Journal of Science, Innovation & Social Impact

Article

Multi-Dimensional Feature Analysis and Evaluation Methods for Anomalous Fund Flow Identification in Cross-Border Financial Transactions

Minju Zhong [1,*]

[1] Department of Analytics, University of Chicago, Chicago, United States
* Correspondence: Minju Zhong, Department of Analytics, University of Chicago, Chicago, United States

Abstract: Cross-border financial transactions are inherently complicated by the multi-currency nature of the transaction, the different regulatory systems, and the various methods used to launder dirty money; anomaly detection is not easy. The paper presents a comprehensive, multi-sided, and characteristic-based analysis framework for anomaly detection in cross-border fund transactions. Using this framework by taking characteristics of transactions, network topology features, and temporal behavior patterns into account, in order to boost detection. A systematic evaluation was conducted on 2.8M transactional data; a combination of graph-structure-based features and time-series behavioral indicators outperformed a single-dimensional approach. After experimentation, this strategy increased the baseline's accuracy by 18.7 percent and recall by 23.4 percent.

Keywords: Cross-border transactions; Anomaly detection; Feature engineering; Anti-money laundering

1. Introduction

1.1. Background and Significance of Cross-Border Financial Transaction Monitoring

Globalization of financial markets, the cross-border volume of transactions is on the rise, the international payment network every day from dozens of countries' millions of messages need to be processed. Transactions across different jurisdictions and currency exchange happened at the same time in different time zones, which formed a complicated ecosystem on which the legitimate businesses based for international trade and investment. Similarly, infrastructure deficiencies can bring it up to an illegal actor's attention to exploit regulatory loopholes and conduct money laundering jurisdictional arbitrage. Financial fraud detection becomes the hot research content, and the development speed of anomaly detection technology is much faster to solve the increasingly complicated and changeable fraudulent behavior [1].

The Cross-Border Trade transaction is more complexity than domestic payment because of above different reasons. Currency exchange added another point of data, exchange rate, exchange time, and use of middleman currency. Because of the geographical scattered of transaction endpoints so that we can't establish baseline behaviour profiles, because of the legitimate business models are so different in different places. Regulatory heterogeneity means that the detection systems need to adapt to different reporting threshold, compliance requirement and so on in different jurisdictions. More and more anti - money - laundering is utilizing deep - learning method by using graphs which is to catch the complicated relationship pattern of the transaction entities [2].

1.2. Limitations and Research Motivation of Traditional Detection Methods

The traditional rule-based detection systems is to use set thresholds, and the use of pattern matching algorithms works based on the detection of the pre-assigned, they are

Received: 05 February 2026
Revised: 17 March 2026
Accepted: 29 March 2026
Published: 01 April 2026

unable to adapt to the ever-changing pattern of criminal activity. These systems have high false positive rates in cross-border environment and increase the burden of operation, reducing the actual utility. Static rules are unable to depict the characteristics of complex money laundering techniques that are constantly changing, such as multiple jurisdictional layers, trade-related money laundering, and using proxy banks related to each other. Time series relationship analysis has also become another way of promising methods that can identify the time factor of the fraud pattern [3].

Machine learning method proves that with veto right to enhance cross border operation is effective, but there are still difficulties for its application in the across border. The extremely imbalanced category ratio of transaction data makes it difficult for standard classification algorithms to handle the extreme category imbalance when there are only several cases of fraudulent transactions out of tens of millions of cases. We special improve gradient boosting algorithm for resolving the financial data severely unbalanced issue [4]. Cross border transaction feature engineering need to acquire knowledge in the domain to capture important signal features from heterogeneous data distributed across different banks, payment networks and regulatory reports formats.

1.3. Research Objectives and Contributions

A way for researching into characteristics for Cross Border Transaction anomaly detection systems. To discover some overall features that contained transactions, network, times and locations, the influence of these different types of features we will call categories on detection ability and some practical guidance when only limited sources of information are available.

The main achievements of this project can be divided into three parts. The Structured framework places the Features in an order that is easily understood, and is lined up with the varieties of money launderers acknowledged by authorities. Empirical assessment quantitatively studies which features are more important in different detection algorithms to give evidence for practitioners. Solutions for data quality problems in the context of cross-border transactions, including missing values, noise, and category imbalance.

2. Related Work and Theoretical Foundation

2.1. Feature Engineering Techniques in Financial Anomaly Detection

Feature engineering is an important component of the financial fraud detection pipeline, and the quality of feature extraction directly affects the performance of the model. The early method relied on domain knowledge to manually establish functions, such as transaction amount, frequency, and counterparty relationships. The graph based anomaly detection method has been applied in banking transaction networks, using centrality metrics and community detection algorithms to identify suspicious account clusters, with an accuracy rate of over 89% in distinguishing money laundering patterns from legitimate business activities [5].

The evolution towards automatic feature learning incorporates representation learning techniques that extract potential features from raw transaction data. A neural model designed for directed multigraphs to solve the problem of heterogeneous edge types in financial networks, where various transaction types are connected to the same entity pairs using different payment channels [6]. These architectures can handle various types of transactions and achieve the best performance in the benchmark dataset for financial crime detection.

2.2. Transaction Monitoring Methods Based on Graph and Network Analysis

A trading network is a natural representation used to express the relationships between entities involved in fund transfers. The method of combining synthetic few oversampling and random forest algorithm performs well in severe class imbalance environments [7]. These methods can only solve fraudulent transactions, which generally account for only 1% of the total transaction volume, and cannot fundamentally solve the problem.

The deep learning methods used for cross-border transaction anomaly detection have shown some hope in capturing and avoiding complex patterns in rule-based systems [8]. Combining convolutional neural networks with attention mechanisms to automatically extract features from raw transaction sequences. Based on the spatiotemporal attention graph convolutional network combined with the correlation between geography and time in simulated transaction flows, the detection rate of collaborative money laundering schemes is improved [9].

2.3. Time Pattern Recognition in Sequential Transaction Data

Time analysis is the process of capturing the dynamic changes in behavior over time and adding additional information to static network features. The transaction sequence reflects the underlying business operation time pattern, and deviations from the established pattern can be used as abnormal indicators. The method of using training data that preserves the statistical characteristics of real transaction flows does not involve privacy issues, and the generation of real synthetic financial transactions has advanced research capabilities [10].

The processing of time characteristics varies according to different detection methods. The sliding window method summarizes transaction statistics at fixed time intervals to obtain features such as rolling average and standard deviation. The use of deep learning ensembles with data resampling techniques has been proven effective in capturing fraud detection time patterns by strategically sampling training data to address class imbalance issues [11].

3. Multi-Dimensional Feature Analysis Framework

3.1. Transactional Feature Extraction and Characterization

The basis of cross-border transaction analysis is to carry out all-round extraction of transaction features and grasp the basic features of cross jurisdictional fund transfer. According to the above, it can be divided into 5: an amount based feature, a frequency based feature, a counterparty feature, a geographic feature, and a currency conversion feature. Different kinds of anomaly recognition contribute to different kinds of anomaly recognition in transactions.

According to the feature of the amount, there are original transaction values and derivative statistics which describe the mode of transfer. This group of features contains single transaction amount, multiple time windows (daily, weekly, monthly), total, statistical measure of mean, median, standard deviation and percentile rank. Cross border transactions have different distribution characteristics compared to other domestic transfers, and international payments usually have larger average amounts and large differences. The ratio of incoming and outgoing amounts of each account is the balance flow indicator, which can reflect possible structural behavior.

According to the frequency to measure trading events' time density and regularity. Counts at what level of activity in different time windows of transactions; Time interval for when a person makes transactions reflects the pattern of behavior. The coefficient of variation of the transaction time can be seen that it is routine fixed payment or irregular temporary transfers. The sudden detection function can detect situations where the transaction frequency suddenly increases, such as account leaks or collaborative money laundering activities. The ratio of cross-border transaction frequency to domestic transaction frequency can obtain jurisdictional risk indicators related to risk assessment.

The counterparty characteristics describe the physical network that conducts transactions with the account. What is unique is that counterparty counting measures the breadth of a relationship, and the concentration of transactions between counterparties reflects the degree of dependence. The emergence rate of new counterparties detected is constantly expanding the trading network, which indicates that new money laundering relationships are forming. The geographical diversity and industry classification characteristics of counterparties provide a background for evaluating the legitimacy of

transactions. We are aware of the existence of high-risk counterparties or proxy banking chains and have introduced classified risk indicators (As shown in Table 1).

Table 1: Transactional Feature Categories and Extraction Methods

Category	Feature Examples	Extraction Method	Dimensionality
Amount-based	Transaction value, Rolling mean, Percentile rank	Statistical aggregation	12
Frequency-based	Transaction count, Inter-arrival time, Burst score	Temporal windowing	8
Counterparty	Unique count, Concentration ratio, New introduction rate	Network enumeration	10
Geographic	Country diversity, High-risk jurisdiction exposure	Categorical encoding	6
Currency	Conversion count, Currency diversity, Rate arbitrage	Currency pair analysis	8

Geographical features can reflect the spatial distribution of cross-border capital flows. The source country and destination country identifiers are categorical variables that can be encoded using either hot encoding or embedded encoding. The country risk ratings issued by the Financial Action Task Force (FATF) and other institutions provide ordinal risk indicators. The complexity index of transaction paths quantifies the number of jurisdictions involved in multi hop transfers. The geographic concentration index is used to measure the international activities of an account, which are concentrated in a certain region and widely carried out in different jurisdictions.

The currency exchange function can reflect the characteristics of cross-border multi currency transactions. The characteristics of account foreign exchange activities are the use of different amounts of currency, frequency of exchange, and typical exchange amounts. If it is found that the operation is carried out using intermediate currency instead of direct exchange, it indicates that the source of funds is intentionally concealed. Exchange rate timing analysis can identify all transactions made under favorable exchange rates, which may be suspected of insider information abuse. (As shown in Figure 1).

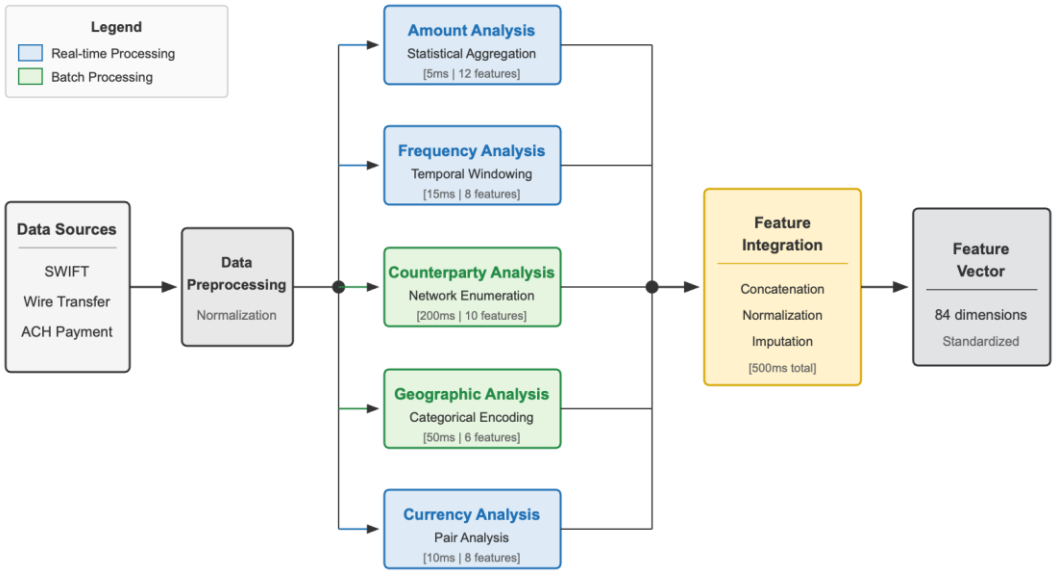

Figure 1: Multi-Dimensional Feature Extraction Pipeline Architecture

This figure shows a complete system architecture diagram, reflecting the cross-border transaction feature extraction pipeline. The figure shows a horizontal flow from left to right, starting from receiving raw transaction data from various source systems (SWIFT messages, wire transfers, ACH payments). There are five parallel processing streams branching out of the pipeline, each corresponding to a feature class name: amount analysis, frequency analysis, counterparty analysis, geographic analysis, and currency analysis. Each stream has a specific processing module with labeled transformation operations. After the flow is collected into the feature ensemble layer, a unified feature vector is obtained. Separate real-time stream features (blue) from batch computed aggregated features (green) using color coding. The processing delay annotation indicates the typical computation time of each module, with simple statistical features taking 5ms and complex network features taking approximately 500ms.

3.2. Network Topology Characteristics of Fund Flow Analysis

Graph based transaction network representation can extract structural features, capturing relationships that are not visible from a transaction record. Transaction diagram G=(V, E), where V represents accounts and E represents fund transfers between accounts. Edge attributes are encoded using transaction amount, timestamp, and classification metadata. This approach is beneficial for using network analysis techniques to discover suspicious structural patterns. Dynamic graph convolutional networks can update node representations in real-time and are used in streaming media environments to perform anomaly scoring on new transactions [12].

Node level centrality measures the importance and connectivity of accounts in a trading network. Degree centrality refers to the number of direct trading partners, which can be divided into two different situations: within degree (accepting) and outside degree (sending). The combination of high degree and low degree can represent the distribution accounts used in the hierarchical scheme. The centrality of the middle determines its role as a bridge between network regions, similar to the behavior of a money mule. For trading networks, PageRank scoring assigns weights to accounts based on the importance of trading partners, identifying influential nodes on the cash flow chain.

The betweenness centrality of node v in a directed transaction graph is calculated using the standard formula: BC (v)=v, the total number of shortest paths between all s and t in s! v=t of(sigma_st(v)/sigma_st), Where sigma_st is the number of shortest paths from

node s to node t, and sigma-s (v) is the number of paths taken through node v (As shown in Table 2).

Table 2: Network Centrality Feature Definitions and Interpretations

Feature	Formula	Interpretation	Anomaly Signal
In-degree	count of incoming edges	Receiving relationship count	Low value with high amounts
Out-degree	count of outgoing edges	Sending relationship count	High value indicates distribution
Betweenness	path intermediation ratio	Bridge position in network	High value suggests intermediary
PageRank	iterative importance score	Influence in transaction flow	Unusual value given profile
Clustering	neighbor connectivity ratio	Local network density	Low value indicates spanning

Discover account groups with close internal transactions and few external connections through community structure. The Louvain algorithm divides the transaction graph into several communities by optimizing modularity. Community affiliation is a classification feature used to determine the category of an account. Accounts that continue to conduct transactions across multiple communities or outside of the main community should be subject to increased scrutiny. The characteristics of community size and internal transaction density are used to describe the background structure of a single account.

Based on path feature analysis, use a trading network to track the path of fund flow. The minimum path length between accounts is the degree to which the topological structure of fund flow is similar. When funds are returned to the original account through the intermediary chain, the existence of the circular trading mode reflects a manifestation of the hierarchical structure. The spatiotemporal gating network captures the temporal and spatial information contained in multi hop transaction sequences by encoding them, effectively grasping the behavioral patterns of transactions based on paths [13] (As shown in Table 3).

Table 3: Network Structure Features for Anomaly Detection

Feature Type	Features	Complexity	Detection Target
Centrality	Degree, Betweenness, PageRank, Closeness	O(V + E) to O(V × E)	Hub accounts, Bridges
Community	Membership, Boundary ratio, Internal density	O(E log V)	Cluster anomalies
Path	Shortest path, Cycle detection, Flow concentration	O(V^2) to O(V^3)	Layering patterns
Subgraph	Motif counts, Clique participation	Exponential	Coordinated fraud

The temporal evolution of network characteristics refers to the process of changes in the structure of transaction relationships over time. The speed at which new edges are formed is used to determine whether the trading network is expanding or shrinking. Over time, changes in centrality indicators represent a shift in the position of roles within the cash flow ecosystem. The differences in network time provide discriminative signals for fraud detection and complement static structure analysis.

3.3. Time Behavior Characteristics and Abnormal Indicators

The temporal behavior characteristic is the time dependence that captures the transaction patterns that distinguish between normal business operations and suspicious activities. They play different roles in different time periods, and the characteristics of daytime will reflect the characteristics of the operating schedule. When there are seasonal changes in business or changes in relationships, there will be a trend of multiple months.

The timing characteristics of transactions are represented by the time at which transactions occur relative to various reference frames. The characteristic of the operating mode of one hour in a day and one day in a week is the potential abnormality of the historical standard deviation explanation. There is a time difference issue in cross-border transactions, and a predictable time pattern is established based on the business hours of the source and destination jurisdictions. Transactions conducted by two endpoints outside of normal working hours must undergo additional scrutiny. The fraud feature enhancement mechanism that amplifies irregular signals has been proven to improve detection performance [14].

The speed characteristic is to measure the rate of change in transaction activity from multiple perspectives. Reflecting changes in activity volume through transaction counting speed, and reflecting changes in transfer value through amount speed. The speed of the counterparty is used to measure the speed at which new relationships are formed. The sudden increase in speed is usually before fraudulent behavior occurs, as criminals have already accelerated their activities before the account is closed or discovered. The normalized anomaly score obtained by comparing the recent speed to the historical baseline can indicate the activity level of a certain account (As shown in Figure 2).

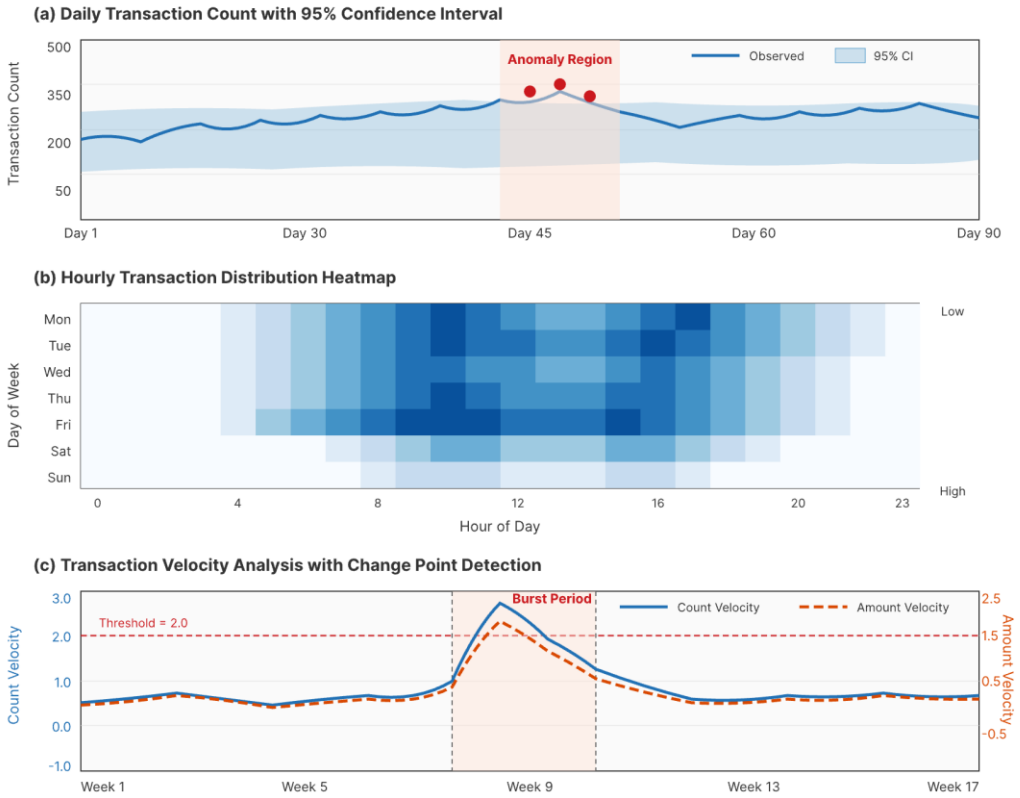

Figure 2. Temporal Pattern Analysis Visualization.

Use a multi panel time series chart to display the extraction results of the temporal characteristics of transaction data. The top panel shows the trading volume line chart and confidence interval for each chart over the past 90 days, with the width of the confidence interval determined by historical behavior. When the observed value is greater than the

upper or lower bound of the confidence interval, the abnormal period is highlighted in red. The middle panel uses a heatmap to represent the hourly trading volume for each time period of the week, with darker colors indicating higher trading frequency and reflecting operational patterns. The bottom panel uses a dual axis chart to represent the trends of trading volume velocity (blue curve on the left axis) and amount velocity (orange curve on the right axis) over time. Draw the abnormal change points with vertical dashed lines when the speed reaches the threshold, and provide specific explanations of abnormal events such as sudden trading periods and abnormal time patterns.

Behavioral baseline features are used to establish expected patterns when compared to current activities. The system calculates the transaction history characteristics of each account through a rolling window of historical activities, including typical transaction amounts, transaction frequencies, counterparty sets, and geographical distribution ranges. Deviation score evaluates the deviation between current transactions and historical baselines from multiple perspectives. Adopting denoising sampling method to achieve undersampling, that is, removing outliers from historical records, thereby improving the accuracy of baseline estimation [15]. For the transaction of amount a, its deviation evaluation is expressed by the formula $| a - \mu |/\sigma$, where μ is the historical mean and σ is the standard deviation.

Seasonal characteristics can reflect the cyclical patterns of transaction activities related to calendar events, economic cycles, or payment arrangements. The Fourier decomposition method is to perform Fourier transform on the time series of transactions to obtain the dominant frequency components for identifying periodic patterns. After removing seasonality, residual analysis can reveal abnormal activities that deviate from normal periodicity. The year-on-year analysis can provide a certain reference basis for evaluating whether the current model conforms to historical data of the same period. (As shown in Table 4).

Table 4: Temporal Feature Categories and Time Scales

Feature Category	Time Scale	Window Size	Update Frequency	Applications
Timing distribution	Intraday	24 hours	Daily	Business hours anomalies
Velocity metrics	Short-term	7 days	Daily	Burst detection
Baseline deviation	Medium-term	30 days	Weekly	Pattern change detection
Seasonality	Long-term	365 days	Monthly	Cyclical anomalies
Trend analysis	Multi-year	24 months	Quarterly	Relationship evolution

4. Comparative Evaluation of Detection Methods

4.1. Experimental Design and Evaluation Metrics

This experiment adopts a comprehensive methodology to systematically study the performance impact of various features on cross-border transaction anomaly detection. The evaluation framework consists of four main parts: dataset preparation, feature extraction, model training, and performance measurement, with the aim of generating reproducible and universally meaningful results.

There are approximately 280000 cross-border transaction records in the master data from January 2022 to December 2023. Originating from 47 representative countries, it

reflects regional distribution and the diversity and differences of various currencies among a total of 156 different currencies. There are 3847 records in the dataset that have been identified by regulatory authorities as suspicious transactions, with a positive classification rate of 0.137%. In this extreme category imbalance phenomenon, cross-border monitoring scenarios are truly present. In order to test how performance changes at various time stages, experiments were conducted on another secondary validation dataset containing a total of 4.2 million transaction records from January to June 2024.

Using the method presented in Section 3, a total of 84 candidate features were obtained, including 44 transaction features, 18 network features, and 22 time features. Using robust scaling methods to standardize feature values can effectively suppress the influence of outliers. For the data, which accounts for 8.3% of the total records and is mostly concentrated in the counterparty industry classification field and belongs to missing values, the practical filling method is to fill in the classification field with the "unknown" category or the most common value, fill in the numerical field with the median method, and add missing marker features if necessary. (As shown in Table 5).

Table 5: Dataset Characteristics and Class Distribution

Characteristic	Primary Dataset	Validation Dataset
Total transactions	2,800,000	420,000
Suspicious transactions	3,847	612
Positive class rate	0.137%	0.146%
Time period	Jan 2022 - Dec 2023	Jan 2024 - Jun 2024
Unique accounts	89,432	15,891
Countries involved	47	43
Currency pairs	156	128

Evaluation indicators can solve the problem of extreme category imbalance, which is a challenge encountered when evaluating detection performance. Accuracy measures the actual number of transactions marked as suspicious, which is related to the operational efficiency of alert investigations. Review the recognition rate of quantitative detection systems for suspicious transactions and reflect their coverage. The F1 score is the harmonic mean of precision and recall, balancing the contradiction between the two. The total area under the receiver operating characteristic curve (AUC-ROC) is used to evaluate all classification thresholds and obtain ranking performance. The area under the precise recall curve (AUC-PR) is used as a threshold independent evaluation metric, and in cases of severe category imbalance, it has more information than AUC-ROC.

We have adopted a time aware evaluation protocol to prevent information leakage of sequential transaction data. Using the main dataset (January 2022 December 2023) as the training set and the timeout prediction set (January June 2024) as the testing set. The hyperparameter optimization uses Bayesian search, with 50 iterations of configuration for each model, and AUC-PR is validated through segmentation during training to optimize.

4.2. Feature Importance Analysis and Selection Strategy

Feature importance analysis uses quantitative methods to measure the contribution of a feature and various feature categories to detection performance. Calculate various important metrics to provide robust support for evaluation: permutation importance, SHAP (Shapley Additive exPlans) value, and information gain ratio. The convergence discovery across methods further strengthens the conclusion on feature utility.

The quantification of permutation importance refers to the decrease in model performance when a single feature value is randomly permuted, thereby disrupting the relationship between the feature and the target. The permutation strength of network centrality features is the highest, with the first step of betweenness centrality being 0.089, the second step of PageRank being 0.072, and the third step of outdegree being 0.064. The

ratio of inflow and outflow amounts in the transaction characteristics is 0.058, and the speed of transaction times is 0.051. The characteristics of time deviation are baseline deviation (0.047), time and irregularity scores (0.043), which play a significant role in detection performance.

The SHAP value analysis yields the feature contribution patterns of each entity at the prediction level. The analysis results indicate that network features can provide powerful information for detecting collaborative fraud in several accounts, and time features are good at detecting changes in the behavior of an account. Transaction characteristics can serve as a baseline indicator for establishing account risk status, but cannot effectively distinguish between suspicious and legitimate large international transfers (As shown in Figure 3).

Figure 3. Feature Category Contribution Analysis.

This chart provides a comprehensive analysis of the importance of three feature categories and presents it in graphical form. The main image uses a grouped bar chart to display the importance (blue bar), Shap value importance (orange bar), and information gain importance (green bar) of the top 20 sorted features, with the average importance of each feature decreasing from high to low. Divide the features into three blocks based on vertical lines, namely transaction features (left), network features (middle), and time features (right). The error line is the standard deviation of cross validation for each fold. The lower auxiliary image uses a six axis radar chart to represent the comprehensive score of various anomaly detections, which are divided into layered anomalies, structural anomalies, sudden activity, circulation anomalies, new relationship anomalies, and temporal anomalies. The characteristics of transactions, networks, and time are represented by overlapping polygons with different colors, vividly depicting the features of various detection targets.

The feature selection experiment evaluates detection performance using all subsets of the complete feature set. Category ablation research is the process of training a model by excluding features of a particular category one by one, and measuring the degree of performance degradation caused by the features of that category. From the results, it can be seen that the AUC-PR metric has the best performance after removing the influence of network attributes (reducing by 12.4%, time features by 8.7%, and transaction features by

5.2%). Due to the redundant relationship between time and network, as well as the fact that network features already contain transaction information, removing time features has a relatively small impact on performance.

The sequential forward selection method can obtain the minimum feature subset that approaches the performance of the complete feature set. After screening, the number of features obtained is 23 (7 transaction features, 10 network features, 6 time features). After training the model with this subset, the AUC-PR value is 0.962, which retains 96.2% of the original feature set's AUC-PR value and has good dimensionality reduction effect. The selected features consist of two parts: clear network centrality indicators, time and amount distribution statistics. The results obtained by recursive feature elimination method are very consistent, with 18 out of the first 23 features appearing in the output results of both selection methods. The relationship between the number of features and detection performance is a feature curve, and when the number of features is greater than about 30, its benefits decrease..

4.3. Handling Data Imbalance and Noise in Cross-Border Transactions

The extreme category imbalance problem in cross-border transaction data, where the proportion of suspicious exchanges is only 0.137%, poses fundamental difficulties for anomaly detection. The standard classification algorithm values overall accuracy and simply categorizes all transactions as legitimate to achieve the goal. Special techniques must be used to make the model learn meaningful patterns from a small number of suspicious categories.

The sampling strategy is a method of solving the problem of class imbalance by changing the distribution of training data. Random undersampling is the process of randomly removing legitimate transactions to reduce the majority of class samples until a predetermined imbalance ratio is reached. Through experiments, it has been found that when the undersampling ratio is between 1:1 and 1:100, a ratio of approximately 1:20 can achieve the best results, ensuring both the representativeness of minority class samples and the diversity among the majority of classes. The Synthetic Minority oversampling technique (SMOTE) interpolates between existing suspicious samples to generate synthetic suspicious transactions. When combining SMOTE with integrated methods, its fraud detection performance is much better than using a single technique alone.

The cost sensitive learning method is to change the training objectives and impose greater penalties on misclassifications of minority classes than those of majority classes. Establish a scientific weight allocation scheme using category frequency and inversely proportional weights (wPositive=N/(2xNPositive), wNegative=N/(2xNNegative)). According to the experiment, while maintaining the same accuracy, using a random forest model with category weights can improve the recall rate, which is 14.3% higher than the original random forest model. The optimal cost ratio should be determined based on specific circumstances, and in cases where misjudgment leads to serious regulatory consequences, it is more reasonable to use strategies with higher costs.

Data quality, such as noise, missing values, and annotation uncertainty, greatly increases the difficulty of imbalanced learning. There are many measurement noises in cross-border transaction data, such as rounding errors in currency exchange, timestamp synchronization issues in different jurisdictions, and differences in bank identification of counterparties. The method of using median for statistics and Winsorization of mean for robust feature extraction can effectively reduce the impact of outliers and noise. When using deep learning methods for cross-border transaction anomaly detection, a noise aware training process is used to enhance the model's ability to resist external influences.

The integration method is to integrate several basic models to improve the performance and robustness of the entire detector. Random forest is the aggregation of decision tree prediction results trained on self-service samples to reduce variance and improve generalization ability. The gradient boosting algorithm uses residual error to perform successive fitting to improve the model, and places special emphasis on considering instances containing a few classes (difficult samples). Stacked ensemble

method is the combination of different types of tree based models, neural networks, linear models, etc., utilizing the advantages of each model. According to the experimental results, the AUC-PR value of the stacked ensemble model is 8.9% higher than that of the best single model, and the gradient boosting and neural network components contribute the most. The accuracy threshold is set to 0.15 (i.e. 15% of marked transactions are genuine suspicious transactions), and the optimized ensemble model yields a recall rate of 0.73. The offline validation set accurately detected 73% of suspicious transactions.

5. Discussion and Conclusions

5.1. Key Findings and Practical Implications

The experimental results show that the method of using multidimensional feature integration is much more efficient than using only one feature category. The greatest contribution of network topology features to this article is the discovery and layering of structural patterns related to schemes, currency mule networks, and collaborative fraud activities. The temporal behavior characteristics are supplemented by anomalies in individual accounts to supplement the temporal behavior characteristics obtained from network analysis. The transaction features have established a baseline risk overview, combining network and time signals.

Reducing 23 feature sets can result in a 96.2% improvement in the performance of the complete feature set. This discovery has significant practical implications. Under computational constraints, an effective detection system can be built using a focused feature extraction pipeline. Feature selection requires first selecting measures of network centrality, such as betweenness centrality PageRank、 Statistics based on speed based time indicators and quantity distribution. The marginal benefits of additional features beyond this core set cannot prove that the implementation complexity and computational overhead are reasonable.

The class imbalance handling strategy has a significant impact on detection in cross-border environments. Combining undersampling with cost sensitive ensemble learning at a ratio of 1:20 to obtain stable performance from different evaluation metrics. Practitioners should not use extreme undersampling rates, where all information is discarded, but should adopt balanced methods to ensure data diversity and integrity. The integrated approach is generally better than a single model, and the stacked architecture brings the greatest performance improvement.

5.2. Limitations and Challenges

Due to the limited generalizability of the research results, there are certain limitations. These datasets come from several or a specific financial institution in a region, and their performance characteristics may vary for institutions with different customer groups, products, or regulatory environments. The confirmed suspicious tags are part of the investigation results, which are inherently biased because not all actual money laundering activities are discovered and investigated.

Due to the limitations of privacy and data availability in cross-border transactions, the features extracted from cross-border transactions are not as diverse. The detailed counterparty information, beneficial owner information, and payment purpose fields in operational data are generally unavailable or incomplete, which can enhance detection. The network feature hypothesis proposed in this study can be utilized by multi-party transaction data that cannot be obtained by a single institution, thus requiring industry cooperation or regulatory data sharing mechanisms. Experienced money launderers will use adversarial adaptation to counter detection systems, making detection increasingly difficult.

5.3. Future Research Directions

One of the future research directions is to solve the real-time problem of cross-border transaction monitoring. The batch oriented feature extraction and model training methods used in this study should be suitable for streaming media environments, where

transactions must be scored within milliseconds of receipt. With the emergence of new things, incremental learning techniques that constantly update models have opened up a promising path for real-time deployment.

Privacy protection feature analysis is at the forefront of cross-border collaboration. Joint learning methods can train models across institutional boundaries without sharing raw transaction data, and can uncover network functionalities that are currently unavailable to an institution. The secure multi-party computing technology adds a function to privacy preserving feature extraction. Integrating the regulatory reporting framework (including requirements for suspicious activity reporting) provides a way to strengthen detection through feedback loops.

References

1. W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: A review of anomaly detection techniques and recent advances," Expert Systems with Applications, vol. 193, p. 116429, 2022.
2. D. Cheng, Y. Ye, S. Xiang, Z. Ma, Y. Zhang, and C. Jiang, "Anti-money laundering by group-aware deep graph learning," IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 12, pp. 12418-12431, 2023.
3. F. Xiao, Y. Chen, J. Zhang, J. Li, J. Liu, and Z. Zheng, "MINT: Detecting fraudulent behaviors from time-series relational data," Proceedings of the VLDB Endowment, vol. 16, no. 12, pp. 3610-3623, 2023.
4. X. Zhao, Y. Liu, and Q. Zhao, "Improved LightGBM for extremely imbalanced data and application to credit card fraud detection," IEEE Access, vol. 12, pp. 159316-159335, 2024.
5. B. Dumitrescu, A. Băltoiu, and Ș. Budulan, "Anomaly detection in graphs of bank transactions for anti-money laundering applications," IEEE Access, vol. 10, pp. 47699-47714, 2022.
6. R. Wu, B. Ma, H. Jin, W. Zhao, W. Wang, and T. Zhang, "GRANDE: A neural model over directed multigraphs with application to anti-money laundering," in 2022 IEEE International Conference on Data Mining (ICDM), 2022, pp. 558-567.
7. F. A. Ghaleb, F. Saeed, M. Al-Sarem, S. N. Qasem, and T. Al-Hadhrami, "Ensemble synthesized minority oversampling-based generative adversarial networks and random forest algorithm for credit card fraud detection," IEEE Access, vol. 11, pp. 89694-89710, 2023.
8. Q. Yu, Z. Xu, and Z. Ke, "Deep learning for cross-border transaction anomaly detection in anti-money laundering systems," in Proceedings of the 2024 6th International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI), 2024, pp. 244-248.
9. H. Huang, P. Wang, Z. Zhang, and Q. Zhao, "A spatio-temporal attention-based GCN for anti-money laundering transaction detection," in Advanced Data Mining and Applications (ADMA 2023), LNCS, vol. 14180, pp. 634-648, Springer, 2023.
10. E. Altman, J. Blanuša, L. Von Niederhäusern, B. Egressy, A. Anghel, and K. Atasu, "Realistic synthetic financial transactions for anti-money laundering models," Advances in Neural Information Processing Systems, vol. 36, pp. 58727-58740, 2024.
11. I. D. Mienye and Y. Sun, "A deep learning ensemble with data resampling for credit card fraud detection," IEEE Access, vol. 11, pp. 30628-30638, 2023.
12. T. Wei, B. Zeng, W. Guo, Z. Guo, S. Tu, and L. Xu, "A dynamic graph convolutional network for anti-money laundering," in International Conference on Intelligent Computing (ICIC 2023), LNCS, vol. 14090, pp. 493-502, Springer, 2023.
13. Y. Xie, S. Liu, G. Li, M. Chen, M. Li, and J. Yin, "A spatial-temporal gated network for credit card fraud detection by learning transactional representations," IEEE Transactions on Automation Science and Engineering, vol. 21, no. 4, pp. 6978-6991, 2024.
14. L. Ni, J. Li, H. Xu, X. Wang, and J. Zhang, "Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection," IEEE Transactions on Computational Social Systems, vol. 11, no. 2, pp. 1615-1630, 2024.
15. H. Zhu, M. Zhou, G. Liu, Y. Xie, S. Liu, and C. Guo, "NUS: Noisy-sample-removed undersampling scheme for imbalanced classification and application to credit card fraud detection," IEEE Transactions on Computational Social Systems, vol. 11, no. 2, pp. 1793-1804, 2024.