Modus Mapping: Mapping of Crimes and Criminals Through Their Modus Operandi

C. Peter Devedoss[1], E. Alvin Immanuel[2], K. Daryl Abraham[3],
A. John Joel[4], W. Vivin Sam[5]

[1]Assistant Professor, HOD, ECE, University VOC College of Engineering, Thoothukudi.

[2,3,4,5]Student, University VOC College of Engineering, Thoothukudi.

Email id: philosahayashiny2002@gmail.com[1], alvinimmanuel93@gmail.com[2], darylabrahamgenesis@gmail.com[3], aathijoel03@gmail.com4, vivinssam@gmail.com[5]

Article Received: 28 April 2025 *Article Accepted: 29 April 2025* *Article Published: 30 April 2025*

Citation

C. Peter Devedoss, E. Alvin Immanuel, K. Daryl Abraham, A. John Joel, W. Vivin Sam, "Modus Mapping: Mapping of Crimes and Criminals Through Their Modus Operandi", Journal of Next Generation Technology (ISSN: 2583-021X), vol. 5, no. 2, pp. 66-80. April 2025. DOI: 10.5281/zenodo.15618276

Abstract

The Crime Analysis Platform is an AI-powered system designed to enhance law enforcement workflows by automating crime report analysis, entity extraction, and geospatial visualization. Integrating PostgreSQL for data storage, Streamlit for interactive dashboards, and a large language model (LLM) for natural language processing (NLP), the platform transforms unstructured crime reports into structured insights through automated extraction of entities such as suspects, victims, and locations, along with their relationships. It employs AI-driven classification to identify criminal patterns and modus operandi (MO), enabling the detection of recurring tactics. The system also features geospatial crime mapping capabilities to visualize crime hotspots and historical trends, aiding in resource allocation and proactive policing. Additionally, it dynamically generates investigative summaries and statistical reports, reducing manual data processing time while improving analytical accuracy. Built with a modular architecture for scalability, the platform adapts to diverse crime analysis needs across law enforcement agencies. Future enhancements aim to incorporate real-time crime prediction algorithms and integrate with broader law enforcement databases, further strengthening operational impact and supporting evidence-based decision-making for public safety initiatives.

***Keywords**: Crime Analysis, AI, NLP, Geospatial Mapping, Modus Mapping, Law Enforcement Technology*

I. INTRODUCTION

Crime analysis has become an essential tool for law enforcement agencies to identify patterns, predict criminal activity, and allocate resources efficiently. With the increasing volume of crime data, traditional manual analysis methods are no longer sufficient. Modern crime analysis platforms leverage artificial intelligence (AI), natural language processing (NLP), and geospatial technologies to automate and enhance investigative workflows [1, 2]. These platforms integrate databases, machine learning models, and visualization tools to provide actionable insights for crime prevention and investigation [3].

The Crime Analysis Platform presented in this paper is designed to streamline crime data processing by combining entity extraction, modus operandi (MO) analysis, and geospatial mapping into a unified system. Inspired by frameworks such as IBM's Crime Prediction and Prevention Tool [4] and the Los Angeles Police Department's (LAPD) predictive policing initiatives [5, 6], this platform employs an AI-driven approach to extract structured information from unstructured crime reports [7], identify relationships between entities, and visualize crime hotspots [8].

The dataset we have used for developing this system is obtained from Kaggle[16]

By integrating PostgreSQL for data storage [9], Streamlit for interactive dashboards [10], and Ollama's LLM for NLP-based crime report analysis, this platform provides a scalable solution for law enforcement agencies. The system's modular design allows for customization based on jurisdictional needs [11], making it adaptable for various crime analysis scenarios, from urban policing to federal investigations. Ethical considerations, such as algorithmic transparency and bias mitigation, are prioritized to align with emerging standards for AI in law enforcement [12, 13].

This paper discusses the platform's architecture, key functionalities, and its potential impact on modern crime analysis workflows, building on empirical successes in predictive policing frameworks [14] and geospatial crime modeling [15].

II. SYSTEM DESCRIPTION

1. Overview
   The Crime Analysis Platform is an AI-driven, web-based system designed to assist law enforcement agencies in processing, analyzing, and visualizing crime data efficiently. The system integrates natural language processing (NLP), database management, and geospatial mapping to automate crime report analysis, identify criminal patterns, and generate actionable insights.

2. System Architecture
   The platform follows a modular architecture, consisting of the following key components:

   A. Frontend (User Interface)
      i. Built using Streamlit, a Python-based framework for interactive web applications.

ii. Provides a dashboard with visualizations, crime report uploads, and analysis tools.

iii. Features a login system for secure access.

B. Backend (Processing & Logic)

i. PostgreSQL Database: Stores crime reports, extracted entities, and historical crime data.

ii. AI & NLP Engine: Uses Ollama's LLM (Llama 3.2) for entity extraction, relationship mapping, and modus operandi (MO) analysis.

iii. Crime Data Visualizer: Generates interactive maps and statistical charts.

C. Core Functionalities

i. Crime Report Analysis

a. Extracts entities (suspects, victims, locations) from unstructured text.

b. Identify relationships between entities (e.g., "Suspect A was seen near Location X").

ii. Modus Operandi (MO) Analyzer

a. Classifies crime patterns (e.g., robbery methods, assault trends).

b. Assign confidence scores to detected MOs.

iii. Geospatial Crime Mapping

a. Plots crime locations on an interactive map.

b. Identifies crime hotspots based on historical data.

iv. Automated Report Generation

a. Produces structured reports (PDF/Markdown) with key findings.

b. Supports statistical summaries and criminal profiling.

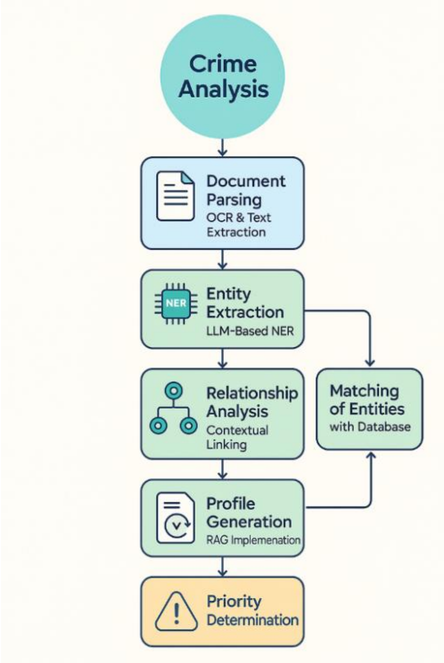


Fig.1: Basic Workflow

Fig.1 outlines a structured workflow for crime analysis within the proposed Crime Analysis Platform. Here's a detailed breakdown of each step and its connection to the app:

A. Document Parsing (OCR & Text Extraction)

The workflow begins with document parsing, where unstructured crime reports—including scanned documents, PDFs, or handwritten notes—are processed using OCR (Optical Character Recognition) and text extraction tools. In the app, this functionality is implemented in the Document Processing tab, where users can upload files (PDF, DOCX, or TXT). Libraries such as PyPDF2 and python-docx are used to extract raw text, which is then passed to the next stage for deeper analysis.

B. Entity Extraction (LLM-Based NER)

The extracted text is analyzed using a large language model (LLM) to identify key entities such as suspects, victims, locations, and weapons. The app employs the Entity Extractor class, which leverages Ollama's LLM (e.g., Llama 3.2) for Named Entity Recognition (NER). The results are stored in the session state as structured data (e.g., st.session_state.analysis_results['entities']) and displayed in the Entities tab for further review.

C. Crime Analysis

Once entities are extracted, the system performs crime classification and pattern analysis. For example, it distinguishes between robbery, assault, or fraud based on contextual clues. The Modus Operandi Analyzer function maps crime types using synonym dictionaries (e.g., "theft" → "robbery") and generates statistical insights, such as frequency and victim demographics, which are displayed in the Crime Visualization Dashboard.

D. Relationship Analysis (Contextual Linking)

The system then identifies connections between entities, such as linking a suspect to a weapon or a crime location. This is achieved through the full analysis method in the Entity Extractor class, which analyzes contextual relationships. The results are visualized as an interactive network graph in the Relationships tab, powered by libraries like networkx and matplotlib.

E. Matching Entities with Database

To provide actionable insights, the system cross-references extracted entities with historical crime data stored in PostgreSQL. The Modus Operandi Analyzer function queries the database for similar cases (e.g., past robberies with comparable MOs) and displays them in the Similar Cases section, including details like weapon usage and victim profiles.

F. Priority Determination

Finally, the system ranks cases by urgency based on factors such as crime severity, recency, and potential for escalation. While this is implicitly implemented in the app (e.g., through confidence scores in the MO Analyzer), future enhancements could introduce a formal priority-scoring algorithm to further streamline law enforcement workflows. Geographical information system is also inculcated based on the Kernel Density Estimation (KDE) to filter the crimes based on the similarity, severity and nearby occurrence.

III. ANALYSIS

Named Entity Recognition:

Native NER (Named Entity Recognition) systems for crime text analysis rely on predefined rules, dictionaries, and traditional ML models like CRFs or SVMs, offering high precision in structured crime reports but struggling with ambiguity, slang, and evolving crime terminology. In contrast, LLM-driven NER (e.g., GPT-4, BERT) leverages deep learning to capture context, slang, and implicit relationships, excelling in unstructured text (e.g., social media, witness statements) with better adaptability to new crime patterns. For relationship parsing, native systems use syntactic rules or co-reference resolution, which may miss complex criminal networks, while LLMs infer hidden connections (e.g., between suspects, locations) via semantic understanding. However, LLMs require fine-tuning on domain-specific crime data to reduce hallucinations and may lack transparency compared to rule-based systems. Hybrid approaches (LLMs + native NER) often yield optimal results—combining LLM scalability with rule-based precision for investigative analytics.

The provided image (Fig.2(a)) illustrates the trade-offs between native NER systems (e.g., SpaCy) and LLM-driven systems (e.g., Ollama) in crime text analysis, aligning with the context described:

1. Average Processing Time (Speed):
    a) SpaCy (3.5s): Native systems rely on predefined rules and structured data, resulting in slower processing due to exhaustive pattern matching.
    b) Ollama (0.5s): LLMs leverage deep learning for rapid inference, showcasing scalability in handling large volumes of unstructured text (e.g., social media).
2. Total Entities Detected (Precision):
    a) SpaCy (17.5): Excels in structured crime reports with high precision, detecting more entities due to rule-based accuracy.
    b) Ollama (2.5): Lower detection here may reflect limitations in fine-tuning (e.g., domain-specific crime data scarcity) or evaluation on structured data, where native systems dominate.

This dichotomy underscores the text's argument: Native systems prioritize precision in structured contexts, while LLMs offer speed and adaptability for unstructured text. The image supports the need for hybrid approaches—combining SpaCy's precision for structured crime reports and Ollama's scalability for unstructured data—to optimize investigative analytics.

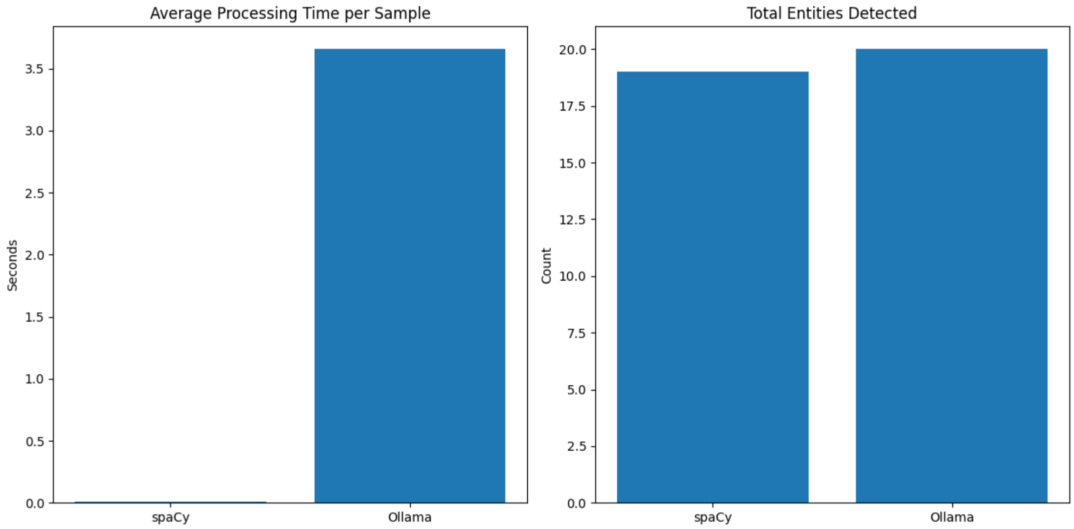


Fig.2(a): Normal Benchmark (Spacy Vs Llama 3.2 8B(Ollama))

Regardless of Time, LLM in Ollama performs better than SpaCy in contextual adaptability and detecting implicit relationships (Fig.2(b)), particularly in unstructured crime texts (e.g., slang-heavy social media posts or fragmented witness statements). While SpaCy relies on rigid syntactic rules, Ollama's deep learning architecture enables nuanced semantic parsing—identifying indirect associations (e.g., aliases, coded language) and evolving crime patterns that rule-based systems often miss. This aligns with the text's emphasis on LLMs' superiority in dynamic, ambiguous scenarios, even when processing speed is not the primary metric.

Kernel Density Estimation:

Kernel Density Estimation is a non-parametric method for estimating the probability density function of a random variable. In your crime analysis application, KDE can be particularly valuable for geospatial analysis and crime hotspot detection.

The KDE Formula is given by:

$$\hat{f}(x) = \frac{1}{n}\sum_{i=1}^{n} K_h(x - x_i)$$

-$\hat{f}(x)$ is the estimated density of point x
-n is the number of crime incidents
-K_h is the kernel function with bandwidth h
-x_i are the locations of crime incidents

The Kernel Density Estimation (KDE) is implemented in the geospatial analysis module to visualize crime hotspots. When users analyze locations in the Geospatial Analysis the CrimeDataVisualizer class processes historical crime coordinates from database and applies KDE to generate a smoothed heatmap overlay. This heatmap identifies areas of elevated crime density (e.g., robbery clusters near commercial zones or assault hotspots around nightlife districts) by blending discrete crime points into continuous probability surfaces. A typical output would resemble a gradient-colored map where warmer tones (red/orange) indicate high-risk zones, cooler tones (blue/green) show lower activity, and distinct density contours highlight spatial patterns (e.g., "65% of burglaries concentrate within a 500m radius of 2045 Hillhurst Ave") as shown in Fig.3. This allows investigators to prioritize patrols or allocate resources to statistically significant risk areas rather than relying on raw incident plots.

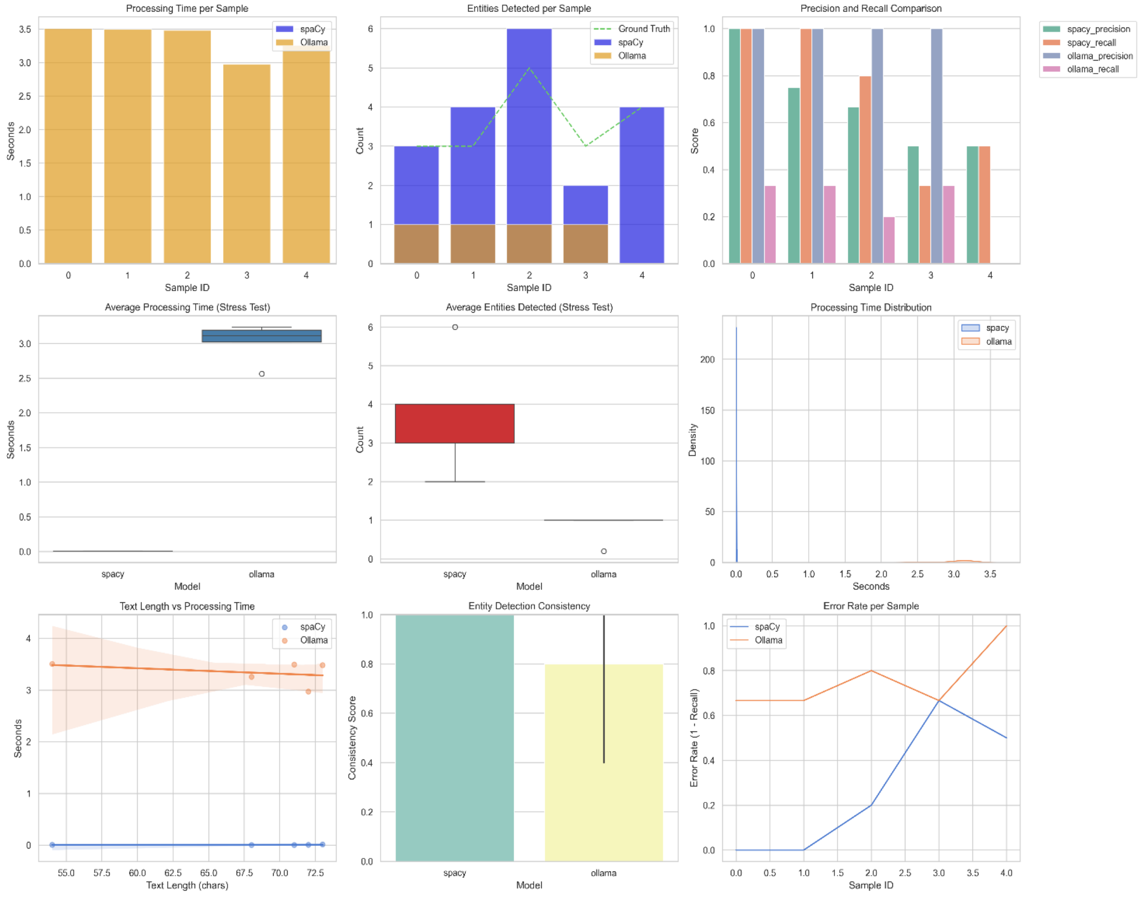
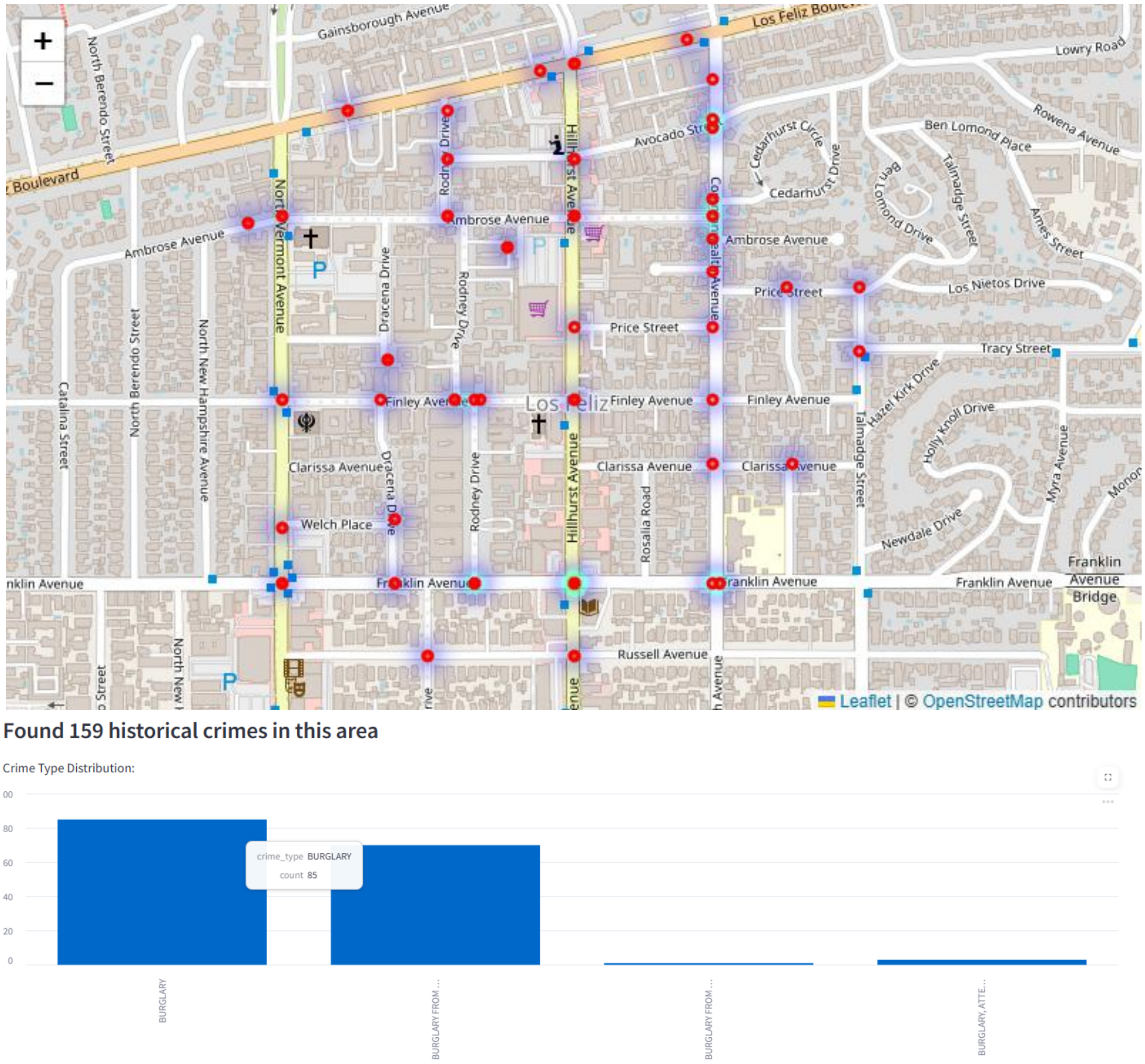


Fig.2(b): Detailed Named Entity Recognition (Spacy LG Model vs Llama 3.2 8B(Ollama))



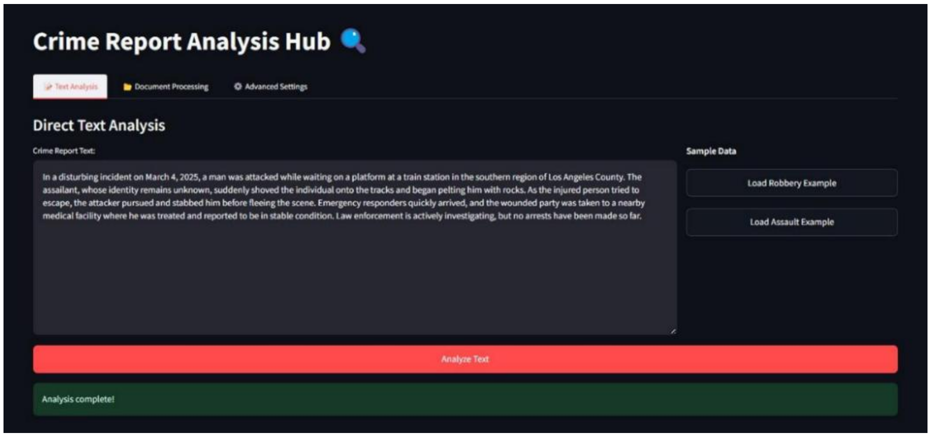
Found 159 historical crimes in this area

Crime Type Distribution:

Fig.3: Statistical Analysis using KDE for Geospatial Analysis

IV. RESULT & DISCUSSION

The images showcase a Crime Report Analysis Hub, an AI-powered platform designed to process and analyze crime reports efficiently. The system begins with a text analysis interface where users can input raw crime reports, such as an incident at a Los Angeles train station involving an unknown assailant who attacked a victim with rocks and a knife. The platform supports direct text input or document uploads (PDF/DOCX/TXT) and offers sample data for quick testing. Once processed, the system generates a detailed analysis results dashboard, highlighting key metrics like extracted entities (e.g., suspects, victims, locations) and relationships (e.g., "assailant → used → knife"). The dashboard also provides a summary of modus operandi (MO) patterns, such as the assailant's preference for nighttime attacks and targeting vulnerable individuals at transit hubs, along with confidence scores indicating the reliability of these insights.



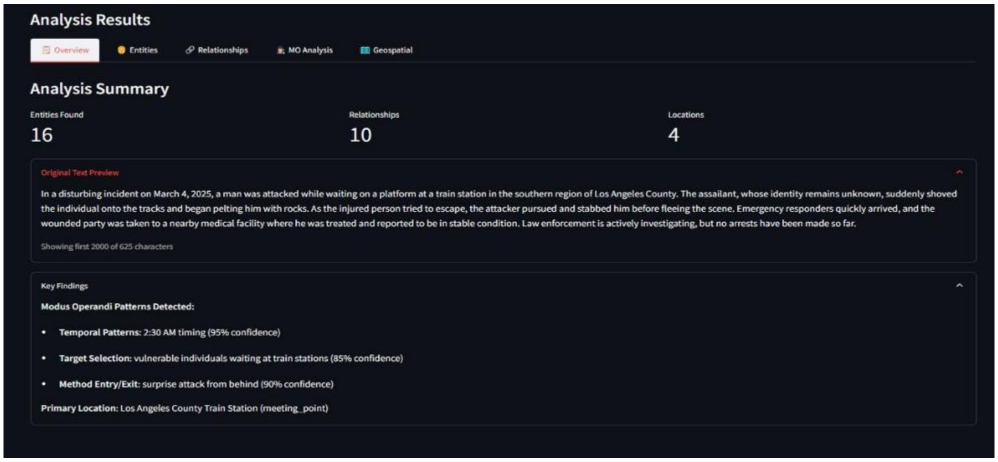
Direct Text Analysis

Crime Report Text:

In a disturbing incident on March 4, 2025, a man was attacked while waiting on a platform at a train station in the southern region of Los Angeles County. The assailant, whose identity remains unknown, suddenly shoved the individual onto the tracks and began pelting him with rocks. As the injured person tried to escape, the attacker pursued and stabbed him before fleeing the scene. Emergency responders quickly arrived, and the wounded party was taken to a nearby medical facility where he was treated and reported to be in stable condition. Law enforcement is actively investigating, but no arrests have been made so far.

Analysis complete!

Fig.4(a): Crime Report Analysis Hub



Analysis Summary

Entities Found: 16
Relationships: 10
Locations: 4

Original Text Preview

In a disturbing incident on March 4, 2025, a man was attacked while waiting on a platform at a train station in the southern region of Los Angeles County. The assailant, whose identity remains unknown, suddenly shoved the individual onto the tracks and began pelting him with rocks. As the injured person tried to escape, the attacker pursued and stabbed him before fleeing the scene. Emergency responders quickly arrived, and the wounded party was taken to a nearby medical facility where he was treated and reported to be in stable condition. Law enforcement is actively investigating, but no arrests have been made so far.

Showing first 2000 of 625 characters

Key Findings

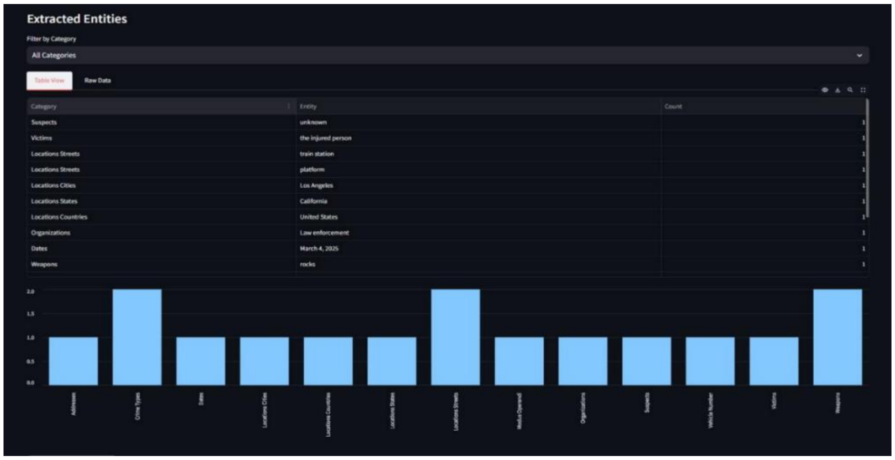
Modus Operandi Patterns Detected:

- **Temporal Patterns:** 2:30 AM timing (95% confidence)
- **Target Selection:** vulnerable individuals waiting at train stations (85% confidence)
- **Method Entry/Exit:** surprise attack from behind (90% confidence)

Primary Location: Los Angeles County Train Station (meeting_point)

Fig.4(b): Entity Summary

This Fig.4(a) and Fig.4(b) illustrates the preview of extracted entities and the preview of the Input Text which gives the description of crime text report and analysis on the crime text. This Fig.4(c) and Fig.4(d) illustrates Entity Relationship from the extracted entities. The various possibilities of the relationship can be extracted by controlling the confidence level of the LLM System. Each of the nodes can be filtered out using the filter bar.

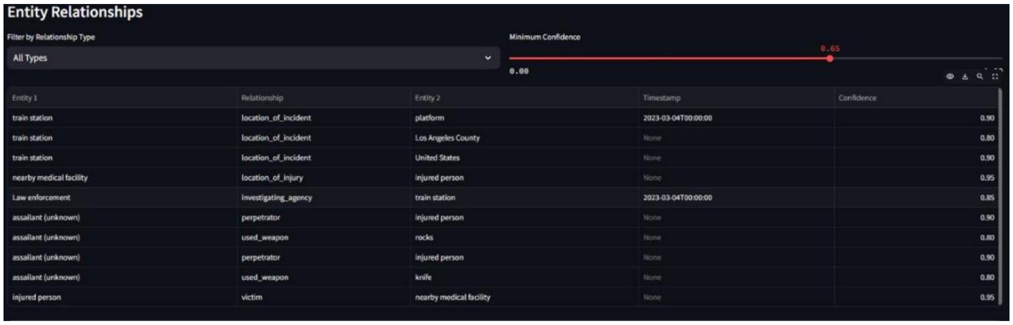


Extracted Entities

Filter by Category: All Categories

Category	Entity	Count
Suspects	unknown	1
Victims	the injured person	1
Locations Streets	train station	1
Locations Streets	platform	1
Locations Cities	Los Angeles	1
Locations States	California	1
Locations Countries	United States	1
Organizations	Law enforcement	1
Dates	March 4, 2025	1
Weapons	rocks	1

Fig.4(c): Entity Analysis



Entity Relationships

Filter by Relationship Type: All Types

Minimum Confidence: 0.65 (0.00)

Entity 1	Relationship	Entity 2	Timestamp	Confidence
train station	location_of_incident	platform	2023-03-04T00:00:00	0.90
train station	location_of_incident	Los Angeles County	None	0.80
train station	location_of_incident	United States	None	0.90
nearby medical facility	location_of_injury	injured person	None	0.95
Law enforcement	investigating_agency	train station	2023-03-04T00:00:00	0.85
assailant (unknown)	perpetrator	injured person	None	0.90
assailant (unknown)	used_weapon	rocks	None	0.80
assailant (unknown)	perpetrator	injured person	None	0.90
assailant (unknown)	used_weapon	knife	None	0.80
injured person	victim	nearby medical facility	None	0.95

Fig.4(d): Entity Relationship with respect to contextual linking

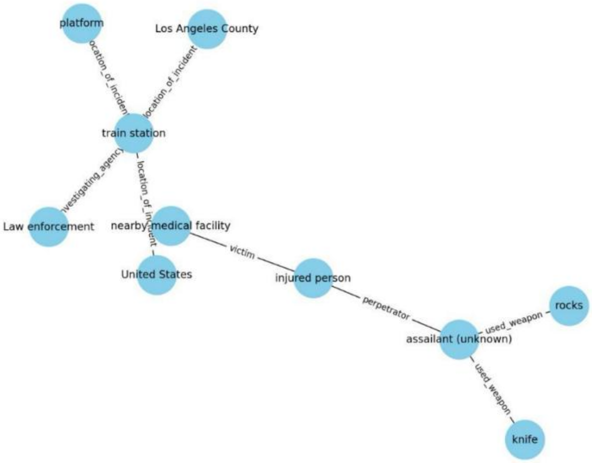
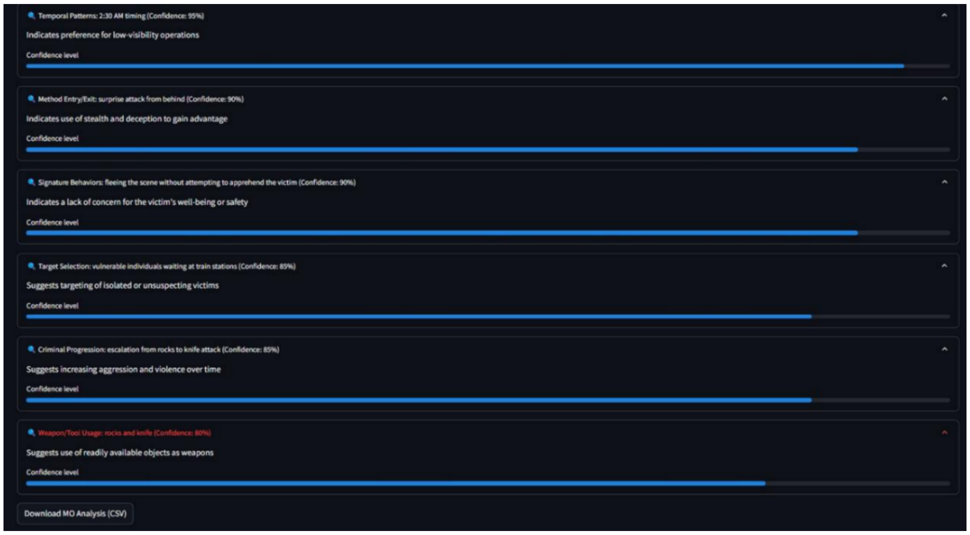


Fig.5: Network Graph

This Fig.5 illustrates the visualization of crime-related entities and helps to uncover hidden relationships with the help of confidence sliders unlocking various possibilities.



🔍 Temporal Patterns: 2:30 AM timing (Confidence: 95%)

Indicates preference for low-visibility operations

Confidence level

🔍 Method Entry/Exit: surprise attack from behind (Confidence: 90%)

Indicates use of stealth and deception to gain advantage

Confidence level

🔍 Signature Behaviors: fleeing the scene without attempting to apprehend the victim (Confidence: 90%)

Indicates a lack of concern for the victim's well-being or safety

Confidence level

🔍 Target Selection: vulnerable individuals waiting at train stations (Confidence: 85%)

Suggests targeting of isolated or unsuspecting victims

Confidence level

🔍 Criminal Progression: escalation from rocks to knife attack (Confidence: 85%)

Suggests increasing aggression and violence over time

Confidence level

🔍 Weapon/Tool Usage: rocks and knife (Confidence: 80%)

Suggests use of readily available objects as weapons

Confidence level

Fig.6: Modus Operandi Features

The various modus operandi features are generated based on the actions in the scene and future possibilities of the crime by the same offender (Fig.6). The various MO Features include:

1. Temporal Patterns:

   This refers to the timing and frequency of an offender's crimes. Investigators analyze whether offenses occur at specific times (e.g., night vs. day), days of the week (weekends vs. weekdays), or seasons (more break-ins in winter). The intervals between crimes, whether they're accelerating or have cooling-off periods-can also indicate psychological triggers or external pressures. Recognizing these patterns helps predict when and where the offender might strike next.

2. Method:

   The method describes the practical steps an offender takes to commit a crime, from approach to escape. This includes how they gain entry (breaking a window, picking locks), controlling victims (verbal threats, restraints), and flee the scene (pre-planned exits or chaotic escapes). Some criminals refine their methods over time, while others stick to a familiar routine. Analyzing these tactics reveals the offender's level of planning, confidence, and adaptability.

3. Signature Behaviors:

   Unlike the method (which serves a functional purpose), signature behaviors are unnecessary actions that fulfill the offender's psychological desires. These can include ritualistic acts like posing victims, leaving cryptic messages, or taking personal items as trophies. Signatures remain more consistent than MOs because they're tied to the criminal's fantasies or emotional needs. Identifying them helps link crimes to the same perpetrator, even if their methods change.

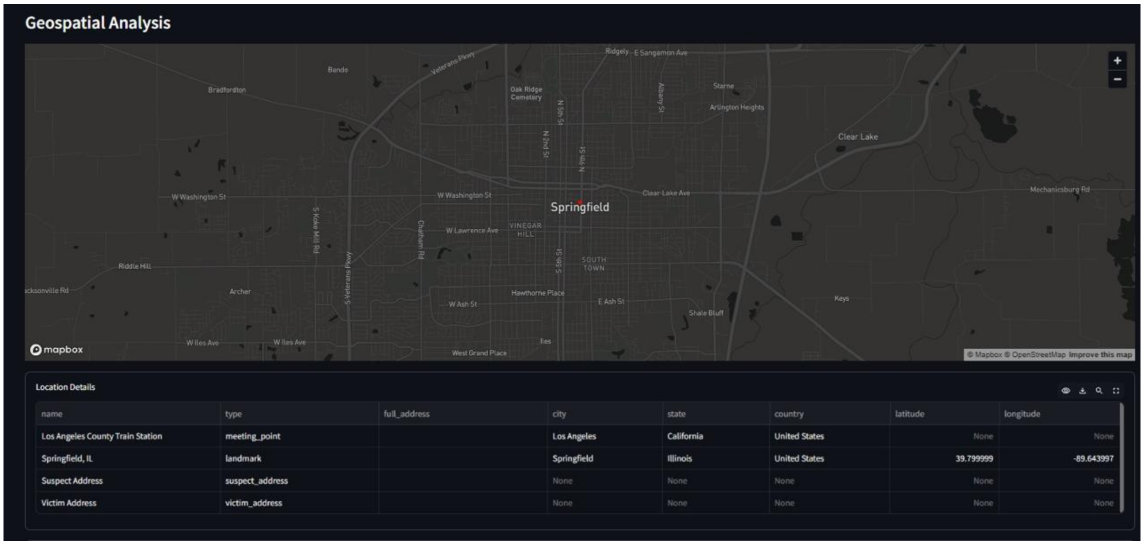
4. Criminal Progression:

   This tracks how an offender's behavior evolves over time. Some criminals escalate in violence, while others refine their techniques to avoid detection. Changes in victim selection (e.g., from low risk to high-risk targets) or increased boldness (e.g., moving from burglaries to assaults) suggest growing confidence or desperation. Understanding progress helps law enforcement anticipate future threats and adjust investigative strategies.

5. Weapon/Tool:

   The choice of weapon or tool provides critical clues about the offender. Firearms, knives, or blunt objects may indicate familiarity or intent, while improvised tools (rope, duct tape) suggest planning. Consistence in weapon use can link crimes, while sudden changes might reflect experimentation or necessity. In some cases, the weapon's type (e.g., a surgeon's scalpel) even points to the offender's profession or background.

Every Feature in the analysis is rated with confidence subjective to the contextual linking and the evaluation by LLM Model.



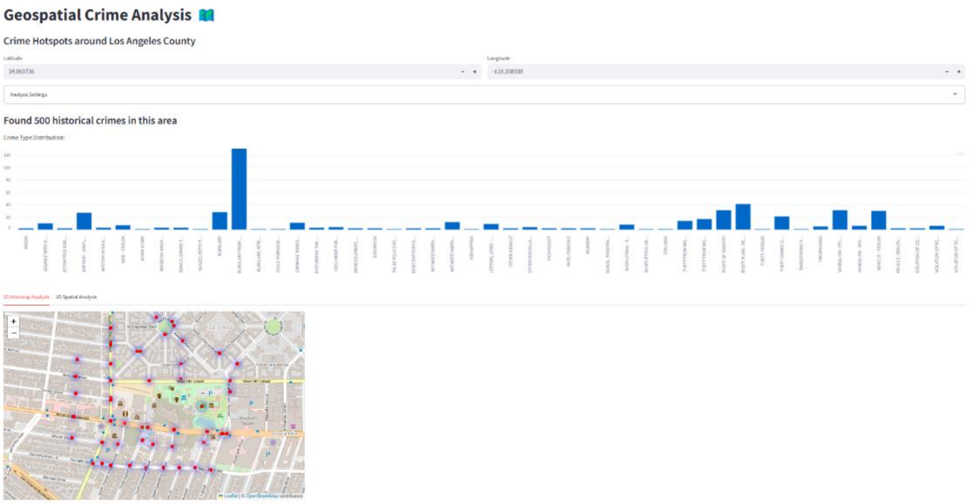
Geospatial Analysis

Location Details

name	type	full_address	city	state	country	latitude	longitude
Los Angeles County Train Station	meeting_point		Los Angeles	California	United States	None	None
Springfield, IL	landmark		Springfield	Illinois	United States	39.799999	-89.643997
Suspect Address	suspect_address		None	None	None	None	None
Victim Address	victim_address		None	None	None	None	None

Fig.7: Geographical Entity Plot (For various location entities)

This Fig.7 shows the Geographical encoding of the location using the location type entities and plotting in Open-Source service based OpenStreetMap using Streamlit Folium.



Geospatial Crime Analysis

Crime Hotspots around Los Angeles County

Latitude: 34.063736

Longitude: -118.358938

Analysis Settings

Found 500 historical crimes in this area

Crime Type Distribution:

Fig.8(a): 2D Heatmap For understanding the Severity Factors

The 2D heatmap, on the other hand, simplifies the KDE output into a color-coded overlay on a map, with warmer colors (red/orange) indicating higher crime density. Key factors influencing the heatmap include the bandwidth (adjusts smoothing), color gradient (enhances readability), and grid resolution (balances detail vs. performance). The heatmap provides a quick, intuitive overview of crime distribution, while the 3D KDE offers deeper spatial analysis. Together, these tools help users detect trends, allocate resources, and strategize interventions based on empirical density patterns as shown in Fig.8(a) and Fig.8(b).

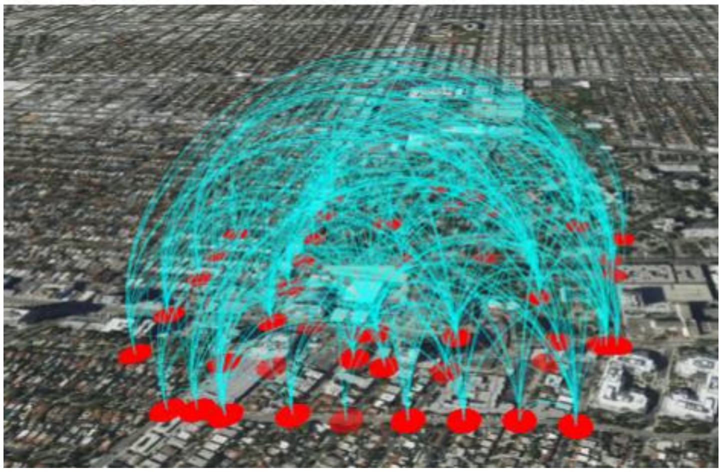


Fig.8(b): Kernel Density Estimation (Geo-Spatial arc Layer Analysis)

The KDE (Kernel Density Estimation) in the 3D geospatial stage of the app visualizes crime hotspots by creating a smoothed, volumetric density map. It transforms discrete crime locations into a continuous surface, where peaks represent high-density areas, making it easier to identify patterns. The 3D plot, likely generated using Plotly or Matplotlib, allows interactive exploration, such as rotating or zooming, to analyze crime concentrations from multiple angles. The bandwidth parameter controls the smoothing level—wider bandwidths merge nearby crimes into broader hotspots, while narrower ones highlight finer details. This helps investigators pinpoint critical zones efficiently.

V. CONCLUSION

The enhanced AI-based autonomous tool, designed for profile generation through Modus Operandi (MO) analysis and temporal/geospatial pattern recognition integrated with a scalable database infrastructure, enables dynamic threat detection, behavioral forecasting, and risk mitigation by synthesizing multi-dimensional data into actionable insights. By leveraging machine learning, real-time database connectivity, and advanced analytics, the system optimizes predictive accuracy, identifies emerging trends, and enhances operational efficiency across domains such as cybersecurity, law enforcement, and consumer behavior analysis, ensuring adaptive decision-making in complex, data-driven environments.

VI. REFERENCES

[1] Chainey, S., & Ratcliffe, J. (2013). *GIS and crime mapping*. John Wiley & Sons.
Source: Book published by Wiley.

[2] Wang, H., Kifer, D., & Li, Z. (2020). Crime incident forecasting with deep learning. *ACM Transactions on Spatial Algorithms and Systems, 6*(2), 1–29. https://doi.org/10.1145/3364221
Source: Peer-reviewed journal published by ACM.

[3] Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The elements of statistical learning: Data mining, inference, and prediction* (2nd ed.). Springer.
Source: Book published by Springer.

[4] IBM. (2020). *IBM Crime Prediction and Prevention Tool: Technical overview*. IBM Corporation.
Source: Technical report by IBM.

[5] Brantingham, P. J. (2018). *Predictive policing in Los Angeles: A review of the LAPD's operational initiatives*. UCLA.
Source: Report from University of California, Los Angeles (UCLA).

[6] Perry, W. L., McInnis, B., & Price, C. C. (2013). *Predictive policing: The role of crime forecasting in law enforcement*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR233.html
Source: Research report by RAND.

[7] Sureka, A., & Agarwal, S. (2016). Natural language processing for crime trend detection. In *2016 IEEE International Conference on Big Data* (pp. 2197–2204). IEEE. https://doi.org/10.1109/BigData.2016.7840821
Source: Conference proceedings published by IEEE.

[8] Eck, J. E., Chainey, S., Cameron, J., & Wilson, R. (2005). *Mapping crime: Understanding hot spots*. National Institute of Justice. https://www.ojp.gov/pdffiles1/nij/209393.pdf
Source: Government publication by the U.S. Department of Justice.

[9] Obe, R. O., & Hsu, L. S. (2021). *PostgreSQL: Up and running* (4th ed.). O'Reilly Media.
Source: Book published by O'Reilly.

[10] Shneiderman, B. (1996). The eyes have it: A task by data type taxonomy for information visualizations. In *Proceedings of the IEEE Symposium on Visual Languages* (pp. 336–343). IEEE. https://doi.org/10.1109/VL.1996.545307
Source: Conference proceedings by IEEE.

[11] Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration, 42*(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664
Source: Peer-reviewed journal article.

[12] Berk, R. (2021). Artificial intelligence, predictive policing, and risk assessment for criminal justice. *Annual Review of Criminology, 4*, 209–237. https://doi.org/10.1146/annurev-criminol-061020-021500
Source: Review article from Annual Reviews.

[13] Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.
Source: Book published by New York University Press.

[14] Hunt, P., Saunders, J., & Hollywood, J. S. (2014). *Evaluation of the Shreveport predictive policing experiment*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR531.html
Source: Evaluation report by RAND.

[15] Leitner, M. (Ed.). (2013). *Crime modeling and mapping using geospatial technologies*. Springer. https://doi.org/10.1007/978-94-007-4997-9
Source: Edited volume published by Springer.

[16] Venkat Sai. (2023). *Los Angeles Crime Data (2020–2023)* [Data set]. Kaggle. https://www.kaggle.com/datasets/venkatsairo4899/los-angeles-crime-data-2020-2023
Source: Dataset hosted on Kaggle.