Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap

Olha Mykhaylova[1], Taras Fedynyshyn[2], Volodymyr Sokolov[2], and Roman Kyrychok[2]

[1] *Lviv Polytechnic National University, 12 Stepan Bandera str., Lviv, 79000, Ukraine*
[2] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

The research problem addressed in the paper centers around the difficulty of identifying Persons of Interest (POIs) in law enforcement activity due to the vast amount of data stored on mobile devices. Given the complexity and volume of mobile forensic data, traditional analysis methods are often insufficient. The paper proposes leveraging Artificial Intelligence (AI) techniques, including machine learning and natural language processing, to improve the efficiency and effectiveness of data analysis in mobile forensics. This approach aims to overcome the limitations of manual data examination and enhance the identification process of POIs in a forensically sound manner. The main objective of the study is to explore and demonstrate the effectiveness of Artificial Intelligence techniques in improving the identification of POIs from mobile forensic data. The study proposes AI-driven approaches, particularly machine learning, and natural language processing, which can significantly enhance the efficiency, accuracy, and depth of analysis in mobile forensics, thereby addressing the challenges of handling vast amounts of data and the complexity of modern digital evidence. The study employs a quantitative research design, utilizing AI algorithms to process mobile forensic data from simulated environments. The study particularly demonstrates how deep learning can be utilized for searching POIs in WhatsApp messenger data. The result of the experiment shows that using AI for face recognition may throw false positive results, which means humans can't be replaced in the stage of AI evolution. Also, results emphasize that using AI is helpful in mobile forensics data analysis and followed 88% of successful face recognition. The findings underscore the transformative potential of AI in mobile forensics, highlighting its capacity to enhance investigative accuracy and efficiency. This advancement could lead to more effective law enforcement and judicial processes by enabling quicker identification of POIs with higher precision. Moreover, the research underscores the importance of addressing ethical and privacy concerns in the application of AI technologies in forensic investigations, suggesting a balanced approach to leverage AI benefits while safeguarding individual rights.

Keywords

Artificial intelligence, AI, deep learning, mobile forensics, person of interest, POI.

1. Introduction

In the ever-evolving landscape of digital forensics, the exponential growth of mobile devices has presented both unprecedented opportunities and challenges for law enforcement agencies, cybersecurity experts, and forensic investigators. As the volume of mobile data continues to soar, there is a pressing need for innovative methodologies that can efficiently analyze and interpret this vast repository of information. The emergence of Artificial Intelligence (AI) as a powerful tool in various domains has sparked a paradigm shift in

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine

EMAIL: olha.o.mykhailova@lpnu.ua (O. Mykhaylova); fedynyshyn.taras@gmail.com (T. Fedynyshyn); v.sokolov@kubg.edu.ua (V. Sokolov); r.kyrychok@kubg.edu.ua (R. Kyrychok)
ORCID: 0000-0002-3086-3160 (O. Mykhaylova); 0009-0006-8233-8057 (T. Fedynyshyn); 0000-0002-9349-7946 (V. Sokolov); 0000-0002-9919-9691 (R. Kyrychok)

the field of digital forensics, opening new avenues for enhancing investigative capabilities. This paper delves into the realm of Person-of-Interest (POI) detection within mobile forensics data and explores the transformative potential of AI-driven approaches in this context. The identification and tracking of individuals of interest play a crucial role in solving criminal cases, counterterrorism efforts, and ensuring public safety. Leveraging advanced AI techniques such as machine learning and deep learning, this research aims to harness the computational prowess of these technologies to extract meaningful insights from mobile device data, thereby streamlining the investigative process.

The investigation of mobile devices involves analyzing a plethora of data types, including call records, text messages, geolocation information, application usage patterns, and more [1]. Traditional methods often struggle to keep pace with the sheer volume and complexity of this data, necessitating a shift towards intelligent systems capable of discerning patterns, anomalies, and relevant connections that may elude manual analysis.

Through this paper, we aim to explore the theoretical foundations, methodological frameworks, and practical applications of AI-driven POI detection on mobile forensics data. By addressing the challenges associated with data volume, diversity, and evolving technologies, we seek to contribute to the ongoing dialogue surrounding the integration of AI into digital forensics practices. As the technological landscape continues to evolve, the fusion of AI and mobile forensics promises to be a game-changer, unlocking new dimensions in investigative capabilities and facilitating more efficient and accurate POI identification.

2. The Concept of Person-Of-Interest

The concept of a “suspicious individual” [2] or “Person of Interest” (POI) in the context of security, law enforcement, and forensics is multifaceted and can vary depending on the situation and the perspective of the observer. In general, it pertains to an individual suspected of displaying behaviors, traits, or engagements that deviate from the norm and could suggest a potential threat or participation in criminal or malicious activities. Yet, determining the criteria that render an individual “suspicious” is subjective and can be shaped by a multitude of factors:

- Behavioral indicators—in certain situations, particular behaviors might be viewed as suspicious. For instance, lingering in a restricted area, displaying an unusual focus on security measures, or making efforts to evade detection can trigger suspicion.
- Context and environment—the context significantly influences the assessment of suspicion. Conduct deemed normal in one environment may appear suspicious in another. For instance, carrying a backpack is commonplace in a university setting but might be regarded with suspicion in a high-security area.
- Historical or background information—individuals with a record of criminal activity or connections to known criminals may be deemed suspicious in specific investigations or situations.
- Anomalies in communication or transactions—within the realms of digital forensics and cybersecurity, deviations from typical patterns, such as uncommon financial transactions, encrypted communications in non-secure contexts, or irregular travel patterns, can raise suspicions about an individual.
- Physical indicators—specific physical manifestations may be considered suspicious, including wearing bulky clothing in warm weather (indicative of potential concealment), displaying nervous behavior, or avoiding eye contact at a security checkpoint.
- Data analysis—in the era of digital technology, tools for data analysis can pinpoint patterns indicative of suspicious behavior. This encompasses the examination of social media activity, financial transactions, or communication patterns.
- Risk assessment models—within the realms of security and counter-terrorism, models for risk assessment are employed to gauge the potential threat an individual might pose, considering various factors, including those mentioned above.

It is crucial to emphasize that categorizing an individual as “suspicious” or “person of interest” does not automatically imply guilt or involvement in illicit activities. This designation serves as an initial evaluation that may necessitate additional observation or investigation. The understanding of suspicion is highly context-dependent, underscoring the substantial responsibility to mitigate biases and ensure that assessments are grounded in objective and reasonable criteria.

3. Mobile Forensics Data Analysis

Contemporary methodologies and tools employed in mobile device forensics have significantly transformed the strategies adopted by investigators and legal professionals. Mobile devices often take center stage in investigations, and these innovative approaches offer enhanced capabilities for simultaneously analyzing numerous devices swiftly and efficiently. The evolving techniques also enable the incorporation of a broader spectrum of information from these devices. For over a decade, mobile devices have played a prominent role in disputes and investigations. The widespread integration of mobile devices for both business and personal purposes [3] has resulted in a trove of data that is more abundant and easily accessible than any other data source. This, combined with the high frequency of usage and users’ strong sense of privacy, renders mobile devices exceptionally valuable in any investigative analysis.

After obtaining the mobile device data, various tools can be employed for extraction and analysis. In straightforward cases with a limited set of devices and known issues, manual analysis using spreadsheets or traditional document review platforms may suffice. However, in more intricate situations, a comprehensive analysis approach utilizing data analysis techniques becomes essential. This approach encompasses the extraction of specific data types and the integration of data from multiple mobile devices into a unified database, facilitating consolidated analysis.

Subsequent phases, namely analysis and reporting, are more time-consuming and may necessitate multiple iterations along with potential additional data collection or adjustment of the analysis scope. The specific types of analyses employed can vary, but the overarching goal is to apply techniques grounded in facts to expedite the analysis process and diminish the time spent sifting through irrelevant data. The analysis phase entails multiple iterations, each adapting or refining the analysis based on insights gained from prior analyses. The review and production phase involves organizing the data into a visual and interactive platform, enabling reviewers to consolidate their findings and present them in the form of documents, metadata, and/or visual representations.

The analysis of mobile devices presents ample opportunities to concurrently examine various data types and devices. Utilizing advanced tools like artificial intelligence and machine learning empowers investigators and legal teams to conduct these analyses more swiftly and comprehensively than traditional document review tools would allow. The essential elements for a successful mobile phone analysis lie in accurately scoping the objectives and known facts of a case and subsequently conducting a systematic and thorough analysis of the data.

4. Related Work

Artificial intelligence usage in forensic data analysis and law enforcement becomes more widespread in the era of the industrial revolution 4.0 where the world is entering.

One of the pioneering examples is face cognitions in surveillance systems. Tang et al. [4] (2004) propose to transform a photo image into a sketch which reduces the difference between photo and sketch significantly, thus allowing effective matching between the two. Zafar et al. [5] (2019) propose to use of deep convolutional neural networks and a method to improve the efficacy of face recognition systems by dealing with false positives through employing model uncertainty for face recognition for robust surveillance systems. Awais et al. [6] (2019) suggest using a histogram of oriented gradient features and a feedforward neural network classifier to improve real-time surveillance performance. Researchers in [7–9] also propose different methods and algorithms related to face recognition in surveillance.

Han et al. [10] (2018) propose a method to track and recognize tattoos on human bodies in images from surveillance pictures for POI detection and social media search.

Boger and Ozer [11] 2023 propose a theoretical framework for using eDNA detection devices to locate missing persons, wanted criminals, and persons of interest in densely populated areas by monitoring sewer water. The proposed system includes a computer application to enter information on missing targets, and the data collected by the system can be used to narrow down their location for rescue or apprehension.

Sachoulidou in [12] 2023 explores the trend of increasing automation in law enforcement and criminal justice settings through three use cases: predictive policing, machine evidence, and recidivism algorithms. The focus lies on artificial-intelligence-driven tools and technologies employed, whether at pre-investigation stages or within criminal proceedings, to decode human behavior and facilitate decision-making as to whom to investigate, arrest, prosecute, and eventually punish. In this context, this article first underlines the existence of a persistent dilemma between the goal of increasing the operational efficiency of police and judicial authorities and that of safeguarding the fundamental rights of the affected individuals.

Authors of [13] describe technology domains where AI is relevant in law enforcement activities, including audio processing, visual processing, resource optimization, and natural language processing. Also provide use cases from law enforcement agencies, including non-intrusive surveillance Systems in Norway, data airlock and harmful materials recognition in Australia, recommender system in Germany, and major events screening, surveillance, and beyond in Japan.

Authors in [14] explore the impact of AI deployment in law enforcement on the exercise of citizens' fundamental rights by contrasting the anticipated promises and policy objectives with the actual practices, funded projects, and operational realities within law enforcement.

5. Fields of Artificial Intelligence

AI refers to the emulation of human thought processes in a computerized model. AI encompasses self-learning systems that employ techniques such as data mining, pattern recognition, and natural language processing to replicate the cognitive functions of the human brain [15].

Operating at scale, reasoning with purpose, and engaging in natural interactions with humans, these systems play a crucial role in decision-making improvement, akin to how search enhances information retrieval. In essence, AI serves to facilitate human experts in making more informed decisions. We define AI by four key attributes:

1. Understands—AI achieves a profound comprehension of its domain primarily by processing diverse forms of data, whether structured or unstructured, text-based or sensory. This occurs within the context and meaning of the information while handling large volumes of data swiftly.
2. Reasons—AI engages in reasoning towards defined objectives, demonstrating the capacity to generate hypotheses through thoughtful arguments and provide prioritized recommendations. These capabilities contribute to assisting humans in making improved decisions.
3. Learns—AI undergoes continuous learning from experience, constantly ingesting and accumulating data and insights from every interaction. It is not programmed but trained by experts who enhance, scale, and expedite their expertise, leading to a continuous improvement of these systems over time.
4. Interacts—AI seamlessly engages with individuals and systems, aiming for an interaction model that flows smoothly while steadily cultivating a sustainable relationship between the AI and its users.

In the next subchapters, we describe some of the artificial intelligence fields that may be valuable in the process of POI detection.

5.1. Computer Vision

Computer vision, within the realm of AI, empowers computers and systems to extract meaningful information from digital images, videos, and other visual inputs. It facilitates the capability to take actions or provide recommendations based on the interpreted visual information. While AI enables computers to think, computer vision empowers them to see, observe, and comprehend visual data [16].

Computer vision operates similarly to human vision, although humans have a head start in this regard. Human sight benefits from a lifetime of context, enabling individuals to learn how to distinguish objects, assess distances, detect movement, and identify abnormalities within an image.

Computer vision teaches machines to execute these tasks, but it does so within a significantly shorter timeframe, utilizing cameras, data, and algorithms instead of relying on retinas, optic nerves, and visual cortex. Systems trained to inspect products or monitor production assets can analyze thousands of items or processes per minute, swiftly identifying imperceptible defects or issues and thereby surpassing human capabilities.

Computer vision relies heavily on extensive data. It repeatedly analyzes data until it can discern distinctions and ultimately recognize images. For instance, training a computer to identify automobile tires, requires a substantial amount of tire images and related items to learn the differences and accurately recognize a tire, particularly one without defects.

Two crucial technologies employed for this purpose are a form of machine learning known as deep learning and a Convolutional Neural Network (CNN).

Machine learning employs algorithmic models, allowing a computer to autonomously grasp the context of visual data. With a sufficient amount of data input into the model, the computer can "look" at the data and independently learn to distinguish one image from another. Algorithms facilitate self-learning in the machine, eliminating the need for explicit programming to recognize images.

A CNN aids a machine learning or deep learning model in the process of "looking" by dissecting images into pixels with assigned tags or labels. Utilizing these labels, the CNN performs convolutions—a mathematical operation on two functions to generate a third function—and generates predictions about what it perceives. Through a series of iterations, the neural network conducts convolutions and assesses the accuracy of its predictions until they align with the actual content. At this point, the network starts recognizing or "seeing" images in a manner akin to human perception.

Similar to a human discerning an image from a distance, a CNN initially identifies hard edges and basic shapes. It then refines its understanding through iterations of predictions, gradually filling in additional details. CNNs are employed for comprehending individual images. Conversely, a Recurrent Neural Network (RNN) serves a similar purpose in video applications, assisting computers in understanding the relationships between images across a sequence of frames.

5.2. Natural Language Processing

Natural Language Processing (NLP) is a machine-learning technology that empowers computers to interpret, manipulate, and understand human language [17]. In contemporary organizations, extensive voice and text data is generated through diverse communication channels such as emails, text messages, social media feeds, video, audio, and more. NLP software is employed to automatically process this data, analyze the intent or sentiment conveyed in the messages, and provide real-time responses to human communication [18–20].

Natural Language Processing (NLP) integrates computational linguistics, machine learning, and deep learning models to handle human language.

Computational linguistics is the scientific discipline focused on comprehending and building human language models using computers and software tools. Researchers employ methods in computational linguistics, including syntactic and semantic analysis, to establish frameworks that enable machines to grasp conversational human language. Tools such as language translators, text-to-speech synthesizers, and speech recognition software are rooted in computational linguistics.

Machine learning is a technology that enhances a computer's efficiency by training it with sample data. Human language, characterized by features like sarcasm, metaphors, variations in sentence structure, as well as grammar and usage exceptions, requires years for humans to fully grasp. Programmers employ machine learning methods to instruct NLP applications in recognizing and accurately understanding these linguistic features from the outset.

Deep learning is a distinct subset of machine learning that instructs computers to emulate human learning and thought processes. It employs a neural network comprising data processing nodes organized to mimic the structure of the human brain. Through deep learning, computers can identify, categorize, and establish correlations within intricate patterns present in the input data.

NLP techniques, also known as NLP tasks, deconstruct human text or speech into smaller components that computer programs can comprehend effortlessly. The following are common text processing and analyzing capabilities in NLP:

- Part-f-speech tagging—this process involves NLP software assigning tags to individual words within a sentence based on their contextual usage, such as identifying nouns, verbs, adjectives, or adverbs. This tagging assists the computer in comprehending how words establish meaningful relationships with one another.
- Word-sense disambiguation—certain words can have varied meanings depending on the context in which they are used. For instance, the word "bat" carries different meanings in the following sentences: a) A bat is a nocturnal creature. b) Baseball players use a bat to hit the ball. With word sense disambiguation, NLP software discerns the intended meaning of a word, achieved through training its language model or referencing dictionary definitions.
- Machine translation—utilizing natural language processing, machine translation software transforms text or speech from one language to another while preserving contextual accuracy.

Named identity recognition—this procedure identifies distinct names associated with individuals, locations, events, companies, and other entities. Named-entity recognition in NLP software is employed to establish relationships between different entities within a sentence.

5.3. Audio Processing

Fundamentally, Audio AI operates through a process called feature extraction. This entails transforming raw audio input into a set of features or data points that are amenable to analysis [21].

The initial step involves breaking down the raw audio into smaller, more manageable segments, typically lasting a few milliseconds each. This process, often referred to as windowing, is crucial for capturing the swift fluctuations in sound waves. Subsequently, the algorithm extracts valuable information from these audio frames, transforming them into a suitable format for analysis.

Following this, the extracted features are fed into a machine-learning model. Trained on an extensive amount of audio data, this model learns to recognize patterns and correlations between the features and the corresponding sound events. When presented with new audio input, the model applies its acquired knowledge to predict the present sounds.

Ultimately, the output from the AI model undergoes post-processing. This may include refining the output, aggregating predictions over time to reach a conclusive decision, or conducting additional analysis based on the specific application of Audio AI.

5.4. Expert Systems

An expert system is a computer system that emulates the decision-making capabilities of a human expert. These systems are designed to address complex problems by reasoning through bodies of knowledge, primarily represented as if–then rules rather than conventional procedural code. The inception of expert systems dates back to the 1970s and experienced widespread development in the 1980s. Expert systems marked one of the initial triumphs in AI software. This system is bifurcated into two subsystems: the inference engine and the knowledge base. The knowledge base encompasses facts and rules, while the inference engine applies these rules to known facts, deducing new information.

Inference engines may also incorporate explanation and debugging functionalities.

An expert system exemplifies [22] a knowledge-based system, marking the early adoption of a knowledge-based architecture in commercial systems. Typically, an expert system consists of several components, including a knowledge base, an inference engine, an explanation facility, a knowledge acquisition facility, and a user interface [23].

The knowledge base serves to encapsulate facts about the world. In the initial expert systems like Mycin and Dendral, these facts were predominantly expressed as flat assertions regarding variables. In subsequent expert systems developed with commercial shells, the knowledge base evolved to possess more structure, incorporating concepts from object-oriented programming. The representation of the world shifted to classes, subclasses, and instances, replacing assertions with values of object instances. The rules are operated by querying and asserting the values of these objects [24].

6. AI Applications in POI Detection

This section describes categories of information that can be found in mobile device forensics data and could be used in person-of-interest identification and searching. The main idea is—utilizing AI in mobile forensics data analysis brings additional knowledge about mobile device users. And that knowledge could obtained automatically or semi-automatically.

6.1. Identity Documents Detection

An identity document (ID document) is any document that can be used to confirm its owner's person and to prove their identity. Among the document fields, it has to contain various details about the person. The most common is the person's full name, birth date, address, identification number, gender, photo, and an image of the personal signature [25].

A person may store photos of identity documents in their mobile phone gallery. In some cases, those photos of documents may be used to identify a person in the law enforcement process. Another case is when a person stores photos of documents of other people. Law enforcement may interpret this action as a potential infringement on privacy rights, unauthorized possession of personal information, or even identity theft, depending on the circumstances and intent.

Automatic identity document recognition could be very useful in person-of-interest identification. It could also be utilized in counter-terrorism and counter-intelligence actions.

6.2. People Faces Recognition

Another important part of mobile forensics data analysis is face recognition. Faces can be found on the device gallery photos and videos, and on the messenger avatars, photos with faces can be sent via messengers or email. Faces could be compared with different databases. For example, police/special services wanted lists, lists of disappeared persons, lists of people under sanctions, etc. The fact that some disappeared person is present in some other person's mobile phone gallery or messenger could mean nothing, it could be a relative or friend of disappeared. But, if a photo of a disappeared or kidnapped [26] person is found in some random person device—the person becomes a POI and requires further investigation and checks.

6.3. Vehicle Plates Recognition

Automated license plate recognition is being used in almost all countries for everyday life, for example for law enforcement, traffic control, access to restricted areas, E-Tolls, or checking in parking areas [27].

Plate recognition could bring some additional value being applied in mobile device forensics data analysis. Its application could help to find stolen vehicles, or vehicles involved in some cases that law enforcement could work on.

6.4. Banking/Financial Data Recognition

Banking and financial data are crucial in law enforcement and person of interest detection for several reasons:

- Financial Crimes Investigation—banking and financial data are instrumental in investigating financial crimes such as fraud, money laundering, embezzlement, and other illicit activities [28]. Transactions and account information provide insights into potential illegal financial activities.

- Tracking Funds—law enforcement relies on banking data to trace the flow of funds, helping them follow the money trail in criminal investigations. This is particularly important in cases involving organized crime, drug trafficking, terrorism, and other serious offenses.
- Intelligence Gathering—financial data is a valuable source of intelligence for law enforcement agencies [29]. Analyzing financial records can reveal connections between individuals, organizations, and criminal networks, aiding in the gathering of intelligence for broader investigations.
- Asset Forfeiture—in cases where criminal activities result in financial gains, law enforcement may use financial data to trace and seize assets obtained through illegal means. Asset forfeiture is a legal process that involves confiscating assets acquired through criminal activities.

National Security—financial data is critical for national security efforts, as it can reveal funding sources for terrorist organizations and other threats to a country's security.

6.5. Tickets Recognition

Ticket recognition is important in law enforcement and person of interest detection. Tickets, especially related to transportation modes like airlines, trains, or buses, provide a record of an individual's travel history. This information can be used to establish timelines, track movements, and identify locations associated with a person of interest.

Tickets may help to identify connections. Analyzing ticket data can help law enforcement identify connections between individuals. Persons of interest might be associated with each other through shared travel patterns, common destinations, or simultaneous visits to specific locations. In cases involving missing persons, especially minors, ticket data can be used to track their movements and assist in locating them. This is particularly relevant in Amber Alerts and other emergencies.

Ticket data is valuable for border and national security and immigration control. Authorities can use this information to monitor individuals crossing third-country borders, identify persons of interest, or track those involved in illegal activities.

6.6. Named Entity Recognition

Named Entity Recognition (NER) helps in identifying and extracting information about specific individuals mentioned in mobile data, such as contacts, text messages, or call logs [30]. This is valuable for investigations related to criminal activities, missing persons, or threats to national security. Also, NER assists in recognizing and extracting location-related entities, such as addresses or geographic coordinates, from mobile data [31]. This is essential for tracking the movement of individuals or understanding the locations associated with specific events. For cases involving financial crimes or fraud, NER can be used to identify entities related to financial transactions, account details, or monetary amounts within mobile data.

In mobile forensics, NER enhances the efficiency of investigators by automating the identification and extraction of critical information from diverse data sources on mobile devices. It contributes to a more thorough and accurate analysis, helping law enforcement agencies in solving cases and ensuring the proper handling of digital evidence.

6.7. Word/PDF/Other Documents Summarization and Search

Mobile devices often contain a vast amount of text data, including messages, emails, documents, and notes. Summarization helps in condensing lengthy documents, allowing investigators to focus on the most relevant information efficiently. Summarization tools can automatically generate concise summaries, reducing the workload for forensic analysts. This is particularly valuable when dealing with large datasets, enabling investigators to sift through information more effectively.

Summarization tools can reveal patterns or trends in the data by highlighting recurring themes, topics, or language used in various

documents. This aids investigators in identifying patterns of communication or behavior [32].
Summarization can assist in ensuring that investigators focus on legally and ethically permissible information, avoiding unnecessary intrusion into individuals' privacy.

6.8. Voice Recognition

Voice recognition helps in identifying speakers based on their unique vocal characteristics. This can be crucial in cases where the origin of a voice message or conversation needs to be established.

Analyzing voice data helps investigators understand communication patterns, frequency of calls, and relationships between individuals. This information can be crucial in cases involving conspiracies, threats, or illicit activities.

As with faces—a person's voice can be found on the device gallery videos or voice memos, on the messengers or email. The voice could be compared with different databases. For example, police/special services wanted lists, lists of disappeared persons, lists of people under sanctions, etc. The fact that some disappeared person's voice is present in some other person's mobile phone gallery or messenger could mean nothing, it could be a relative or friend of the disappeared. But, if the voice of a disappeared or kidnapped person is found in some random person's device—the person becomes a POI and requires further investigation and checks.

7. Case study—Applying Deep Learning for Searching POIs in WhatsApp Messenger Data

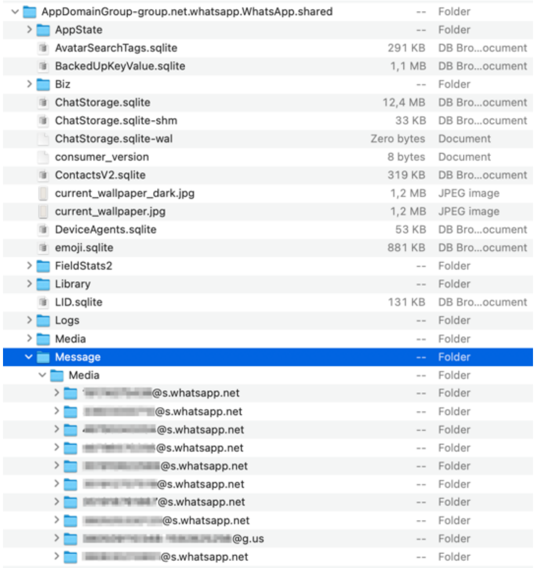
This section describes an experiment conducted using mobile forensic data—WhatsApp application data in this case and face recognition technology to identify if persons listed in wanted lists could be found.

7.1. Experiment Preparation

To conduct the experiment the following preparation steps were done:

1. Photos and names from the Security Service of Ukraine's wanted list were parsed (Fig. 1)—355 photos total.
2. For some persons from the SSU-wanted list [33] additional photos were found [34] and downloaded—27 photos total.
3. Those additional photos were sent via WhatsApp messenger from an iPhone device.
4. iPhone device backup was captured using iMazing software ("Export raw files" option).

Figure 1: Example of faces from SSU wanted list used in the experiment



AppDomainGroup-group.net.whatsapp.WhatsApp.shared	--	Folder
AppState	--	Folder
AvatarSearchTags.sqlite	291 KB	DB Bro...ocument
BackedUpKeyValue.sqlite	1,1 MB	DB Bro...ocument
Biz	--	Folder
ChatStorage.sqlite	12,4 MB	DB Bro...ocument
ChatStorage.sqlite-shm	33 KB	DB Bro...ocument
ChatStorage.sqlite-wal	Zero bytes	Document
consumer_version	8 bytes	Document
ContactsV2.sqlite	319 KB	DB Bro...ocument
current_wallpaper_dark.jpg	1,2 MB	JPEG image
current_wallpaper.jpg	1,2 MB	JPEG image
DeviceAgents.sqlite	53 KB	DB Bro...ocument
emoji.sqlite	881 KB	DB Bro...ocument
FieldStats2	--	Folder
Library	--	Folder
LID.sqlite	131 KB	DB Bro...ocument
Logs	--	Folder
Media	--	Folder
Message	--	Folder
Media	--	Folder
[redacted]@s.whatsapp.net	--	Folder
[redacted]@s.whatsapp.net	--	Folder
[redacted]@s.whatsapp.net	--	Folder
[redacted]@s.whatsapp.net	--	Folder
[redacted]@s.whatsapp.net	--	Folder
[redacted]@s.whatsapp.net	--	Folder
[redacted]@s.whatsapp.net	--	Folder
[redacted]@s.whatsapp.net	--	Folder
[redacted]@g.us	--	Folder
[redacted]@s.whatsapp.net	--	Folder

Figure 2: WhatsApp application raw data structure

7.2. Experiment Theoretical Base

AI part of the experiment is run by dlib [35] C++ library wrapped in the Python package face_recognition [36].

Dlib is a modern [35] C++ toolkit containing machine learning algorithms and tools for creating complex software in C++ to solve real-world problems. It is used in both industry and academia in a wide range of domains including robotics, embedded devices, mobile phones, and large high-performance computing environments. Dlib is a general-purpose cross-platform software library written in the programming language C++. Its design is heavily influenced by ideas from design by contract and component-based software engineering. Thus it is, first and foremost, a set of independent software components. It is open-source software released under a Boost Software License.

The library implements numerous machine learning algorithms, including SVMs, K-Means clustering, Bayesian Networks, and others.

7.3. Experiment Execution

To execute the experiment a Python script was written. The script implemented the sequence of the following steps:

1. Process each SSU-wanted list photo and extract encoding—a 128-dimensional vector of floating numbers using.
2. Process the WhatsApp application directory and extract encoding for each photo in the Message folder and subfolders.
3. For each photo found on the WhatsApp folder calculate the distances between the face on this photo and each face in the SSU-wanted list.
4. Order each distance list ascending by distance and remove all items except the first.
5. Save results in a file.

Check manually what number of photos sent via WhatsApp were found in the SSU wanted list.

7.4. Experiment Result

As a result of experimenting—24 of 27 (88%) persons whose photos were sent via WhatsApp were recognized in the SSU wanted list. Figs. 3–4 show faces that were successfully recognized. Fig. 5 shows faces that were recognized with error.

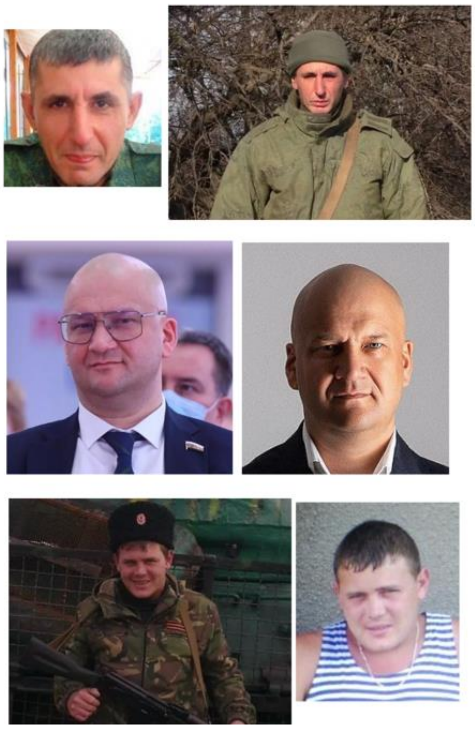


Figure 3: Example #1 of successful face recognition

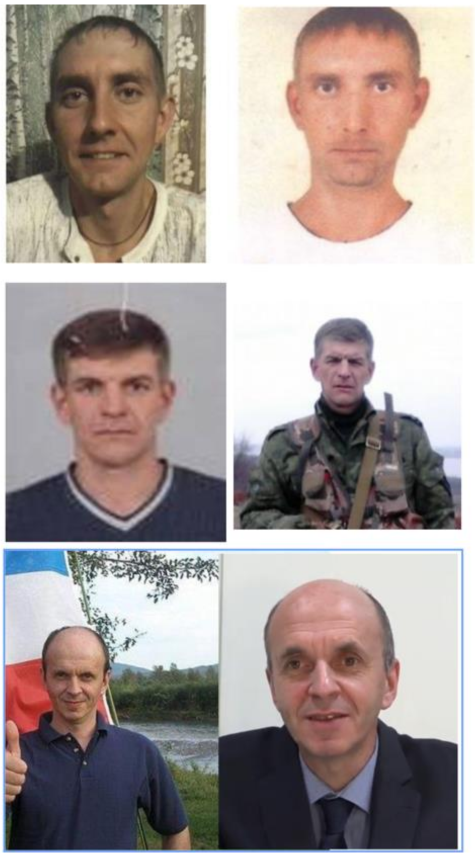


Figure 4: Example #2 of successful face recognition

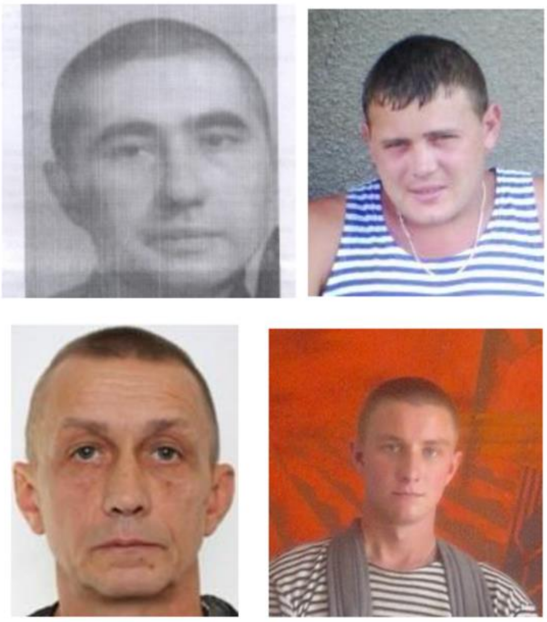


Figure 5: Example of unsuccessful face recognition

8. Conclusions and Future Directions

Applying AI to mobile forensic data analysis, particularly in the context of searching for persons of interest, presents a promising and dynamic direction for research. The integration of AI technologies in mobile forensics holds the potential to revolutionize the efficiency, accuracy, and depth of investigations. By leveraging machine learning, natural language processing, and other AI techniques, researchers can enhance the capabilities of forensic analysts in identifying and extracting critical information from vast and complex datasets on mobile devices.

The significance of this research direction lies in its capacity to address the evolving landscape of digital crimes and security threats [37]. The prevalence of mobile devices as primary communication tools underscores the need for advanced methodologies to analyze diverse data sources effectively. AI-powered tools can assist in automating repetitive tasks, expediting the identification of patterns, and offering valuable insights into the behavior and connections of persons of interest.

Moreover, AI-driven mobile forensic data analysis contributes to the development of proactive and preventive measures. By efficiently processing and interpreting large volumes of data, these systems can aid law enforcement in early detection, prediction, and intervention, ultimately contributing to the enhancement of public safety.

However, as we delve into this direction, it is crucial to address ethical considerations, privacy concerns, and the legal implications surrounding the use of AI in forensics. Striking a balance between technological advancements and safeguarding individual rights is imperative to ensure the responsible and ethical deployment of AI tools in the pursuit of justice.

In summary, the application of AI to mobile forensic data analysis for searching persons of interest emerges as a forward-looking and transformative avenue for research. This interdisciplinary approach, blending cutting-edge technologies with forensic methodologies, has the potential to shape the future of digital investigations, providing law enforcement agencies with powerful tools to navigate the complexities of the digital age.

References

[1] Y. Sadykov, et al., Technology of Location Hiding by Spoofing the Mobile Operator IP Address, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 22–25. doi: 10.1109/UkrMiCo52950.2021.9716700.

[2] T. Fedynyshyn, O. Mykhaylova, I. Opirskyy, 2023, Method TO Detect Suspicious Individuals Through Mobile Device Data, Ukrainian Sci. J. Inf. Secur. doi: 10.18372/2225-5036.29.18075.

[3] J. Sremack, Forensic Data Analysis of Mobile Devices: A Primer (2023). URL: https://www.kroll.com/en/insights/publications/forensic-data-analysis-of-mobile-devices.

[4] X. Tang, X. Wang, Face Sketch Recognition, IEEE Transactions on Circuits and Systems for Video Technology 14(1) (2004) 50–57. doi: 10.1109/TCSVT.2003.818353.

[5] U. Zafar, et al., Face Recognition with Bayesian Convolutional Networks for Robust Surveillance Systems, J Image Video Proc. 10 (2019). doi: 10.1186/s13640-019-0406-y.

[6] M. Awais et al., Real-Time Surveillance Through Face Recognition Using HOG and Feedforward Neural Networks, IEEE Access 7 (2019) 121236–121244. doi: 10.1109/ACCESS.2019.2937810.

[7] R. Melnyk, R. Kvit, T. Salo, Face Image Profiles Features Extraction for Recognition Systems, Scientific Bulletin of UNFU 31(1) (2021) 117–121. doi: 10.36930/40310120.

[8] E. Jose, et al., Face Recognition Based Surveillance System Using FaceNet and MTCNN on Jetson TX2, 5th International Conference on Advanced Computing & Communication Systems (ICACCS), (2019) 608–613. doi: 10.1109/ICACCS.2019.8728466.

[9] D. Chawla, M. Trivedi, Face Recognition under Partial Occlusion for Security Surveillance Using Machine Learning (2019).

[10] H. Han, et a., Tattoo Image Search at Scale: Joint Detection and Compact Representation Learning, IEEE Transactions on Pattern Analysis and Machine Intelligence 41(10) (2019) 2333–2348. doi: 10.1109/TPAMI.2019.2891584.

[11] N. Boger, M. Ozer, Monitoring Sewer Systems to Detect the eDNA of Missing Persons and Persons of Interest, Forensic Sci. Int. 349 (2023) 111744, doi: 10.1016/j.forsciint.2023.111744.

[12] A. Sachoulidou, Going Beyond the “Common Suspects:” to be Presumed Innocent in the Era of Algorithms, Big Data and Artificial Intelligence, Artif. Intell. Law. (2023). doi: 10.1007/s10506-023-09347-w.

[13] Towards Responsible AI Innovation Second Interpol-Unicri Report On Artificial Intelligence for Law Enforcement (2020). URL: https://www.interpol.int/content/download/15290/file/AI%20Report%20INTERPOL%20UNICRI.pdf.

[14] B. Sanz-Urquijo, E. Fosch-Villaronga, M. Lopez-Belloso, The Disconnect Between the Goals of Trustworthy AI for Law Enforcement and the EU Research Agenda, AI Ethics 3 (2023) 1283–1294. doi: 10.1007/s43681-022-00235-8.

[15] IBM, Design for AI, Fundamentals (2022). URL: https://www.ibm.com/design/ai/fundamentals/

[16] IBM, What is computer vision? (2022). URL: https://www.ibm.com/topics/computer-vision

[17] AWS, What is Natural Language Processing (NLP)? (2024). URL: https://aws.amazon.com/what-is/nlp/

[18] I. Iosifov, et al., Natural Language Technology to Ensure the Safety of Speech Information, in: Workshop on Cybersecurity Providing in In-formation and Telecommunication Systems, vol. 3187, no. 1 (2022) 216–226.

[19] O. Iosifova, et al., Analysis of Automatic Speech Recognition Methods, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 252–257.

[20] O. Iosifova, et al., Techniques Comparison for Natural Language Processing, in: 2nd International Workshop on Modern Machine Learning Technologies and Data Science, vol. 2631, no. I (2020) 57–67.

[21] How Does Audio AI Work? (A guide for beginners) (2024). URL: https://engineeryoursound.com/how-does-audio-ai-work-a-guide-for-beginners/

[22] Expert System. (2024). URL: https://en.wikipedia.org/wiki/Expert_system

[23] A. Lea, Digitizing Diagnosis: Medicine, Minds, and Machines in Twentieth-Century America, Johns Hopkins University Press. (2023) 1–256.

[24] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/picst54195.2021.9772181.

[25] A. Adawadkar, N. Kulkarni, Cyber-Security and Reinforcement Learning—A Brief Survey, Eng. Appl. Artificial Intell. 114 (2022) doi: 10.1016/j.engappai.2022.105116.

[26] J. Alsayaydeh, et al., Face Recognition System Design and Implementation using Neural Networks, Int. J. Adv. Comput. Sci. Appl. (IJACSA) 13(6) (2022). doi: 10.14569/IJACSA.2022.0130663.

[27] U. Salimah, V. Maharani, R. Nursyanti, Automatic License Plate Recognition Using Optical Character Recognition, IOP Conf. Ser.: Mater. Sci. Eng. 1115 (2021). doi: 10.1088/1757-899X/1115/1/012023.

[28] S. Sukardi, Reconstruction of Financial Crime Investigation Methods in Law Enforcement in The Era of the Industrial Revolution 4.0., Unnes Law J. 8(1) (2022) 133–158. doi: 10.15294/ulj.v8i1.53059.

[29] P. Lagerwaard, M. de Goede, In Trust We Share: The Politics of Financial Intelligence Sharing, Economy and Society 52(2) (2023) 1–25. doi: 10.1080/03085147.2023.2175451.

[30] F. Rodrigues, et al., Natural Language Processing Applied to Forensics Information Extraction with Transformers and Graph Visualization, IEEE Transactions on Computational Social Systems, doi: 10.1109/TCSS.2022.3159677.

[31] H. Studiawan, M. Hasan and B. Pratomo, Rule-based Entity Recognition for Forensic Timeline, Conference on Information Communications Technology and Society (ICTAS) (2023) 1–6. doi: 10.1109/ICTAS56421.2023.10082742.

[32] G. Dagher, B. Fung, Subject-based Semantic Document Clustering for Digital Forensic Investigations, Data & Knowledge Eng. 86 (2013) 224–241. doi: 10.1016/j.datak.2013.03.005.

[33] Security Service of Ukraine, Wanted Persons. URL: https://ssu.gov.ua/u-rozshuku

[34] Non-government Center for Research of Elements of Crimes against the National Security of Ukraine, Peace, Humanity, and the International Law Information for law Enforcement Authorities and Special Services About Pro-Russian Terrorists, Separatists, Mercenaries, War Criminals, and Murderers. URL: https://myrotvorets.center/

[35] D. King, dlib. Version 19.22, dlib.net (2022). URL: https://dlib.net

[36] A. Geitgey, face_recognition (Version 1.3.0) [Software]. (2023). URL: https://github.com/ageitgey/face_recognition

[37] D. Shevchuk, et al., Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 217–225.