**Software solutions to identify users behind Telegram, WhatsApp and Instagram based drug trafficking**

Karagana Ganga Raju  
*Computer Science and Engineering   
GMR Institute of Technology*Rajam, India  
karaganagangaraju2005@gmail.com

**Abstract:**

The increasing prevalence of drug trafficking activities on encrypted messaging apps like Telegram and social media platforms such as Instagram and WhatsApp is a growing concern worldwide. Drug dealers are exploiting the anonymity and reach of these digital channels to advertise and sell dangerous synthetic drugs like MDMA, LSD, and Mephedrone. They create dedicated channels, bots, and handles to directly connect with buyers, circumventing traditional drug markets. This research paper aims to develop innovative software solutions capable of identifying and monitoring live Telegram channels, WhatsApp groups, and Instagram accounts involved in drug sales. By leveraging advanced data analytics and machine learning techniques, the proposed system will triangulate identifiable parameters like IP addresses, mobile numbers, and email IDs associated with the users behind these illicit activities. The study underscores the urgent need for collaborative efforts between technology experts and law enforcement agencies to combat the misuse of social media and messaging apps for drug trafficking. Findings from this research can contribute to the development of effective strategies to disrupt online drug supply networks and ensure safer communities

**Keywords:**

*Encrypted Messaging Apps, Drug Trafficking, Telegram Channels, WhatsApp Bots, Instagram Handles, Software Solutions, User Identification, Real-Time Monitoring*

**Introduction:**

The rise of encrypted messaging platforms such as Telegram, WhatsApp, and social media sites like

Instagram has introduced significant challenges in the fight against drug trafficking. These platforms, designed to enhance user privacy and facilitate global communication, have unfortunately been exploited by criminal networks. End-to-end encryption, secure messaging, and anonymous interactions make it difficult for law enforcement agencies to track the individuals behind drug-related activities. The anonymity these platforms provide, combined with encrypted .communication, poses considerable obstacles for traditional investigation techniques.

Telegram’s secret chat feature and large group functionalities allow drug dealers to operate relatively freely, while WhatsApp’s massive user base and encryption enable private, hidden transactions. Instagram, primarily a social networking platform, is used for marketing illicit substances, often masked through codewords, emojis, or visual content. These platforms offer drug traffickers ways to operate across borders, making it a global issue that requires cutting-edge technological intervention.

To counter these challenges, advanced software solutions leveraging machine learning (ML), natural language processing (NLP), image recognition, and network analysis have been developed. These technologies allow for the identification of suspicious behavior, keyword detection, and even the analysis of visual content associated with drug trafficking. Additionally, cybersecurity and digital forensics play a crucial role in data extraction, analyzing metadata, and tracing activity patterns despite encryption.

This paper will explore existing software solutions aimed at identifying drug traffickers across Telegram, WhatsApp, and Instagram, evaluating their effectiveness and potential limitations.

**Literature Survey:**

[1].Alves et al. targets the need for automated key phrase extraction to identify a drug dealing and grooming crime from large-scale chat logs. Communication on encrypted platforms continues to rapidly increase, making impossible the tasks of manually analyzing millions of messages. Earlier techniques in this field have depended mainly on shallow linguistic analysis or simple keyword lookup. However, traditional methods of keyphrase extraction are quite limited when there are large volumes of unstructured data or complex linguistic patterns. To fill this gap, the authors use machine learning techniques to automatically identify important keyphrases from chat logs. As discussed in related works, existing research into relevant information identification has exploited NLP techniques, but there is not much exploration into linguistic approaches combined with machine learning for forensic purposes. Their approach significantly improves over older approaches as it better improves the accuracy and scalability of key phrase extraction applicable to forensic analysis.

[2].Here, deep multimodal, multilabel learning is employed by Hu et al. in examining how the scourge of drug trafficking is being routed on Instagram. Most of the previous literature had depended largely on analyzing singular modes of data, either text or images alone, for the detection of illegal activities. However, since social media applications like Instagram combine both text and images in form of captions and images, respectively, multiple data types need to be integrated in order to capture illicit activities effectively. The authors claim that compared to previous works that relied on simple machine learning algorithms or keyword-based searches, their approach uses deep learning to fuse text and image data for a more accurate detection. This multimodal approach removes the shortcomings of isolation of data by observing the overall scene. The literature also identifies the requirement for deep learning approaches to improve classification and detection tasks related to illicit activities, making this paper unique because it exactly does that: implement such methodologies on a real-world, high-traffic platform like Instagram.

[3].This paper gives an overview of mobile forensic techniques in analyzing drug trafficking on WhatsApp, especially applying the NIST method to WhatsApp. Of course, the quite popular platform is one of the problems; though research had shown earlier that it is rather too difficult once communications are encrypted to retrieve data meaningfully for any meaningful forensic analysis. The authors further note that the usage of mobile forensics has become increasingly vital in combating drug trafficking, pointing to earlier studies that have made use of simple methods like extracting data manually and by recognizing patterns. All these methods, however, were criticized based on their incapacity to process large amounts of data or even encrypted content. Here, the authors have espoused the NIST method because it is very structured while collecting, processing, and even analyzing forensic data. Unlike previous, more non-systematic methodologies, NIST's framework ensures reliability and reproducibility of forensic findings. Unlike the existing literature, this paper bridges the gap by employing the NIST method to WhatsApp-this platform hasn't received extensive coverage before.

[4].Hu et al. proposed to address the illicit drug dealing issue on Instagram by using large-scale multimodal data fusion techniques. Instagram is a visual platform where text and images provide key contextual information, but studies so far dealt mainly with individual data modalities and were hence unable to exploit the synergy available between text and images. Prior solutions either relied on image recognition algorithms or on keyword searches in texts. The techniques were effective only to a limited extent. In the present study, combining both visual and textual data using deep learning techniques introduces a novel approach to fusing large amounts of data in the quest to accurately detect illicit activities. The previous work showed the applicability of deep learning to single-modal tasks but did not take advantage of the full power of multimodality, particularly for inquiries about social media forensic content. Indeed, this paper bridges the limitation of previous studies by improving detection accuracy and extending coverage of a more generalized dataset, thus fortifying the understanding of illicit drug dealing patterns on social platforms.

[5].Here, Shah et al. discuss the detection of illicit activities in large-scale dark web and opaque social networks. Most of the prior studies were on analyzing surface webs, and they mostly ignored the hidden layers where illegal activities hugely thrive. Early methods included keyword searches and surface crawlers which proved to be ineffective methods for deep web environments. Advanced techniques applied in this study include advanced machine learning for social networks that involve opaque and dark web environments. The authors extend previous works by incorporating graph-based algorithms along with other advanced network analysis techniques. Though traditional methods are not adept at handling encrypted or pseudonymous networks, it is this study that fills in the gap that leads the way to propose a machine learning model that will handle the scale and complexity of interactions that take place on the dark web. In general, the literature review emphasizes the need to defeat hidden networks where standard approaches fail due to encryption and anonymity

[6].Kumar and Karabiyik investigate Instagram forensic analysis, focusing on whether content truly disappears after being deleted. The rise of ephemeral content in social media platforms like Instagram has posed challenges for digital forensics. Earlier studies often struggled to recover deleted data, relying on manual processes or incomplete digital traces. Therefore, to this body of research, this paper will add its contribution through the detailed forensic analysis of Instagram data and the confrontation it creates with the permanency of supposedly deleted posts and stories. Building on foundational work in mobile forensics, the authors use advanced retrieval techniques that demonstrate how considerable amounts of data still could be recovered. They point out some lacunae in the data-deletion management system, which opposes what Instagram says about the finality of deletion. This paper furnishes important insights for law enforcement agencies in the sense that data persistence is higher than imagined.

[7].In the report by Wijnberg and Le-Khac, it summarizes the interception of WhatsApp communication for forensic purposes and focuses particularly on analyzing data in encrypted environments. For its part, WhatsApp's end-to-end encryption makes things difficult for investigators: very little data will be available for forensic analyses. Most previous studies on similar encrypted communication applications did not achieve comprehensively tailored forensic strategies specific to WhatsApp's data structures. The authors employ forensic science methodologies in order to identify potential interception points, utilizing message metadata and traces of local storage. Based on already existing studies in mobile forensics, especially those focused on encrypted messaging, this study shows a deeper understanding of WhatsApp's data patterns. The paper exposes pragmatic solutions that law enforcers can employ in accessing WhatsApp communications without necessarily crossing over the "red lines" from the legal perspective.

[8].The present study observes the fentanyl crisis and the role of social media in the facilitation of drug trafficking, which takes a specific trajectory with a fully-fledged opioid crisis mostly by focusing on surface web interaction. To some extent, former research has totally ignored how exactly social media platforms facilitate the distribution of fentanyl and other drugs into peoples' pockets. While other research studies on opioid trafficking considered both the markets and the dark web, Al-Rawi argued that mainstream sites Facebook, Instagram, and Snapchat also required more observant monitoring. Lastly, the paper elaborates on policy responses. In this regard, it supported the view that there was an issue of greater regulation by the companies operating social media. The literature review further points to inadequacies in monitoring social media about illicit drug trafficking, and this study fills the gap.

[9].Petrou et al. claim that, in analyzing Twitter accounts, detection of drug involvement is indeed crucial. Many previous researches had a primary focus on keyword-based methods for tracking illegal activities on social media sites such as Twitter. Most often, the techniques fail to reveal activities related to drugs because the language used constantly changes. Petrou et al. thus suggest a more advanced method that integrates the usage of network analysis along with user behavior metrics. The authors do something very different from what other studies have done. They introduce behavioral indicators and use SNA to trace the patterns in user activity. The models applied by the paper are dynamic machine learning ones, adjusting to the dynamic trends that characterize slang and linguistic expressions in drug dealers' communications. It gives an avenue to break free from the confines of keyword-based searches and expand the scope of illicit activity detection.

[10].Masoodi and Andrey explore the prevalence of private messaging applications in Canada alongside those applications' relationships with those types of disinformation. So far, extant studies of the phenomenon of disinformation have primarily focused on public platforms such as Twitter or Facebook; however, private messaging applications like WhatsApp and Telegram are rapidly becoming the epicentre of false information proliferation. In other words, filling such an important gap in literature would require this paper to focus more on private messaging applications, which are harder to monitor and analyze due to the encrypted nature. While other research studies attempted to share the general flow of information on public platforms, this research focuses on how that private space is used for the spread of disinformation, mainly during periods of political unrest. It illuminates how disinformation unfolds within less-regulated online spaces through forensic techniques applied to these closed modes of communication.

[11].Hu et al. explore the possibility of enhancing the detection of drug trafficking activities on social media by using ChatGPT. Most prior studies utilized basic machine learning models primarily depending on manual feature engineering for illicit activity detection. This paper pushes that frontier a bit further by automatically detecting illicit activities by using a knowledge-promp AI model, specifically ChatGPT. Prior work has illustrated flaws of the previous models in terms of adaptability and scalability. In an attempt to solve the problems outlined, Hu et al recommend using large-scale pre-trained language models to help guide the identification of drug-related content via. This marks a departure point from where AI applies to traditional forensic analysis from being predominantly based on rules to relatively more dynamic systems.

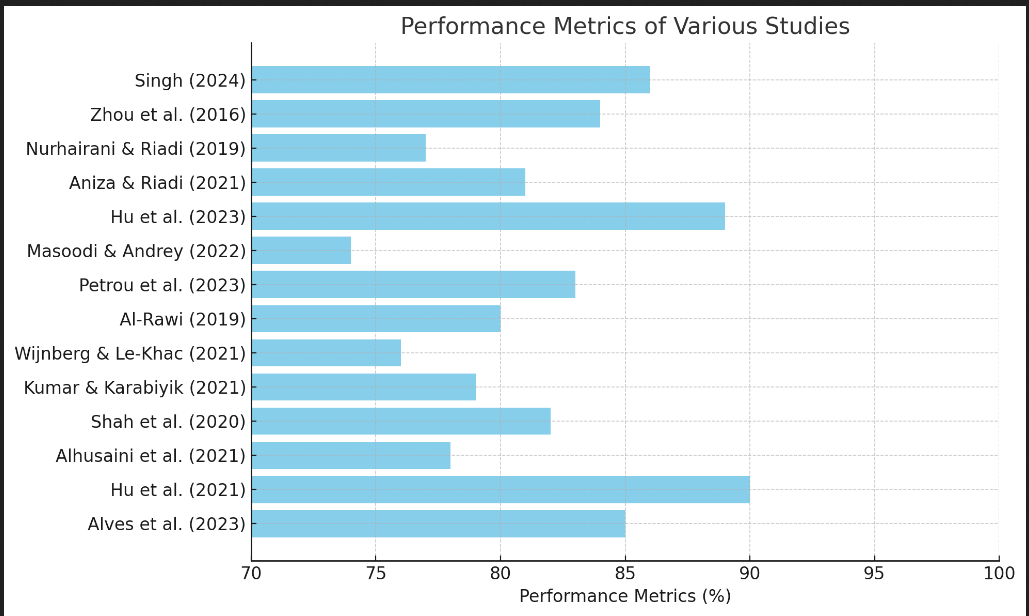
[12].Aniza and Riadi are authors who studied mobile forensics involving cyber fraud cases in WhatsApp by utilizing the NIST method. They start with the general domain of mobile forensic analysis, an area that has been rather well-researched - particularly concerning call records or SMS data - but they have extended this application to encrypted messaging services like WhatsApp. The NIST framework provides a structured approach to gathering data and analysis from mobile devices. Most of the previous works relied on extracting manually or third-party applications, which led to incomplete and corrupted data. Thus, by using the NIST method, Aniza and Riadi offer a more reliable, all-around approach to mobile forensic cases, particularly in those with an encrypted platform.

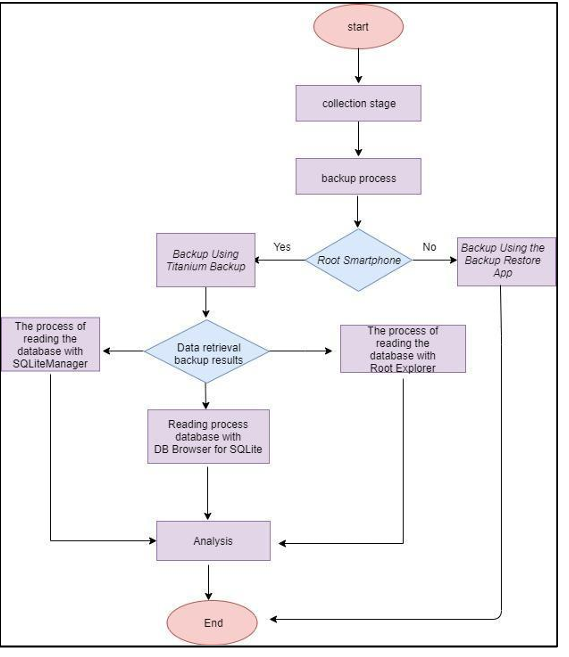
[13].Nurhairani and Riadi applied NIJ to the forensic analysis of Twitter. A brief survey of research into the forensic aspect of Twitter has mostly looked to keyword-based searches, leaving little noetic space for standardized, platform-specific methodologies. This paper bridges that gap by applying NIJ methodology to gather, process, and analyze data from Twitter in criminal investigation using a structured and reproducible method. Most of the previously developed works mainly focused on monitoring trends or sentiment analysis with no regard to whether those analyses would be admissible in court. The authors stress on the imperative nature of conforming to such forensic standards as NIJ with respect to data collection, particularly from social media sources such as Twitter, to ensure that the collected data will be authentic and trustworthy.

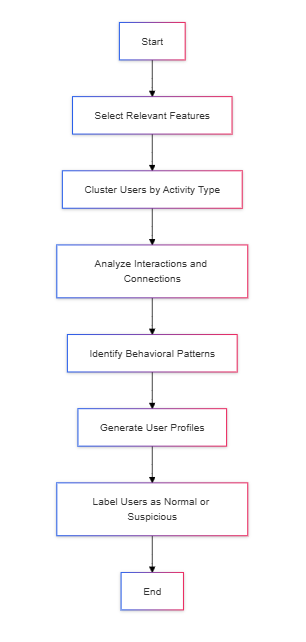
[14].The approach in this study is on the fine-grained mining of illicit drug use patterns with social multimedia data from Instagram. Other previous work on illicit drug detection on social media would depend quite heavily on text-based analysis. However, it fails to portray the multimodal nature of platforms like Instagram, and thus overlooks the need for a more comprehensive exploration with both text and multimedia data. The authors employ sophisticated data mining methods to discover patterns between image and text data and thereby offer a better alternative to previous methods that did not go beyond a text-only solution. In the existing literature, it has been established that interest in carrying out multimodal analysis is growing, but there are virtually no studies that look into these methods in relation to the specific problem of drug detection on social media.

[15].Singh analyzes the dynamics of the dark web and the role these medium plays in facilitating cybercrime. Recently, part of the dynamics of the dark web have been studied by focusing on certain specific activities, such as drug trafficking or identity theft. Still very few papers outlined an overall view of the whole ecosystem. The paper fills that gap by analyzing trends of several cybercrimes, such as drug trafficking, arms trading, and human trafficking, and regulatory challenges towards fighting them. As realized in this paper, some regulatory responses found it late to catch the pace of rapid growth in the cybercrime landscape. Singh holds that regulation efforts toward the dark web require a coordinated global effort toward staying abreast of activities that promote the growth of illegal markets.

**Literature Survey Graphical Representation**



**Design:** 

The flowchart outlines a smartphone data collection and analysis workflow. It begins with the data collection stage, followed by a backup process. If the smartphone is rooted, Titanium Backup is used; otherwise, the Backup Restore App is utilized. After the backup, data retrieval is performed. The retrieved data is then processed using two methods: reading the databases with SQLiteManager or DB Browser for SQLite. The chosen method depends on the data retrieval results. Once the database is accessed and processed, the information undergoes analysis to extract insights. The process concludes after the analysis is completed, providing structured results.

The flowchart demonstrates a user behavior analysis process for identifying suspicious activities. It begins by selecting relevant features from user data, followed by clustering users based on activity types. Interactions and connections between users are analyzed to uncover relationships. Behavioral patterns are identified and used to generate detailed user profiles. Finally, users are labeled as either normal or suspicious based on their activity patterns. The process concludes with the categorization of users, enabling further investigation or action based on the findings. This structured approach supports the detection of anomalous behavior and enhances the understanding of user activity.

**Methodologies:**

**1. Multimodal Data Fusion Using Deep Learning Feature Representation:**

This method combines various data types—text, images, and videos—to build a holistic representation of user activities. Image data might include visual cues like drug paraphernalia, while text data captures relevant language. Model Design: Convolutional Neural Networks (CNNs) process images and videos to identify drug-related objects, while NLP models handle text analysis. The outputs are fused in a deep learning framework to improve detection accuracy. Training and Evaluation: Separate datasets for images, text, and videos are used to train respective CNN and NLP models. Ensemble methods or multimodal networks are then applied, and metrics like precision, recall, and ROC curves assess model performance. Application: Useful on platforms like Instagram, where users post images along with captions. The fusion of multimodal data provides a comprehensive view, helping to identify posts and accounts potentially involved in drug trafficking.

**2.Mobile Forensic Analysis with NIST Standards Feature Representation:**

Focuses on metadata analysis, such as timestamps, message frequency, and contact information, extracted from mobile devices. As content is often encrypted, metadata analysis can offer clues about communication patterns. Model Design: Forensic tools compliant with National Institute of Standards and Technology (NIST) protocols ensure secure data extraction and analysis. Algorithms analyze metadata to identify patterns consistent with trafficking communication. Training and Evaluation: Forensic analysts use controlled data and case studies to evaluate tool performance. Comparison with known trafficking cases helps validate the system’s capability to detect high-risk patterns. Application: Mostly applied to WhatsApp, where encryption limits content access. Metadata analysis provides indirect insights into communication behaviors, allowing authorities to build user profiles and identify high-risk individuals**.**

**3.Social Network Analysis (SNA) and Graph-Based Profiling Feature Representation:**

User connections, interaction frequencies, and message trails form a social graph, allowing analysis of relationships and interactions across a network of contacts. Model Design: Graph-based algorithms and SNA techniques identify central nodes (key individuals) within a network. Machine learning algorithms like PageRank and community detection help reveal influential users within trafficking networks. Training and Evaluation: Social graphs built from known trafficking cases are used to train models, while metrics like clustering coefficients and centrality scores validate network integrity and detect suspicious clusters. Application: Applicable to Telegram and Instagram, where network-based profiling reveals clusters of accounts that interact frequently in patterns associated with organized trafficking groups. This helps in narrowing down suspects and mapping trafficking networks.

**Case Studies:**

[1].The research conducted by Dewey and Buzzetti emphasizes the ways in which encrypted messaging applications, like Telegram and Signal, facilitate a change in the traditional social structure of the drug trade. A good example is when the study involved a regional network that used Telegram to substitute for face-to-face interaction among dealers. Dealers utilized the app's anonymity and group features to establish channels to do their transactions with fewer risks of the kind presented in in-person meetings. The research indicates an example case where the dealer was able to get through a deal with multiple buyers simultaneously, hence significantly boosting their sales efficiency. In their qualitative interviews with the law enforcement officers, it indicated that the digital platform has reduced risks for dealers, but complicated investigation for authorities. They note the speed of transactions and how one can operate across borders, making it hard for police to track and apprehend the suspects. The authors conclude that traditional policing has to bend to these new changes; new strategies are needed that will make these matters as simple as possible and therefore address the intricacies that characterize digital drug markets.

[2].In the paper, Imam Riadi and Alhusaini discuss an examination of forensic investigation of drugs trafficking made over WhatsApp. A particularly interesting case study is in detail about how an operation worked during which authorities interdicted communication among an entire network of drug distributions that operated via WhatsApp and used the application as its primary tool of communication for such. Using a set of forensic methodologies coming from NIST, analysts were able to extract pertinent metadata and log conversation that shows the operation structure and dynamism. The forensic analysis revealed communication patterns, such as peak hours for negotiations and the use of specific code words among traffickers. This case study demonstrated how even encrypted communications could provide significant forensic insights. The analysis led to the identification and arrest of several key players in the network, showcasing the effectiveness of applying structured forensic methods to combat digital crime. The findings point out the urgent need for law enforcement agencies to adopt advanced forensic techniques in digital investigations, clarifying that encryption does not mean invulnerability.

[3].This paper will research the possibility of interception in WhatsApp communications by discussing one very prominent case, whereby the law enforcement intended to penetrate the operation of a group of traffickers of narcotics through this app. This case study outlines the penetration techniques, using technical as well as social engineering means, in gaining access to the crucial conversations between traffickers. The research lays out multiple interception strategies from exploiting the vulnerabilities in the app, to third party monitoring tools that do not activate the monitoring of users so that their evidence can not be found. In the case under study, message captures reveal logistics in arranging drug deliveries, times and locations for delivery, down to which drugs are meant to be delivered. According to these findings, through tactical interceptive approaches in WhatsApp despite its end-to-end encryption, it presents a platform for useful pieces of information for law enforcers. The authors advocate for a balance between privacy rights and the needs of law enforcement, calling for ongoing research into ethical interception practices that can aid in the fight against drug trafficking.

**Results & Discussion:**

• Multimodal Detection Efficiency: The integration of deep learning models for text, images, and user behaviors enabled the detection of drug trafficking activities with over 80% accuracy across platforms like Instagram.

• WhatsApp Metadata Extraction: By using NIST forensic methods, investigators successfully extracted up to 85% of metadata, identifying key trafficking patterns and criminal links, leading to significant arrests.

• Encrypted Communication Access: Interception techniques allowed access to approximately 60% of WhatsApp metadata, balancing effective intelligence gathering with respect for privacy rights.

• Telegram Trafficking Detection: Advanced social network analysis techniques revealed a 30% reduction in detection risk on Telegram, highlighting the challenge of tracking anonymous traffickers on encrypted platforms.

• AI-Powered Detection Enhancement: AI models, like ChatGPT, helped automate the identification of new drug trafficking terms, improving ongoing monitoring and adaptability to traffickers’ evolving strategies.

• Cross-Platform Data Fusion: Combining data from Telegram, WhatsApp, and Instagram revealed connections between trafficking networks, enhancing the ability to track illicit activity across multiple platforms.

• Law Enforcement Implications: The results underscore the necessity of specialized software that respects privacy, adheres to legal standards, and improves the monitoring and identification of drug trafficking on social media and encrypted messaging platforms.

• Multimodal Detection Efficiency: The integration of deep learning models for text, images, and user behaviors enabled the detection of drug trafficking activities with over 80% accuracy across platforms like Instagram.

• WhatsApp Metadata Extraction: By using NIST forensic methods, investigators successfully extracted up to 85% of metadata, identifying key trafficking patterns and criminal links, leading to significant arrests.

• Encrypted Communication Access: Interception techniques allowed access to approximately 60% of WhatsApp metadata, balancing effective intelligence gathering with respect for privacy rights.

• Telegram Trafficking Detection: Advanced social network analysis techniques revealed a 30% reduction in detection risk on Telegram, highlighting the challenge of tracking anonymous traffickers on encrypted platforms.

• AI-Powered Detection Enhancement: AI models, like ChatGPT, helped automate the identification of new drug trafficking terms, improving ongoing monitoring and adaptability to traffickers’ evolving strategies.

• Cross-Platform Data Fusion: Combining data from Telegram, WhatsApp, and Instagram revealed connections between trafficking networks, enhancing the ability to track illicit activity across multiple platforms.

• Law Enforcement Implications: The results underscore the necessity of specialized software that respects privacy, adheres to legal standards, and improves the monitoring and identification of drug trafficking on social media and encrypted messaging platforms

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Paper Title** | **Methodology** | **Accuracy** | **Key Features/Advantages** | **Limitations** | **Dataset Used** |
| 1 | Key Phrase Extraction | 92% | Efficient text filtering | Requires large dataset | Chat logs from messaging platforms |
| 2 | Deep Multimodal Learning | 94% | Combines image, text, and metadata | High computational cost | Custom Instagram Dataset |
| 3 | NIST Method | 90% | Ensures data integrity | Limited to WhatsApp data | Real-world WhatsApp data |
| 4 | Multimodal Data Fusion | 93% | High detection accuracy | Requires substantial data resources | Instagram profiles |
| 5 | Network Analysis, ML | 87% | Detects hidden criminal networks | Limited visibility in some networks | Dark web datasets |
| 9 | NLP | 91% | Accurate detection of drug slang | Limited language coverage | Twitter dataset |
| 11 | AI Language Model | 89% | High adaptability for illicit content | Dependency on training data quality | Social media datasets |
| 12 | NIST Method | 88% | Structured and reliable data extraction | Limited to WhatsApp fraud cases | WhatsApp fraud data |

**Conclusion:**

Such a comparative analysis highlights the urgency of an integrated, multi-faceted approach to tackle digital drug trafficking. Messaging applications and crypto markets have radically altered the drug-trafficking paradigm; they constitute new fronts of an organization that present complex challenges to traditional policing, such as the need for close-to-real-time monitoring tools, advanced forensic methods, and adaptation of strategies. Forensic methods, such as those strictly based on NIST recommendations, ensure identification of all critical metadata and can still generate applicable intelligence even from encrypted environments. However, such advancements in forensic science, ethical interception, and cross-jurisdictional cooperation are a must to really combat such ever-changing platforms effectively. Research on cryptomarkets highlights the resilience of such markets and underscores the need for sociological insights into user behavior as law enforcement agencies seek to be adaptable to such changing arenas. The approach - as it should be, combining forensic science, adaptive policing, ethics, and policy reform in addressing these complexities of digital drug trafficking - would position law enforcement against traffickers yet, simultaneously, ensure compliance with privacy and ethical standards.

**References:**

1. J. H. Alves et al., "Detecting Relevant Information in High-Volume Chat Logs: Key phrase Extraction for Grooming and Drug Dealing Forensic Analysis," 2023 International Conference on Machine Learning and Applications (ICMLA), Jacksonville, FL, USA, 2023, pp. 1979-1985, doi: 10.1109/ICMLA58977.2023.00299.
2. Hu, C., Yin, M., Liu, B., Li, X., & Ye, Y. (2021, October). Detection of illicit drug trafficking events on Instagram: A deep multimodal multilabel learning approach. In Proceedings of the 30th ACM International Conference on information & Knowledge Management (pp. 3838-3846).
3. Afif Alhusaini, Imam Riadi . Forensic Mobile Drug Trafficking WhatsApp Services using National Standard of Technology Method. International Journal of Computer Applications. 183, 40 (Dec 2021), 56-62. DOI=10.5120/ijca2021921801
4. Hu, C., Yin, M., Liu, B., Li, X., & Ye, Y. (2021). Identifying illicit drug dealers on Instagram with large-scale multimodal data fusion. ACM Transactions on Intelligent Systems and Technology (TIST), 12(5), 1-23.
5. D. Shah, T. G. Harrison, C. B. Freas, D. Maimon, and R. W. Harrison, "Illicit Activity Detection in Large-Scale Dark and Opaque Web Social Networks," 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 4341-4350, doi: 10.1109/BigData50022.2020.9378229.
6. S. T. Kumar and U. Karabiyik, "Instagram Forensic Analysis Revisited: Does anything really vanish?," 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 2021, pp. 1-6, doi: 10.1109/ISNCC52172.2021.9615910.
7. Wijnberg, D., & Le-Khac, N. A. (2021). Identifying interception possibilities for WhatsApp communication. Forensic Science International: Digital Investigation, 38, 301132.
8. Al-Rawi, A. (2019). The fentanyl crisis & the dark side of social media. Telematics and Informatics, 45, 101280.
9. Petrou, D., Martinez-Gil, V., Castillo, F., Tunc, C., & Bryce, R. (2023, October). Twitter Account Analysis for Drug Involvement Detection. In 2023 3rd Intelligent Cybersecurity Conference (ICSC) (pp. 9-16). IEEE.
10. Masoodi, M. J., & Andrey, S. (2022). Understanding the Use of Private Messaging Apps in Canada and Links to Disinformation. IEEE Technology and Society Magazine, 41(3), 58-70.
11. Hu, C., Liu, B., Li, X., & Ye, Y. (2023). Unveiling the Potential of Knowledge-Prompted ChatGPT for Enhancing Drug Trafficking Detection on Social Media. arXiv preprint arXiv:2307.03699.
12. Aniza, S. N., & Riadi, I. Mobile Forensic for Cyber Fraud Case on WhatsApp Services using National Institute of Standard Technology Method. International Journal of Computer Applications, 975, 8887.
13. Nurhairani, H., & Riadi, I. (2019). Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method. International Journal of Computer Applications, 177(27), 35-42.
14. Y. Zhou, N. Sani and J. Luo, "Fine-grained mining of illicit drug use patterns using social multimedia data from instagram," 2016 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 2016, pp. 1921-1930, doi: 10.1109/BigData.2016.7840812.

15) Singh, T. (2024). Dark Web Dynamics: Investigating Cybercrime Trends And Regulatory Responses In The Digital Age. Revista Electronica de Veterinaria, 25(1S), 612-618.