, doi: 10.1016/j.protcy.2013.04.008.

[12] E. Giovannini *et al.*, "Importance of dashboard camera (Dash Cam) analysis in fatal vehicle–pedestrian crash reconstruction," *Forensic Sci Med Pathol*, vol. 17, no. 3, pp. 379–387, Sep. 2021, doi: 10.1007/s12024-021-00382-0.

[13] S. D. Nelson, G. Del Fiol, H. Hanseler, B. I. Crouch, and M. R. Cummins, "A case report of refining user requirements for a health information exchange dashboard," *Appl Clin Inform*, vol. 7, no. 1, pp. 22–32, 2016, doi: 10.4338/ACI-2015-07-CR-0091.

[14] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Academic Press.

[15] Smith, R. (2007). An overview of the Tesseract OCR engine. *Proceedings of the Ninth International Conference on Document Analysis and Recognition (ICDAR)*, 629–633.
[16] Zeng, J., Li, M., & Cai, Y. (2015). A Tracking System Supporting Large-Scale Users Based on GPS and G-Sensor. *International Journal of Distributed Sensor Networks*, *2015*. https://doi.org/10.1155/2015/862184
[17] Suhardjono, B., Handayani, P., Sugiarto, H., Aisyah, N., & Syah Putra, A. (2022). *Forensic Analysis Video Metadata Authenticity Detection Using Exiftool.1*.

Appendix A:

presents the User Acceptance Testing (UAT) questionnaire and summary of responses collected for the Dashcam Footage Analysis Tool.The questionnaire was distributed via Google Forms and completed by 16 respondents consisting of students, lecturers, and IT/Digital Forensics practitioners. The appendix includes the survey questions, response options, and graphical summaries of the collected data used to evaluate system usability, functionality, effectiveness, and overall user satisfaction.