Available Online: 18 July 2025 DOI: 10.54254/2753-7102/2025.25357

Application of intelligent interrogation technology in cross-border telecommunication fraud cases: theoretical foundations, system construction, and practical pathways

Yaxian Qiu[1], Yile Wang[1], Xinyu Guo[1]*

[1]Shanxi Police College, Taiyuan, China

*Corresponding Author. Email: yaxianqiu@126.com

Abstract. Against the backdrop of efforts to significantly enhance the modern combat capabilities of public security, this paper focuses on the interrogation challenges in cross-border telecommunication network fraud cases and explores the application of Artificial Intelligence (AI) technology to improve interrogation efficiency and quality. It proposes the construction of an intelligent interrogation system by identifying the criminal characteristics of cross-border telecommunication fraud and analyzing the current technical and practical difficulties faced in interrogations. Focusing on AI-assisted interrogation in telecommunication fraud investigations, the study develops algorithms and models to build an intelligent interrogation system for cross-border fraud cases. The results indicate that AI-based interrogation systems can enhance the efficiency of information extraction, optimize investigative strategies, and provide technological support for the rapid resolution of cross-border telecommunication fraud cases.

Keywords: cross-border telecommunication fraud, criminal investigation and interrogation, artificial intelligence, intelligent policing

1. Introduction

Cross-border telecommunication fraud has become a major criminal issue worldwide. Offenders exploit various communication tools and online platforms to fabricate facts or disseminate false information in order to defraud victims, with such crimes often involving multiple countries and regions [1]. These cases are typically characterized by transnational operations, tight organizational structures, technologically advanced methods, and high levels of concealment, all of which present serious challenges for law enforcement agencies in terms of investigation, evidence collection, interrogation, and sentencing [2]. Based on literature reviews and interviews, the main pain points in the investigation and interrogation process of cross-border telecommunication fraud cases are illustrated in Figure 1.

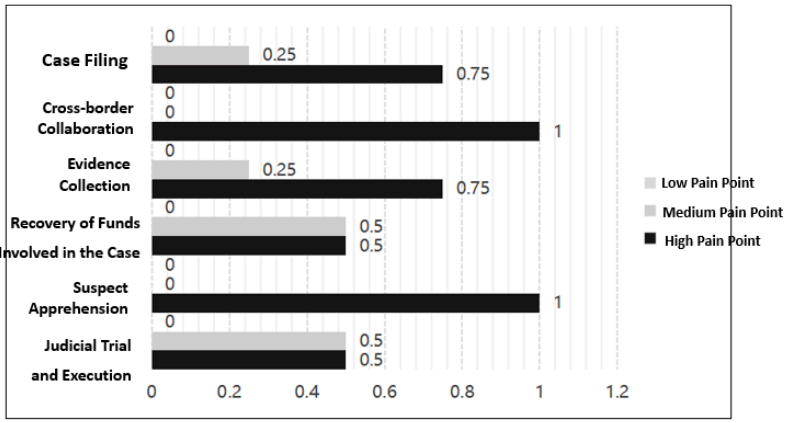


Figure 1. Heatmap of pain points in the investigation and interrogation process of cross-border telecommunication fraud cases

Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

According to data released by the Supreme People's Procuratorate, more than 34,000 individuals were prosecuted nationwide for telecommunication fraud in 2023, representing a year-on-year increase of nearly 52% [3]. Cross-border telecommunication fraud now accounts for over 60% of all telecommunication fraud cases, with the average financial loss per case reaching 427,000 RMB. The number of such cases continues to grow at an accelerating pace [4]. Notably, in cases originating from northern Myanmar, the difficulty in obtaining electronic evidence from abroad has led to an average case resolution period of 9.8 months.

Based on data from the Judgments Online (Jufa) database, a search for the keyword "telecommunication fraud" during the period from January 1, 2019 to December 31, 2023 yielded 21,240 verdicts. A further search using the keywords "cross-border" and "telecommunication fraud" within the same timeframe resulted in 1,307 verdicts. The number of such judgments has been increasing steadily, with cross-border telecommunication fraud accounting for 6.55% of all telecommunication fraud cases in 2023.

As technology continues to advance, criminal groups are continuously upgrading their fraud techniques. Law enforcement agencies must therefore urgently build intelligent countermeasure systems. Artificial Intelligence (AI) technology has become a key enabler in enhancing investigative capabilities [5]. Against this backdrop, this study aims to explore how AI can help resolve the technical and practical challenges encountered in handling cross-border telecommunication fraud cases. The core research questions include: How can the difficulties in recognizing multilingual confessions be overcome? How can effective chains of evidence be constructed to improve case-handling efficiency in cross-border investigations? How can technical limitations during interrogation—such as model overfitting and algorithm transparency—be addressed?

2. Research gaps

Existing studies have predominantly focused on the application of AI technologies in areas such as crime prediction, intelligence analysis, and behavioral modeling, achieving to some extent the integration and intelligent processing of multimodal data. However, there remain several deficiencies in research on intelligent interrogation systems specifically tailored to cross-border telecommunication fraud cases.

First, there is insufficient analysis of the current technological landscape. At present, AI applications in interrogation mainly concentrate on foundational uses, such as information collection through mobile policing terminals. However, research and analysis on dedicated AI interrogation systems—such as lie detection technologies based on semantic mining, affective computing, and multimodal data analysis—remain insufficiently explored. For instance, existing LSTM-based voice emotion analysis models achieve only 72.4% accuracy in micro-expression recognition, which is inadequate for effectively countering suspect disguise behaviors in cross-border telecommunication fraud cases. Current AI systems largely rely on unimodal data analysis, whereas interrogation of cross-border cases demands the integration of multi-source data such as IP geolocation, financial transaction flows, and multilingual confessions. This technical bottleneck urgently requires resolution.

Second, there are issues related to policy and regulatory adaptation. Although China has introduced multiple AI governance regulations, including the Administrative Measures for Generative AI Services and the Regulations on Algorithmic Recommendation for Internet Information Services [6], these legal frameworks still have blind spots in their application to intelligent interrogation. In particular, the Rules on Electronic Evidence Collection in Criminal Cases by Public Security Organs (2020) and Article 13 of the Personal Information Protection Law, which restrict the collection of biometric data, create legal ambiguities regarding the data acquisition necessary for micro-expression analysis during interrogations. Cross-border interrogations also face legal conflicts involving multiple jurisdictions—for example, Article 48 of the EU's General Data Protection Regulation (GDPR) restricts cross-border data transfer—posing elevated challenges to the acquisition and use of data by AI systems across borders.

Third, practical operational demands have not been fully explored. Current research inadequately addresses the specific technical obstacles encountered in actual police work involving cross-border cases. For example, challenges such as IP tracing difficulties caused by overseas server hops and conflicting suspect statements due to rotating interrogations of personnel at Southeast Asian fraud dens have not been sufficiently discussed. Taking the "3.15 Northern Myanmar Telecom Fraud Special Case" supervised by the Ministry of Public Security in 2024 as an example, nearly half of the suspects had received counter-interrogation training, exposing deficiencies in existing AI models' robustness against deliberately deceptive behaviors.

3. Key issues to be addressed by the intelligent interrogation system for cross-border telecommunication fraud cases

In the process of investigating cross-border telecommunication fraud cases, intelligent interrogation systems must provide effective solutions tailored to specific challenges. Existing interrogation systems tend to be overly generalized and fail to adequately address the unique issues inherent in cross-border cases. This study focuses on three core contradictions: the data silo problem, the confession verification problem, and the adversarial interrogation problem.

3.1. Data silo problem: challenges in obtaining cross-border evidence

The issue of data silos is particularly acute in cross-border telecommunication fraud cases, especially the difficulty in retrieving electronic evidence from overseas. Analysis of the 18th batch of guiding cases published by the Supreme People's Procuratorate highlights the unavailability of data from foreign servers as a significant obstacle in case investigations. This problem not only severely compromises the integrity of the evidence chain but also presents enormous challenges to case resolution. To address this, the study emphasizes the use of Natural Language Processing (NLP) technologies to analyze existing textual information in cases (such as confessions and witness testimonies). Text mining techniques will be employed to identify potential key information that can effectively supplement and complete the evidence chain. Particularly when evidence cannot be obtained by traditional means, NLP can leverage its strong textual comprehension and analytical capabilities to help investigators extract valuable information from confessions and case materials.

However, NLP technologies still face challenges due to mixed languages and contextual differences in cross-border cases. For instance, in northern Myanmar, mixed Chinese-Myanmar bilingual confessions are common, and conventional NLP models such as BERT cannot effectively handle these hybrid-language confessions. Therefore, optimized multilingual models, such as a fine-tuned interrogation-specific language model based on BERT-Base (PoliceBERT), are required to cope with the complexity of different languages and dialects. This technology improves the system's adaptability to linguistic barriers in cross-border cases and enhances the accuracy and effectiveness of confession analysis in multilingual mixed environments.

3.2. Confession verification problem: challenges in multilingual confession and contradiction detection

Confession verification is particularly complex in multilingual environments, where differing linguistic and cultural backgrounds often cause contradictions and inconsistencies in statements. In practice, suspects in cross-border cases have a high rate of recanting confessions, largely due to exploiting jurisdictional loopholes across borders, which affects the authenticity and reliability of their statements. To effectively verify confessions, this study adopts multilingual NLP models and utilizes PoliceBERT, a BERT-Base fine-tuned interrogation-specific language model, to resolve issues such as dialect mixing and language barriers. Through this technology, the system can accurately analyze key information within multilingual confessions and perform consistency and logical coherence checks to identify contradictions. This process provides strong support to interrogators, helping them assess the credibility of suspect statements and make necessary adjustments or corrections.

Technical challenges may arise during confession verification, such as false positives or misidentification. Multimodal data fusion (e.g., combining micro-expression analysis with voice recognition) may cause cumulative errors, where misclassification of micro-expressions overlaps with voice recognition inaccuracies, thereby affecting the accuracy of confession verification. To mitigate this, the study proposes incorporating a risk control module into the system that quantifies error rates and accuracy metrics of various technologies, enabling real-time monitoring of analysis risks to ensure system stability and accuracy.

3.3. Adversarial interrogation problem: optimization and intelligence of interrogation strategies

In the interrogation process of cross-border telecommunication fraud cases, optimizing interrogation strategies is key to improving case-solving efficiency. Traditional interrogation methods often rely heavily on experienced experts, but such approaches can lead to rigid strategies and dependence on routine techniques when facing complex cross-border cases, potentially causing risks of coerced or induced confessions. To optimize interrogation strategies, this study proposes using Q-Learning and Monte Carlo Tree Search (MCTS) algorithms.

Learning is a value-based, model-free, off-policy reinforcement learning algorithm designed to find an optimal policy for an agent in a given environment. Monte Carlo Tree Search (MCTS) is a decision-making algorithm that simulates multiple trajectories from the current state, progressively focusing on and selecting paths with higher evaluation values to find the optimal solution. Q-Learning can iteratively optimize interrogation strategies through interactions with interrogators, enabling the system to autonomously generate the best interrogation plans. Meanwhile, MCTS can simulate potential outcomes under different interrogation strategies and select the most likely successful strategy for implementation. Although these techniques have considerable theoretical potential, they also face challenges such as convergence efficiency and practical effectiveness. For instance, Q-Learning models may suffer from overfitting to historical data, leading to a lack of innovation in interrogation strategies and difficulty adapting to novel case scenarios. Therefore, this study employs extensive adversarial training—such as Generative Adversarial Networks (GAN)—to further optimize strategies, reducing the likelihood of strategy collapse and ensuring flexibility and accuracy during interrogations. The proposed technical solution focuses on three core contradictions in cross-border telecommunication fraud investigations: data silos, confession verification, and adversarial interrogation.

By leveraging Natural Language Processing (NLP) techniques and intelligent interrogation strategy optimization, this study provides effective technical support for case investigations. Quantitative indicators such as the completeness of evidence chains, accuracy of confession alignment, and convergence efficiency of interrogation strategy optimization enable the system to define

clear improvement thresholds. Combined with a risk control module, the solution ensures the reliability and practical effectiveness of the technology. This approach not only addresses the core requirements outlined in the Opinions on Several Issues Concerning the Application of Law in Handling Cross-border Telecommunication Network Fraud and Other Criminal Cases jointly issued by the Supreme People's Court, Supreme People's Procuratorate, and Ministry of Public Security on July 26, 2024, but also aligns with the Ethical Norms for a New Generation of Artificial Intelligence, offering an innovative technological pathway for combating cross-border telecommunication fraud cases.

4. Construction of the intelligent interrogation system for cross-border telecommunication fraud cases

The core challenge in constructing an intelligent interrogation system for cross-border telecommunication fraud cases lies in efficiently extracting key information from multimodal data and formulating optimal interrogation strategies accordingly. Specifically, the handling of mixed languages presents a significant difficulty. Therefore, this study adopts a BERT-Base fine-tuned interrogation-specific language model (PoliceBERT) to address the multilingual confession problem during interrogations. PoliceBERT demonstrates significant advantages in multilingual processing, enabling precise comprehension of textual information and accurate identification of contradictions within statements. Compared to the general BERT model, PoliceBERT is fine-tuned for interrogation scenarios, allowing it to better understand professional terminology and complex contextual nuances encountered in interrogations, thereby enhancing the accuracy and reliability of confession analysis. For instance, when processing mixed Chinese-Myanmar bilingual confessions, PoliceBERT can accurately distinguish semantic elements from different languages, effectively avoiding semantic confusion commonly encountered by traditional models in mixed-language contexts.

To optimize interrogation strategies, this study employs a hybrid strategy optimization algorithm combining Q-Learning and Monte Carlo Tree Search (MCTS) to further refine interrogation approaches in cross-border telecommunication fraud cases. For processing image data during interrogations, ResNet-18 is selected as the feature extraction algorithm instead of traditional CNN architectures. The core advantage of ResNet-18 lies in its residual learning mechanism, which effectively mitigates the vanishing gradient problem common in deep networks. To more comprehensively analyze suspects' body movements, a Spatio-Temporal Graph Convolutional Network (ST-GCN) is introduced. ST-GCN effectively captures the motion trajectories of body joints and, when combined with Long Short-Term Memory (LSTM) networks to capture temporal dependencies, it can score behavioral abnormalities throughout the interrogation process. Compared to traditional behavior analysis methods, ST-GCN more accurately identifies abnormal body movements that may indicate underlying tension, anxiety, or deceptive intent by the suspect.

To achieve multimodal data fusion analysis and dynamic adjustment of interrogation strategies, the system is divided into two main modules: the Interrogation Assistance Module and the Intelligent Analysis Module (see Figure 2).

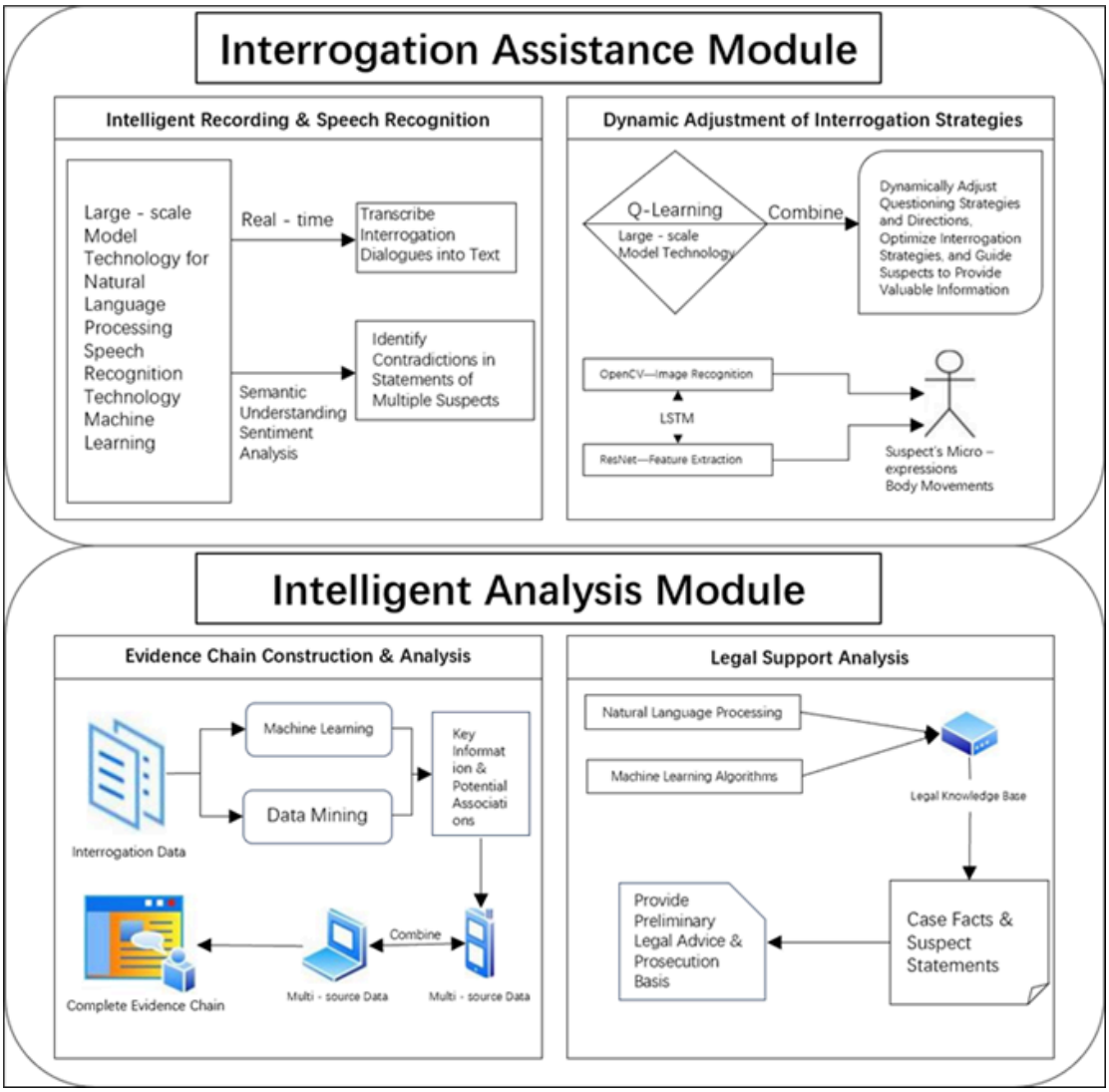


Figure 2. Modular architecture of the ai-powered intelligent interrogation system

4.1. Interrogation assistance module

This module leverages natural language processing, large-scale models, and speech recognition technologies. During the current interrogation process, intelligent transcription converts dialogue into text in real time. It optimizes recognition and transcription accuracy for Mandarin, regional accents, police technical jargon, and foreign language translations to ensure high accuracy. Given the characteristic "multiple suspects in the same case" in cross-border telecommunication fraud, this module applies natural language processing combined with the PoliceBERT model to deeply analyze the semantic content and emotional undertones of multiple suspects' statements. It identifies temporal and behavioral contradictions, automatically flags inconsistencies or illogical parts—such as differing descriptions of the same crime process or outcomes among suspects—and quickly pinpoints contradictions across multiple interrogation transcripts. This significantly reduces human oversight in the interrogation process and ensures the accuracy and reliability of the records. PoliceBERT's notable multilingual processing capabilities enable it to precisely grasp textual information and accurately detect contradictions within confessions amidst complex linguistic environments characteristic of cross-border telecom fraud cases.

Empowered by large-scale model technology, the system dynamically adjusts the interrogation personnel's subsequent questioning strategies and directions based on the context of the case and suspects' responses during the interrogation. This dynamic adjustment mechanism greatly enhances the targeting and success rate of interrogations, making each session more efficient. Q-Learning, a model-free reinforcement learning method based on Markov decision processes, learns optimal policies in discrete environments. The combined Q-Learning + MCTS hybrid strategy optimization algorithm further optimizes interrogation strategies in real time during the interrogation, dynamically adapting questioning tactics based on suspect reactions to elicit the most valuable information. Additionally, suspects' micro-expressions and body movements during interrogations

often reflect their true psychological states. The system integrates OpenCV for image recognition and uses ResNet-18 for feature extraction, alongside ST-GCN for analyzing motion trajectories of body joints. An LSTM model analyzes suspects' behavioral patterns and, combined with their verbal statements, evaluates the credibility of their confessions in relation to observed actions or expressions. If a suspect exhibits frequent body tremors, gaze aversion, or other behavioral cues while providing statements that conflict with other evidence, the system synthesizes this information to alert interrogation personnel to conduct focused scrutiny on that suspect's confession.

4.2. Intelligent analysis module

The intelligent analysis process is divided into two submodules: evidence chain construction and legal support. The evidence chain construction and analysis employs machine learning and data mining techniques to deeply analyze the vast amount of data generated during interrogations, extracting key information and potential correlations. By integrating multi-source data, dispersed pieces of evidence are linked to form a complete evidence chain. For example, by analyzing temporal, spatial, and behavioral information in suspect confessions combined with electronic evidence such as call records and transaction logs, a timeline and behavioral logic of the case can be constructed. Evidence visualization techniques convert complex data into intuitive and comprehensible charts, aiding interrogators in organizing case facts more quickly and clearly. Natural Language Processing (NLP) can also be applied for in-depth understanding and analysis of case facts; logical reasoning algorithms verify the logical consistency and rationality of the evidence chain to ensure its completeness and reliability. Moreover, real-time data collection and analysis allow dynamic updates to the evidence chain, continuously incorporating new evidence and adjusting the chain accordingly to maintain its current state. The legal support analysis function leverages a combination of NLP and machine learning algorithms to semantically understand and categorize legal provisions and cases through fusion algorithms, thereby constructing a comprehensive legal knowledge base. Interrogators can rapidly query relevant laws and precedents through the system, obtain legal support, and based on case facts and suspect statements, receive automated recommendations for applicable legal provisions, providing preliminary legal advice and supporting subsequent prosecution.

When the interrogation assistance module captures suspect reactions, it immediately updates their behavioral and emotional state in real time. The evidence chain construction submodule within the intelligent analysis module promptly analyzes the new information to assess its impact on the existing evidence chain. If new evidence potentially alters the case trajectory, the evidence chain construction submodule swiftly adjusts the evidence chain structure and triggers the legal support submodule to re-match relevant legal provisions, ensuring alignment between interrogation direction and legal application.

4.3. System technical architecture

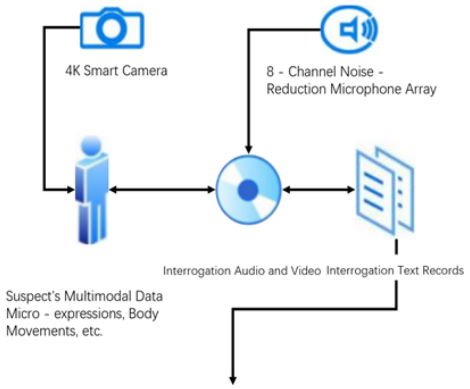
Data collection and processing form the foundation, involving real-time acquisition and handling of various data types generated during interrogations, including audio, video, physiological signals, and textual records. Multisensory data acquisition devices collect multimodal data such as suspects' speech, micro-expressions, and body movements in real time. On the hardware side, 4K intelligent cameras supporting H.265 encoding are deployed, offering high resolution and excellent low-light performance to accurately capture suspects' facial expressions and body movements, ensuring even subtle expression changes and gestures are clearly recorded. Additionally, an 8-channel noise-reduction microphone array effectively filters ambient noise and precisely focuses on suspects' speech to ensure voice data clarity and usability.

Collected data undergoes preprocessing and analysis. Audio and video data are first synchronized using timestamp alignment technology, achieving precise synchronization of audio, video, and physiological signals with a maximum temporal deviation controlled within 10 milliseconds, ensuring data consistency and usability. Irrelevant natural muscle reactions and spontaneous facial expressions unrelated to the case are filtered out to reduce data redundancy and outliers. For image data, OpenFace technology is used to extract multiple facial action units, accurately identifying suspects' micro-expression changes. Speech data is processed by extracting 26-dimensional Mel-Frequency Cepstral Coefficients (MFCC) features and fundamental frequency standard deviations to better capture emotional and semantic information in voice. Physiological signals are filtered and denoised to remove artifacts and noise, extracting high-quality physiological feature data. To ensure data uniformity and accessibility, all collected data is converted into a standardized format and stored in databases. Data storage adopts a hybrid approach combining relational and non-relational databases to meet storage needs for structured data (such as interrogation records and suspect information) and unstructured data (such as audio-video files and textual transcripts).

Finally, the data analysis module is constructed based on a dual-stream neural network architecture that separately processes textual and visual data. The textual branch utilizes the pre-trained PoliceBERT model to analyze suspects' verbal content; the visual branch inputs 30 frames per second (fps) facial landmark sequences, extracting spatiotemporal features via ResNet-18, and outputs probability distributions over six emotional categories including tension and avoidance. This dual-stream architecture simultaneously handles linguistic and visual information, providing comprehensive emotional analysis. Within the visual branch, a Spatio-Temporal Graph Convolutional Network (ST-GCN) is incorporated to analyze motion trajectories of body joints,

combined with LSTM networks to capture temporal dependencies, thereby scoring behavioral abnormalities during interrogations. Aiming for real-time analysis, the model will be optimized using TensorRT to compress end-to-end inference latency below 200 milliseconds, ensuring immediate capture and analysis of suspects' emotional and physical state changes, and providing prompt feedback to interrogators to assist accurate interrogation decisions (see Table 1).

Table 1. Technical architecture of the AI-powered intelligent interrogation system

<table>
<tr><td colspan="3">Data Acquisition Method and Hardware Configuration</td><td colspan="3">Data Analysis</td></tr>
<tr><td colspan="3" rowspan="2"> 
</td><td colspan="3">Purpose: To extract valuable information and provide decision support for assisted interrogation.</td></tr>
<tr><td>Text Branch</td><td colspan="2">Visual Branch</td></tr>
<tr><td colspan="3">Fine-tuned PoliceBERT model based on BERT-Base, specialized for interrogation language</td><td colspan="2">30 fps facial landmark sequences → ResNet-18 for spatiotemporal features
ST-GCN → analysis of body joint movement trajectories;
LSTM → capture temporal dependencies and score abnormal behaviors</td></tr>
<tr><td colspan="6">Inference optimized using TensorRT, achieving end-to-end latency <200 ms for real-time feedback supporting interrogation decisions</td></tr>
<tr><td colspan="3">Data Processing</td><td colspan="3">Data storage (relational database + non-relational database)</td></tr>
<tr><td>Synchronization Processing</td><td>Data Filtering</td><td>Multimodal Data Processing</td><td>Text Data</td><td>Audio-Video Data</td><td>Relationship Network Data</td></tr>
<tr><td>Timestamp alignment with maximum error <10 ms to ensure data consistency and usability</td><td>Removal of irrelevant natural muscle responses and other noise to reduce data redundancy</td><td>OpenFace + 26-dimensional MFCC features + filtering and denoising algorithms to extract high-quality multimodal feature data</td><td>Interrogation transcripts, case files, legal documents (txt, xlsx)</td><td>Audio and video recordings of interrogations (MP3, MP4, WAV)</td><td>Suspect relationship graphs, fund flow diagrams (Graph ML, JSON)</td></tr>
</table>

The cross-border telecom fraud interrogation assistance system leverages pre-trained models such as PoliceBERT, which, after fine-tuning, is adapted to interrogation scenarios and is expected to accurately identify semantic and emotional information in multilingual confessions. By combining the reinforcement learning algorithms Q-Learning and Monte Carlo Tree Search (MCTS), the system can intelligently adjust interrogation strategies in real time, exploring optimal interrogation paths and improving efficiency. It conducts comprehensive analyses of suspects' speech, text, and body movements to construct detailed suspect profiles. Performance testing of the algorithms demonstrates high accuracy, recall, and F1 scores, offering strong support for solving cross-border telecom fraud cases. As there is currently no access to real interrogation data, this study conducts an initial empirical analysis using simulated data. The simulated data is generated based on common features and scenarios of cross-border telecom fraud cases, including multilingual confessions, micro-expressions, and body movement information.

In the simulated environment, the system's response time is within 200 ms. It supports multiple languages and adapts to diverse interrogation scenarios, providing fast and precise support for cross-border telecom fraud interrogations. In the simulation experiments, the system used the following types of analytical data and algorithm parameter settings, as shown in Tables 2 and 3.

Table 2. Types of analytical data for the intelligent interrogation system

Text Data (txt, excel)	Audio-Video Data (MP3, WAV, MP4)	Relational Network Data (Graph ML/json)
Interrogation transcripts, case files, legal documents	Audio recordings and video footage from interrogations	Relationship graphs among suspects, diagrams of financial flows

Table 3. Selected parameter settings for the intelligent interrogation system

Parameter Name	Reference Value	Reference Description
PoliceBERT Learning Rate	5e-5	Balances learning speed and stability, consistent with common BERT fine-tuning learning rates
PoliceBERT Batch Size	16	Ensures training stability while maximizing GPU memory utilization to accelerate training
Q-Learning Learning Rate (α)	0.1	Controls the magnitude of Q-value updates, enabling the agent to appropriately adapt to dynamic changes in interrogation scenarios
Q-Learning Exploration Rate (ε)	0.2	Initial exploration rate set at 0.2 to ensure sufficient exploratory behavior in early training, decaying over time
ResNet-18 Input Size	224×224 pixels	Landmark sequence images are standardized to this size to meet ResNet-18's input requirements
ResNet-18 Feature Dimension	512	ResNet-18 outputs 512-dimensional features for use in emotion classification and other analysis tasks
ST-GCN Graph Convolution Layers	3 layers	Three graph convolution layers effectively capture spatial relationships and motion patterns among body keypoints

5. Potential challenges in implementing intelligent interrogation for cross-border telecom fraud cases

In practical application, intelligent interrogation tools face a wide range of technical, legal, and operational challenges, including technological limitations, cross-border legal conflicts, ethical considerations, and the adaptation of systems to human users. Based on this study's findings, these challenges are further detailed below, along with proposed mitigation strategies.

5.1. Technological penetration challenge: quantum computing threats and the fragility of current encryption systems

Under existing encryption frameworks, the security of intelligent interrogation systems in cross-border telecom fraud cases faces significant technological threats. With the rapid development of quantum computing, traditional encryption algorithms (such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC)) may become vulnerable to future attacks, posing new security risks for cross-border data transmission and evidence storage. This study recommends deploying quantum-resistant algorithms such as CRYSTALS-Kyber and Quantum Key Distribution (QKD) technology within the system to ensure long-term sustainability of encryption and data security. Adopting quantum encryption technology can effectively prevent data theft or tampering during cross-border transmission, providing a robust security foundation for the intelligent interrogation system.

5.2. Legal "swamp" challenge: conflicts in cross-border data legality and evidence recognition

Cross-border telecom fraud cases typically involve multiple jurisdictions, each with distinct legal standards for data admissibility and electronic evidence recognition. Mutual recognition of electronic evidence in international cases remains low. To address this issue, this study proposes building a Legal Adaptation Blockchain (based on Hyperledger Fabric), using smart contracts to enforce automatic compliance and resolve cross-border legal conflicts in evidence recognition and data transmission. This blockchain system can ensure lawful and compliant data exchange among parties, improving the efficiency of cross-border law enforcement. Moreover, by reducing disputes arising from international legal conflicts, the blockchain can offer strong technical support for mutual recognition of electronic evidence, thereby overcoming existing challenges in cross-border legal frameworks.

5.3. Human-AI trust building challenge: police officers' acceptance of AI-generated decisions

Implementing human-AI collaboration in intelligent interrogation faces significant challenges, particularly in frontline officers' trust in AI recommendations. Survey data indicate that initial adoption rates for AI decision support among officers are below 40%, highlighting that effective use depends not only on system accuracy but also on officers' trust and acceptance. This study recommends developing a dynamic trust model to monitor and evaluate the transparency of AI decision-making processes. By implementing hybrid augmented intelligence training systems, the AI can iteratively adjust based on officers' feedback, thereby improving both trust and system adaptability. Additionally, the system should provide clear, interpretable decision rationales and enable officers to review and provide feedback on AI recommendations, ensuring transparency and fairness in decision-making.

5.4. Addressing legal and ethical challenges

5.4.1. Data security in cross-border maintenance

Cross-border telecom fraud investigations involve large volumes of highly sensitive data. Any data breach or tampering can trigger international legal disputes and ethical controversies. According to the European Union European Union Agency for Cybersecurity (EU ENISA) report, 83% of cross-border law enforcement data breaches involve jurisdictional conflicts. This study recommends integrating robust data privacy protection measures into system design, including encryption, access controls, and multi-factor authentication, to ensure security during cross-border data transmission.

5.4.2. Multidimensional risks in intelligent interaction

Interactions between humans and AI in interrogation settings often face dual challenges of trust and ethics. AI systems rely on data and legal codes, but case handling must balance both legal rigor and human empathy to ensure fairness and humanity. This study therefore recommends strengthening ethical assessments of AI systems, particularly regarding emotion recognition applications, to avoid algorithmic biases that could adversely affect interrogation outcomes. Introducing adversarial training and continuous improvement of emotion recognition algorithms can reduce risks stemming from emotional bias.

5.5. Practical challenges and implementation pathways

Achieving effective human-AI collaboration is key to the success of intelligent interrogation. However, frontline officers' familiarity with AI technologies is currently limited, and system complexity can create initial barriers to adoption. This study recommends that police agencies strengthen technical training and establish incentive mechanisms to encourage officers to learn and adopt new technologies, enabling more effective AI-assisted interrogation.

Moreover, officers' acceptance and adaptability are critical factors in promoting AI technology. To address this, the study suggests a gradual rollout strategy, allowing officers to incrementally understand the system's benefits and improve operational proficiency through practical use. The system should also support personalized needs and user feedback, enhancing flexibility and adaptability to real-world investigative contexts.

6. Conclusion

Given the increasingly technological and organized nature of cross-border telecom fraud cases—and the higher education levels often found among perpetrators—traditional interrogation models are no longer sufficient to address such complex investigations effectively. AI-assisted interrogation systems offer significant potential in this context. During interrogations, such systems can capture suspects' physiological data in real time, analyze their roles in the criminal organization, and account for existing evidence to generate personalized interrogation plans. This can support investigators in devising more effective strategies, improving interrogation success rates, and enhancing social security and stability [7].

Of course, in practice, it is necessary to recognize and address the challenges arising from current institutional shortcomings, equipment limitations, and variability in technical personnel capabilities. Key unresolved issues include technical challenges in data collection, limitations in emotion recognition and algorithm performance, as well as legal and ethical concerns around data privacy, security, the balance of power in interrogations, and conflicts between different countries' legal systems. Additionally, on the operational side, challenges such as inadequate human–AI collaboration and limited willingness among police officers to adopt new technologies remain pressing problems that require focused solutions.

Against the backdrop of efforts to enhance the new-quality combat capabilities of the police and advance technology-driven policing, integrating artificial intelligence into critical stages of case handling represents a key step toward building a new operational model characterized by "online intelligence sharing, integrated and unified command, and precise coordinated action." Research on AI-powered intelligent interrogation for cross-border telecom fraud can help strengthen police work through technology, explore policing solutions that meet the needs of the new era, promote innovative tactics for prevention and control, and advance more scientific decision-making, flatter organizational structures, standardized law enforcement, and refined management [8].

Funding projects

Shanxi Province Preferential Funding Program for Scientific and Technological Activities of Returned Overseas Students (20240038); Shanxi Police College 2024 Undergraduate Innovation Training Program (2024XY39)

References

[1] Li, L., & Gong, Y. (2018). Analysis of the characteristics and countermeasures of telecom network fraud cases: Based on nationwide samples from 2014 to 2016. *Jingyue Journal*, (1), 78–90.

[2] Sun, F. (2024). Overseas telecom network fraud exhibits four characteristics such as clustering in industrial parks. *Supreme People's Procuratorate of China*. https: //www.spp.gov.cn/spp/zdgz/202407/t20240727_661702.shtml.

[3] Supreme People's Procuratorate. (2023). *Work report on prosecutorial efforts to combat and govern telecom network fraud and related crimes (2023): Lawfully punishing overseas fraud groups and promoting integrated cyber governance*. https://www.spp.gov.cn/xwfbh/wsfbt/202311/t20231130_635181.shtml.

[4] Zou, S. (2022). *Research on investigation of telecom network fraud crimes* [Master's thesis, Shenzhen University]. CNKI. https: //link.cnki.net/doi/10.27321/d.cnki.gszdu.2022.002082.

[5] Chen, Q. (2024). The path of AI empowering new-quality public security combat capacity. *Journal of Jiangsu Police Institute, 39*(4), 24–29.

[6] Hua, D., Chen, R., Tang, T., & Jiang, J. (2024). A brief analysis of the intelligent applications of Artificial General Intelligence (AGI) in modern policing. *Today's Science & Technology*, (5), 66–68.

[7] Cao, M. (2020). *Research on investigation and evidence collection in telecom fraud cases* [Master's thesis, Southwest University of Political Science and Law]. CNKI. https: //link.cnki.net/doi/10.27422/d.cnki.gxzfu.2020.000123.

[8] Cao, L., Gong, T., & He, M. (2025). Connotation and enhancement path of new-quality combat capacity in public security organs. *Journal of China People's Police University, 41*(1), 77–83+90.