Enhancing Anti-Money Laundering Protocols: Employing Machine Learning to Minimise False Positives and Improve Operational Cost Efficiency

Jose Ricardo Oliveira
Master's Student in Applied Computing
IPT - Institute for Technological Research
Sao Paulo, SP, Brazil
jose.oliveira@ensino.ipt.br

Adriano Galindo Leal*
Artificial Intelligence and Analytics Department
IPT - Institute for Technological Research
Sao Paulo, SP, Brazil
leal@ipt.br

Abstract

Recent advancements in anti-money laundering (AML) strategies underscore the imperative for more accurate and efficient detection systems. This paper delineates a robust approach utilising machine learning (ML) and artificial intelligence (AI) to refine AML frameworks within national financial institutions, reducing false positive alerts. Integrating data from 'Know Your Customer' (KYC) initiatives with comprehensive transactional datasets, our methodology identifies high-risk transactions and complies with rigorous regulatory standards while curtailing operational costs. Through a comparative analysis of various ML models—including Decision Trees, Random Forest, Support Vector Machines, Logistic Regression, Artificial Neural Networks (ANN), and Convolutional Neural Networks (CNN)—we have identified that the Random Forest model notably decreased false positive rates to 2.1% and maintained an elevated detection rate for potentially illicit transactions. This model markedly surpasses traditional rule-based systems in performance, confirming its efficacy and suitability for broad implementation. By streamlining AML processes and diminishing compliance-related expenditures, this study presents a scalable and efficient model for financial institutions, optimising operational efficiency and fostering better cost-effectiveness in combating economic crimes. This analysis identifies the most effective models that balance detection accuracy with the need for explainability, an essential requirement for gaining trust from regulatory bodies and internal compliance teams. The findings of this study contribute to the field by offering a replicable and efficient AML framework that can safeguard financial institutions against regulatory penalties and reputational risks.

*Corresponding author.

ICAAI 2024, October 17–19, 2024, London, United Kingdom

ACM ISBN 979-8-4007-1801-4/24/10
https://doi.org/10.1145/3704137.3704156

CCS Concepts

• **Computing methodologies** → Modeling and simulation; Simulation evaluation; Machine learning; Learning paradigms; Supervised learning; Machine learning; Machine learning approaches; Classification and regression trees.

Keywords

Anti-Money Laundering, AML, Explainable AI, Machine Learning, Artificial Intelligence

ACM Reference Format:
Jose Ricardo Oliveira and Adriano Galindo Leal. 2024. Enhancing Anti-Money Laundering Protocols: Employing Machine Learning to Minimise False Positives and Improve Operational Cost Efficiency. In *2024 The 8th International Conference on Advances in Artificial Intelligence (ICAAI 2024), October 17–19, 2024, London, United Kingdom.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3704137.3704156

1 Introduction

The recent advancements in banking technology have made it possible to transfer large sums of money across borders and between banks in seconds. Thus, identifying and reporting transactions susceptible to money laundering is at the core of banking activities. A report from [1] estimated that the amount of money laundered in the global financial system accounts for 2.7% of the world's GDP. Correctly identifying potential money laundering and reporting it to the authorities has become a prominent issue in avoiding arrests and reputational damage to entities locally and globally.

As [2] stated, most banks rely on transaction selection for investigation based on rules. These rules are primarily simple criteria or limits created by compliance analysts, which result in many transactions being flagged for analysis. An excellent example of a rule would be selecting all fund withdrawals above a particular value. The problem with this approach is that the high number of false positives leads transaction review teams to spend days analyzing false alerts.

Given this scenario, with the prohibitive costs associated with analyzing erroneously selected transactions, searching for more effective models to select transactions closer to money laundering becomes essential for cost reduction and improving detection efficiency. Machine learning techniques for classification, such as Decision Trees, Random Forest, KNN, Naive Bayes, SVM, ANN, CNN, and transformers (not used here), among others, may improve AML performance.

One of the significant challenges in this classification is data imbalance. The number of alerts that are not false positives compared to regular transactions makes analyzing and applying learning models a complex issue. Additionally, attribute selection becomes an essential component of this analysis, as banks possess vast information about their customers regarding demographics and transactional data.

Another significant challenge regarding machine learning is explaining the details after training each algorithm. Compliance teams and regulatory bodies cannot trust something that is not understandable, and it becomes difficult to implement it.

Furthermore, data quality should not be overlooked. [3] states that data quality is crucial for applying sophisticated models, as emphasized by [4]. Banks do not always have the necessary data quality to use more sophisticated models, even with enormous volumes of data.

2 Literature review

2.1 Money Laundering Context

"Follow the Money" is a motto often cited in political and legal circles of various countries as a method to identify those responsible for illegal transactions. However, this is not always easy, especially considering today's digital world and the sophistication of participants in these transactions. Prohibited transactions can arise from various sources, with the most traditional being drug trafficking and organized crime. However, fraud, theft, human or animal trafficking, arms dealing, corruption, and sale of stolen art, human organs, and gold, among others, are also sources of funds that will be laundered in the financial market.

According to [5], with the development of the global economy, electronic transactions, and the Internet, it is predicted that the volume of money laundering will grow and become increasingly difficult to investigate. [1] states that estimating the financial volume obtained from illegal transactions is not simple. However, by gathering national and global information, $2.1 trillion was reached in 2009, approximately 3.6% of the worldwide GDP (with a 95% confidence interval between 2.7% and 4.4%). Of this amount, $1.6 trillion (2.7% of global GDP) was laundered within the financial market.

Therefore, finding ways to combat money laundering is crucial. For this reason, all market participants, whether regulators or participating entities such as banks, brokerage firms, insurance companies, among others, develop Anti-Money Laundering and Counter-Terrorist Financing programs. The regulator's role is to supervise and standardize, while participants have the role of detecting and communicating with the regulator.

Around the financial world, market participants' role in detecting suspicious transactions and communicating them to the regulator became evident. Developing an efficient detection program at a low cost is essential for any bank that does not want to expose its brand to a risk of image or its directors' imprisonment, spend large sums in the process, or face deep inspection from regulators.

2.2 Machine Learning to Detect Money Laundering

According to [6], models for detecting suspicious money laundering transactions are based on predefined rules (e.g., transaction patterns with predefined limits). According to the authors, the problem with this methodology is that it generates a considerable number of false positives, demonstrating the low efficiency of the method. [6] also state that this method presents two main limitations. Firstly, money launderers can easily understand the rules, which results in many false positives. Secondly, the rules are always based on the past and cannot adapt to new patterns.

[2] note that there are three significant deficiencies in computerized systems that detect money laundering: 1. Keeping the rules updated and relevant and deciding the weight of each one is a Sisyphean task. 2. Although rules can be derived from data analysis, they are typically too simple. 3. Reducing the number of false alerts is of primary importance.

Rule-based detection systems generate many false alerts, increasing transactions and increasingly sophisticated money laundering attempts require larger compliance teams and higher costs.

To avoid prohibited cost increments and even reduce them, several authors have proposed using Machine Learning (ML) or Artificial Intelligence (AI) techniques to detect potential money laundering transactions, as cited by [7]. However, the authors report that financial institutions have difficulties moving from the project model to the business-as-usual model, where models must be updated and maintained. Another point raised is trust, as models make automatic decisions.

[7] acknowledge that other issues related to organizations' use of Machine Learning (ML) and Artificial Intelligence (AI) techniques must be addressed. These include problems such as poor data quality, lack of knowledge for model development, using black box models that are not easily understood, and concerns around data privacy and security.

In addition to the above, local regulators have become deeply involved in the mechanisms and rules for detecting money laundering. Developing models that are not easily explainable to regulators is a challenge. Accordingly [8], despite the vast literature on applying machine learning to credit risk and fraud, the literature on detecting suspicious money laundering activity is limited, primarily due to the lack of public databases that can be used. They also report that obtaining money laundering cases in databases is complex and rare. To address this issue, they suggest mechanisms for increasing observations.

[9] propose a model exploring XGBoost, which compares it to other literature model suggestions like SVM, Random Forest, KNN, and Decision Tree, achieving better recall than others.

On the other hand, [6] proposes a more straightforward and well-known model, supervised Support Vector Machine (C-SVM), and one-class SVM for heterogeneous data. The advantage of SVM is that it is not sensitive to dimensional disorder. It can also be used as a density estimator or outlier identifier. Thus, SVM fits well in high-dimensional and heterogeneous data problems. [8] propose applying supervised models such as Decision Trees, Random

Forests, Support Vector Machine (SVM), and Artificial Neural Network (ANN). They used Maximum Likelihood Logistic Regression (MLLR) as a benchmark [10].

All the studies above conclude that using Machine Learning (ML) or Artificial Intelligence (AI) models has enormous potential in detecting money laundering alerts while minimizing the number of false alerts. The implementation challenge lies in the number of actual events, the data quality, and how to explain the algorithm easily to Compliance teams and regulators.

Considering all algorithm possibilities mentioned in the literature above, this study aims to compare some of them, such as KNN, Randon Forest, Decision Tree, Logistic Regression, and Naive Bayes on the Machine Learning spectrum and ANN, Autoencoder, and CNN on Artificial Intelligence spectrum.

Decision Trees were used for their simplicity and interpretability, making them ideal for regulatory compliance. Random Forest models, which are ensembles of Decision Trees, were chosen for their higher accuracy and robustness against overfitting, which is suitable for managing the complex and varied data typically involved in financial transactions. Logistic Regression was applied for its efficiency in binary classification tasks, making it well-suited for distinguishing between legitimate and illicit transactions. RNN and CNN models were included to compare with machine learning techniques as they can be more performative and accurate, even if they are not easily explained.

Furthermore, the selection of Random Forests leverages its high accuracy, robust handling of data variability, and inherent transparency, which aligns with the growing demand for explainable AI in regulatory environments.

Explainable AI (XAI) refers to methods and models that make the outputs of AI systems transparent and understandable to humans, ensuring that stakeholders can trace and understand the decision-making process. This characteristic is essential for meeting stringent compliance standards and maintaining trust with regulatory bodies and internal compliance teams. By employing XAI principles, Random Forests facilitates a more explicit justification of decisions, which is an asset when seeking regulatory approval and ensuring operational transparency.

Each model used in this work was chosen based on several strategic considerations. First, the need for transparency and explainability to compliance teams and regulatory bodies made Decision Trees a preferred choice; their decision-making process can be easily traced and understood, even by those without a technical background. Second, the accuracy and ability to oversee large datasets without significant performance drops led to the inclusion of Random Forest models, which effectively manage transaction data's variability and high dimensionality. Lastly, Logistic Regression was included for its proven history in financial applications, particularly its capacity to provide quick and reliable predictions essential for real-time transaction monitoring.

3 DATA SELECTION AND PREPARATION

3.1 Scenario diagnosis

The anonymized data provided for this study is from a medium-sized bank in the national market, operating in both retail and corporate banking sectors. The bank's rule-based detection system captures customer data from daily transactions and processes this information according to pre-established rules. The study was conducted to understand the bank's business model, products, customer types (individuals or legal entities), transaction volumes, and current rules for detecting potential money laundering transactions. The study presented here considered only individual customers.

Also, a meaningful definition emerged during this diagnostic stage: alerts generated are named Level One. During these alert analyses, there are two options: first, close the alert as a false alert (Closed at Level One), and second, move to a superior level to be analyzed by more experienced staff (Not Closed at Level One). Thus, the algorithm must identify, but not differentiate, these two different classes.

Based on this definition, the study aims to create models that analyze generated alerts but with additional data available in the institution. This choice was made to apply the algorithm after the current detection phase, automatically closing alerts, thereby minimizing manually reviewed transactions and, consequently, the costs associated with manual analysis.

Data capture proved costly during the Data Preparation stage due to incomplete and unstructured data. Four databases were identified: the Alert Database selected for Level One, the Customer Database, the Know Your Customer (KYC) Database, and the Database of Transactions made in the last six months. The database of transactions from the previous six months was not used due to its complexity, but it could be helpful for the model.

The alert database for the year 2020 contained 4,874 records, of which 1,525 were discarded due to lack of data quality. Some of these alerts did not have a corresponding client (closed clients), and some had missing data. Therefore, 3,259 alerts were used, concatenated with customer and KYC data. Among the 3,259 alerts used, 14.5% were closed at levels higher than Level One. Although the database was not perfectly balanced, these quantities could be modelled using specific techniques.

With the defined database, in the Modeling stage, five different Machine Learning algorithms were evaluated, namely Decision Tree, Random Forest, KNN, Naive Bayes, and Logistic Regression, and three AI algorithms ANN [8], ANN with Autoencoder for non-linear features [10] and CNN, to analyze the database and detect alerts that were closed at the first level and those that went to higher levels. Comparing the models is extremely important for the Money Laundering Detection process, as the algorithm needs to be easily explained to regulators.

As discussed in Section II, various sources report on using machine learning to identify money laundering transactions. [9] proposed the use of XGBoost, [6] analyzed the use of SVM, and [8] applied Artificial Neural Networks (ANN), Random Forests, Decision Trees, and Support Vector Machines (SVM).

As mentioned earlier, this study used some of the models recommended by the literature, which can be explained to regulators. However, as the idea is to perform alert analysis post-generation, other techniques were employed, and some were discarded to analyze their efficiency.

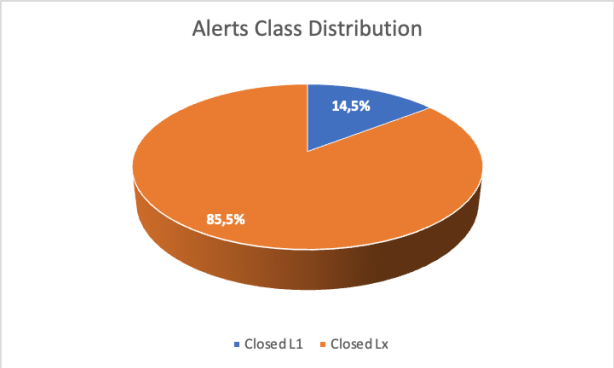

Figure 1: Alerts Class Percentage Distribution. (Author)

3.2 Data analysis, cleaning, and preparation

The data received for analysis was divided into three databases, as mentioned in section III.A. Together, they held 128 attributes, some redundant and some irrelevant for the study according to the analysis of the problem to be addressed.

After cross-referencing the databases and removing irrelevant and redundant attributes, the Alerts Database to be analyzed consisted of 68 attributes related to alerts from individual customers. These attributes were divided into Alert Selection Criteria, Occupation, Gender, Marital Status, Relationship Duration, Financial Capacity, Alerts in the Last 6 Months, PEP Indicator, Customer Risk, Customer Blocks, Customer Industry, and Country of Residence, among others.

As mentioned in section III.A, many records had missing data, and the solution was to remove them from the study. The missing data occurred because the alerts considered the entire database, and the customer and Know Your Customer (KYC) databases were filtered for active clients only. Therefore, cleaning the alerts from inactive clients (terminated relationships) was necessary. This strategy can be questioned because terminated clients may provide information for the model.

However, because behavior patterns of this type of crime change often, the goal is to work on alerts generated by current clients; these additional records could introduce an unwanted bias into the model. Therefore, the Alerts database for the study had 3,259 records with 68 attributes, with 2,758 records labelled as finalized at Level One and 474 finalized at higher levels, as shown in Fig. 1.

It is essential to remember that using imbalanced datasets can generate a classification bias in the machine learning model, favoring the majority class. To reduce/avoid this bias, the data used in training the model underwent Oversampling using the [11].

The database attributes provided as descriptors (e.g., Gender: Male or Female) underwent preprocessing to make them interpretable by machine learning methods. Several columns, using the one-hot-encoding method (Country of Residence, Gender, Marital Status, among others), were transformed into N additional columns in the database. Numerical attributes such as assets and balances, among others, were discretized and converted into six levels to standardize them before one-hot encoding.

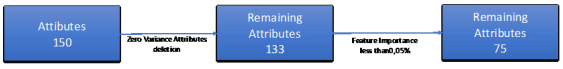

Figure 2: Alerts Class Percentage Distribution. (Author)

After processing, the number of attributes for each record increased from 68 to 150, which is a reasonable computational cost, especially considering a more extensive database.

3.3 Dimension reduction

Two-dimensional reduction techniques were used to reduce computational costs, as shown in Fig. 2

The first procedure used was to remove attributes with zero variance because they do not contribute to class separation in machine learning algorithms. Another method involved Feature Selection using the Extra Tree Classifier from the Sklearn library. This classifier calculates the Gini Importance Index for each attribute, and based on this index, we selected only the attributes with an indicator above 0.05%. Finally, the dataset used for training and testing ML algorithms shown in Table 1 ended up with 75 attributes and 3,259 records.

4 RESULTS DISCUSSION

The dataset was split into 80% for training and 20% for evaluating the models. Additionally, the Principal Component Analysis (PCA) technique increased the model's efficiency by focusing the analysis only on the main components. Another factor to consider in the results is the confidence factor in an algorithm's class assignment.

This factor was set to 95% in all ML algorithms used. However, when assigning confidence indexes, a question arises: What should be done with the records that do not have the confidence index to be Class 0 (alerts overseen at higher levels or manually) or Class 1 (alerts that are closed on Level One)? In the case of the study below, a Class 2 was created, which we called uncertainty.

Since the study deals with Money Laundering and, in this case, we always need to be on the side of caution, Class 2 was considered Class 0, thus being added to the Class that should be manually treated at Level One as it has chances of escalating to a higher level. The results for the True Positive Rate (Recall - TPR), False Positive Rate (Probability of False Alarm - FPR), False Omission Rate (FOR), Precision (PPV), and Accuracy (ACC) are shown Table 1.

All models performed better than the randomness line except Naive Bayes with PCA, which already demonstrates the excellent capability of the tested models. However, with a simple analysis, we noticed that ANN, CNN, Naive Bayes, and Autoencoder exhibit a Probability of False Alarm (FPR) greater than 40% and appear unfeasible, even though they have a TPR above 75%. In this case, the FPR makes it unviable since we are dealing with identifying money laundering alerts, even considering that ANN and CNN have lower false omission rates (FOR). These numbers may also suggest overfitting of the model, adapting to the training data.

Using a ROC curve, as illustrated in Figure 3, makes examining each algorithm's performance easier. ROC curves enable us to evaluate each technique's TPR and FPR.

Table 1: CONFUSION MATRIX METRICS FOR EACH ALGORITHM

Models	TPR	FPR	FOR	PPV	ACC
KNN	0,975	0,114	0,141	0,981	0,962
ANN	0,975	0,748	0,082	0,536	0,592
CNN	0,971	0,621	0,131	0,757	0,774
Decision Tree entropy	0,946	0,061	0,253	0,989	0,945
Decision Tree Gini	0,940	0,061	0,253	0,988	0,940
ANN + Autoencoder	0,856	0,333	0,992	0,999	0,855
Random Forest	0,853	0,021	0,469	0,996	0,871
Decision Tree Gini - 10 Levels	0,787	0,046	0,567	0,990	0,811
Naive Bayes	0,763	0,390	0,695	0,920	0,741
Logistic Regression com PCA	0,520	0,424	0,830	0,878	0,528
Logistic Regression	0,162	0,021	0,834	0,978	0,280
Naive Bayes com PCA	0,119	0,141	0,858	0,832	0,226

Figure 3: ROC Chart – Recall (TPR) x Probability of False Alarm (FPR). (Author)

The logistic regression model with PCA still shows a highly prohibitive false positive rate of above 40% and a high false omission rate of 83% but with a lower true positive rate.

Random Forest had a false positive rate of 2.1%, lower than the algorithms mentioned, and a true positive rate of 85,3%, demonstrating that the technique best combines TPR and FPR rates. Random Forest is well-known as a good technique for its higher accuracy and robustness against overfitting. It could be the best choice, but the false omission rate of 46,9% makes it not a good option, as it will close alerts that should be analyzed at higher levels.

Decision Tree Gini or Entropy, Decision Tree with 10 Levels, and KNN models present a much more reasonable false positive rate than all other models and are excellent candidates for implementation, considering they are easily explained. KNN has a higher true positive rate and a lower false omission rate. However, considering that KNN is sensitive to oversampling techniques, it could not be a desirable choice and may be implemented carefully. Also, it is not easy to explain to regulators.

Among the three Decision Trees, the 10-level model has the best positive predictive value (PPV), and best false positive rate (FPR) achieved after 50 level tests, but it fails with a false omission rate of 56,7%.

The confusion metrics between the Gini and Entropy Decision Trees are almost identical. Both presented more than 94% of the true positive rate and just 6,1% of the false positive rate. Considering the false omission rate of 25,3%, a positive predictive rate (PPV) above 98%, and accuracy above 94%, Decision Trees demonstrate the best algorithm among the others. On top of that, Decision Trees are easy to explain to Compliance teams and regulators, which brings another positive point to the algorithm.

Since we are dealing with money laundering, the FPR and FOR of these algorithms are critical. Involving any bank in such a case can permanently damage its reputation and heavy fines from local and international regulators.

5 CONCLUSION

National banks have traditionally relied on rule-based systems for their anti-money laundering (AML) initiatives in the challenging sphere of global finance. While these systems are dependable, they are often hampered by high operational costs and a notable incidence of false positives.

Our comprehensive investigation reveals that integrating machine learning algorithms, notably Decision Trees, Random Forests, and KNN, significantly enhances these systems. By automating the differentiation between alerts that can be closed at Level One and other alerts, these models drastically reduce the analytical burden on staff and decrease operational expenses while maintaining strict risk management standards.

Our analysis highlights the practicality of Decision Trees, which perform robustly and promote transparency, aligning with the principles of explainable AI. This transparency makes them more suited for regulatory approval and internal compliance than their more complex counterparts.

Transitioning from traditional rule-based frameworks to those supported by machine learning requires meticulous planning and continuous dialogue with regulatory bodies to ensure that advanced tools are seamlessly integrated within existing regulatory frameworks. The application of explainable AI techniques ensures these models are not only practical but also understandable, which fosters trust and eases compliance processes.

As financial transactions and criminal methodologies evolve, AML systems must be regularly reviewed and updated to preserve their relevance and efficacy. This initiative-taking approach establishes a new standard in the efficiency and effectiveness of anti-money laundering technologies.

In conclusion, this investigation not only confirms the significant potential of machine learning to enhance AML strategies but also lays the foundation for future research into the adaptability of these technologies across varied financial platforms. The ongoing evolution and refinement of these technologies are vital for maintaining the security and integrity of financial institutions worldwide.

Future research should explore the use of advanced Transformer models, known for their exceptional ability to capture temporal dependencies and nuanced patterns. These models could be uniquely effective in detecting coordinated, small-value transactions intended to elude traditional detection methods, which sophisticated criminal networks increasingly use. Integrating such innovative technologies will augment the predictive capabilities of our systems, enabling them to identify isolated incidents and complex, distributed schemes over time. Implementing these models will necessitate careful adjustments to the financial domain, including creating customized training datasets that accurately represent the sequential nature of monetary transactions and the strategic behaviors of money launderers. This forward-looking strategy promises to redefine the benchmarks for efficiency and effectiveness in anti-money laundering technologies, potentially revolutionizing how financial institutions protect against illegal activities.

Acknowledgments

We extend our heartfelt thanks to support from IPT (Institute for Technological Research) and São Paulo Research Foundation (FAPESP) Grant Numbers #2019/01664-6, #2020/09850-0.

The authors would like to express their most profound gratitude and appreciation to Anderson Ribeiro Correia, Liedi Legi Bariani Bernucci, Fabricio Araujo Mirandola, Maria Cristina Machado Domingues, Denis Bruno Virissimo, Alessandro Santiago dos Santos, Silvia Elisabete Ferrari, Ester Garcia Ferreira da Silva, Itanna Caroline Mota de Oliveira, Janaina Galindo Leal, Terezinha Rosaboni, Maria Aparecida Leal, Pedro & Dirce Chinelato and Ana Paula Xavier da Silveira.

While preparing and revising this manuscript, we used MS Word 365, ChatGPT-4o, Grammarly, and Google Translate to ensure clarity and grammatical precision, as English is our second language. The authors assume full responsibility for creating the primary content and ensuring technical accuracy, and they have appropriately cited all secondary sources used in this publication.

References

[1] T. Pietschmann, J. R. Walker, U. N. O. on Drugs and Crime, Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: Research Report, United Nations Office of Drugs and Crime, 2011.

[2] M. Jullum, A. Løland, R. B. Huseby, G. Ånonsen and J. Lorentzen, "Detecting money laundering transactions with machine learning," *Journal of Money Laundering Control*, vol. 23, p. 173–186, January 2020.

[3] A. Gupta, D. N. Dwivedi, J. Shah and A. Jain, "Data quality issues leading to sub optimal machine learning for money laundering models," *Journal of Money Laundering Control*, vol. 25, no. 3, pp. 551–555, jan 2022.

[4] S. Wang, Y. Dai, J. Shen and J. Xuan, "Research on expansion and classification of imbalanced data based on SMOTE algorithm," *Scientific Reports*, vol. 11, p. 24039, 2021.

[5] Z. Zhang, J. Salerno and P. Yu, "Applying data mining in investigating money laundering crimes," in *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, 2003.

[6] J. Tang and J. Yin, "Developing an intelligent data discriminating system of anti-money laundering based on SVM," in *2005 International Conference on Machine Learning and Cybernetics*, 2005.

[7] R. Al-Shabandar, G. Lightbody, F. Browne, J. Liu, H. Wang and H. Zheng, "The Application of Artificial Intelligence in Financial Compliance Management," in *Proceedings of the 2019 International Conference on Artificial Intelligence and Advanced Manufacturing*, New York, NY, USA, 2019.

[8] Y. Zhang and P. Trubey, "Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection," *Computational Economics*, vol. 54, p. 1043–1063, 2019.

[9] A. N. Bakry, A. S. Alsharkawy, M. S. Farag and K. R. Raslan, "Automatic suppression of false positive alerts in anti-money laundering systems using machine learning," *The Journal of Supercomputing*, vol. 80, no. 5, pp. 6264–6284, 2024.

[10] D. Charte, F. Charte, S. García, M. J. del Jesus and F. Herrera, "A practical tutorial on autoencoders for nonlinear feature fusion: Taxonomy, models, software and guidelines," *Information Fusion*, vol. 44, pp. 78-96, 2018.

[11] Y. Bao and S. Yang, "Two Novel SMOTE Methods for Solving Imbalanced Classification Problems," *IEEE Access*, vol. 11, pp. 5816-5823, 2023.