融合序列訊息與圖結構之反洗錢異常行爲分析
Integrating Sequential Information and Graph Structures for Anti-Money Laundering Anomaly Detection

Yin-Ju Wu[1], Gavin Tseng[2], Berlin Chen[1]
[1]National Taiwan Normal University
[2]VIS Experimental High School
[1]{61247075s, berlin}@ntnu.edu.tw
[2]cheetahbooked@gmail.com

摘要

反洗錢 (Anti-Money Laundering, AML) 是金融科技領域的重要研究課題，其目標在於識別潛在的可疑帳户與交易。然而隨著跨境支付與新型態交易的興起，洗錢行爲往往具有高度隱匿性與複雜的網路結構，傳統規則式方法在偵測效能與泛化能力上皆表現不足。近年來，雖然有研究嘗試將機器學習或深度學習方法應用於 AML，但仍存在許多挑戰。爲了解決這些問題，本研究提出一個基於序列圖融合的 AML 帳户風險預測框架。該方法的核心在於同時建模帳户的個體時序行爲與其在交易網路中的結構特徵。首先，將每個帳户的交易歷史分解爲入邊和出邊序列，使用雙分支 GRU 架構分別編碼，捕捉帳户的時序交易模式，接著使用雙向注意力圖卷積層，通過差異感知的消息傳遞機制同時處理正向和反向鄰居關係，學習帳户間的行爲差異，並通過注意力機制自適應融合節點自身特徵與雙向鄰居聚合特徵。此外，針對 AML 資料集的極度不平衡特性，引入類別重加權與平衡採樣策略。我們在公開的反洗錢資料集上驗證所提方法，實驗結果顯示該框架在極度不平衡的情境下能取得穩定的 F1 表現，相較於傳統基線方法具有顯著優勢。

Abstract

Anti-Money Laundering (AML) is a critical research area in Financial Technology (FinTech) focused on detecting suspicious financial activity. However, the rise of new transaction types has led to increasingly subtle and complex money laundering schemes, rendering traditional rule-based methods inadequate for both detection and generalization. While machine learning and deep learning offer a promising alternative, there are still many challenges. To address these challenges, we propose an AML prediction framework based on sequence-graph fusion. Its core innovation is the joint modeling of an account's individual temporal behavior and its structural features within the transaction network. Our approach begins by decomposing each account's transaction history into incoming and outgoing sequences, which are encoded via a dual-branch Gated Recurrent Unit (GRU) to capture nuanced temporal patterns. We then utilize a bidirectional attention-based graph convolutional layer that employs a difference-aware message-passing mechanism to process relationships in both forward and backward directions, learning the behavioral contrasts between connected accounts. Through the attention mechanism, the model adaptively fuses each node's intrinsic features with the aggregated features from both forward and backward neighbors. To counteract the extreme class imbalance inherent in AML data, our framework incorporates class re-weighting and balanced sampling strategies. We validated our proposed method on a public AML dataset. The experimental results demonstrate that our approach achieves stable F1-scores under severely imbalanced datasets, significantly outperforming traditional baseline methods.

關鍵字：反洗錢 (AML)；圖卷積網路；金融詐欺偵測

Keywords: Anti-Money Laundering (AML); Graph Convolutional Network; Financial Fraud Detection

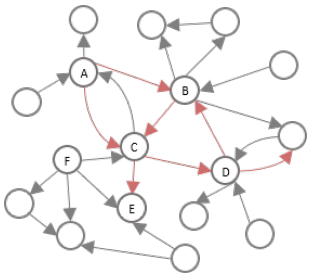
1 前言

在全球化金融體系快速發展的今日，反洗錢（Anti-Money Laundering, AML）已成爲金融監管與資訊科技研究的核心議題之一。根據國際洗錢防制組織（Financial Action Task Force, FATF）發布的指引與統計報告顯示洗錢活動對全球金融體系和經濟造成重大威脅 (Financial Action Task Force, 2010)，並且會影響國

Proceedings of the 37th Conference on Computational Linguistics and Speech Processing (ROCLING 2025), pages 320–325

Time-stamp	From Bank	Account	To Bank	Account	Amount Received	Receiving Currency	Amount Paid	Payment Currency	Payment Format	Is Laundering
2022/9/1 12:20:00	1	A	1	B	1000	USD	1000	USD	Credit Card	1
2022/9/1 12:22:00	1	A	3	C	2500	USD	2500	USD	Credit Card	1
2022/9/1 12:35:00	1	B	3	C	1200	USD	1200	USD	Credit Card	1
⋮										
2022/9/7 16:31:17	2	D	1	B	900	USD	900	USD	ACH	0

(a) 原始交易資料結構



(b) 轉換後的圖結構

Figure 1: 表格數據到圖結構的轉換

家的聲譽和金融系統的穩定性，更與跨國犯罪、毒品走私等高度相關。傳統的 AML 系統多依賴規則式方法 (Chen et al., 2018)，例如金額閾值檢測、異常交易模式識別與黑名單比對。然而，這些方法在面對日益複雜的交易網路與高隱匿性的洗錢手法時，往往面臨準確率不足與誤報率偏高的問題。

近年來，圖神經網路（Graph Neural Networks, GNNs）的崛起爲 AML 提供了新的解決思路 (Weber et al., 2019)(Johannessen and Jullum, 2023)。金融交易可以建模爲圖結構：帳户可視爲節點，交易可視爲邊，而交易金額、幣別與時間戳等屬性則成爲邊的特徵。透過圖建模方法，我們能捕捉到帳户間的交互關係與交易模式，並利用 GNN 進行節點分類，進而識別潛在的高風險帳户。這種方法具有兩大優勢：能從資料中自動學習複雜的異常行爲特徵，而不僅依靠人工設計的規則；能透過鄰居關係與結構訊息，偵測到更隱晦的洗錢模式，例如環狀交易或跨境分散匯款。

然而，單純的圖結構訊息仍不足以涵蓋洗錢行爲的全部特徵 (Tariq and Hassani, 2025)。許多可疑帳户的異常往往表現在交易時間序列上，例如短時間內進行多筆分散轉帳，或在固定週期內重複出現可疑資金流。若忽略時間維度，僅依靠靜態圖特徵，很可能無法正確區分正常高頻使用者與眞正從事非法活動的帳户 (Ghimire, 2023)。爲了同時捕捉交易的時序特徵與網路結構特徵，序列圖融合的建模思路逐漸受到關注 (Egressy et al., 2024)。這類方法最早在加密貨幣異常檢測領域得到成功應用 (Ding et al., 2024)，展現出結合時序行爲分析與圖結構學習的優勢。受此啓發，我們提出了一個專門針對 AML 任務的序列與圖融合框架，系統性地整合帳户時序行爲建模與交易網路結構分析，以實現更精確的異常帳户識別。

首先，我們將其交易歷史按方向性分解爲入邊序列和出邊序列，分別使用 GRU 編碼器學習其隱含的時序模式。這種設計能夠區分帳户的「資金流入」和「資金流出」的行爲特徵，對於識別不同類型的洗錢角色具有重要意義。其次，我們提出了雙向圖卷積層，專門處理有向交易圖中的複雜鄰居關係。與傳統圖卷積僅考慮無向鄰居不同 (Kipf and Welling, 2017)，我們的方法同時聚合正向鄰居（帳户指向的節點）和反向鄰居（指向該帳户的節點）的資訊 (Rossi et al., 2023)，並採用差異感知的消息函數，同時編碼節點間的行爲差異和鄰居原始特徵。這種設計使模型能夠學習到帳户間行爲模式的相似性和差異性 (Pahng and Hormoz, 2025)，進而識別異常的交易關係。

爲了解決 AML 資料中普遍存在的極度類別不平衡問題，我們採用了多重策略：包括基於類別頻率的加權損失函數、過採樣技術 (Chawla et al., 2002) 以及平衡採樣策略，確保模型能夠有效學習稀有的異常模式。本研究使用公開的大規模模擬 AML 資料集進行實驗驗證。該資料集專爲研究反洗錢與交易異常偵測而設計，包含多種已標註的洗錢模式，能夠模擬眞實金融網路中的轉帳行爲。實驗結果表明，我們提出的序列圖融合框架在多個評估指標上均優於傳統基線方法，特別是在極度不平衡的測試場景下仍能保持穩定的性能表現。

綜合而言，本文提出包括：(1) 一個序列與圖融合框架，在 AML 場景中系統性地結合了帳户時序行爲建模與網路結構分析；(2) 設計了雙向圖卷積層與差異感知消息傳遞機制，有效捕捉有向金融網路中的複雜鄰居關係；(3) 引入自適應特徵融合策略，通過注意力機制動態整合多源特徵。

2 方法

本研究採用圖結構的方法對金融交易網路進行建模，將複雜的資金流動關係轉換爲圖結構，以便後續的深度學習分析。

2.1 資料處理

原始 AML 資料集以關聯式表格形式儲存，每筆交易記錄包含時間戳、來源帳户、目標帳户、交易金額、幣別等基本屬性。爲了充分利用交易網路的拓撲特性，我們將表格數據(如 Figure 1(a)) 轉換爲有向多重圖 (如 Figure 1(b)) 表示：帳户作爲節點，交易作爲邊，交易屬性作爲邊特徵。

考量到反洗錢研究的核心挑戰之一是避免未來資訊洩漏，我們在資料集的切割上採取時間導向分割的策略，而非隨機分割。遵循原始資料集的建議 (Altman, 2019)，我們將資料按 60%/20%/20% 的比例分割爲訓練集、驗證集和測試集，確保分割過程遵循時間順序原則。這種分割方式不僅符合實際金融監控場景的時序性要求，也確保了實驗結果的可重現性和實用性。

2.2 模型架構

我們的學習框架採用序列和圖融合的設計理念(如 Figure 2)。對於交易圖中的每個帳户節點 v_i，我們首先將節點 i 的交易行爲分解爲入邊序列 S_i^{in} 和出邊序列 S_i^{out}：

$$S_i^{in} = \{t_1^{in}, t_2^{in}, ..., t_{m_i}^{in}\} \quad (1)$$

$$S_i^{out} = \{t_1^{out}, t_2^{out}, ..., t_{n_i}^{out}\} \quad (2)$$

其中每個交易 t_j 包含時間戳、金額、幣別等多維特徵。序列編碼採用雙分支 GRU 架構，分別處理入邊和出邊序列：

$$h_i^{in} = \text{GRU}_{in}(S_i^{in}) \quad (3)$$

$$h_i^{out} = \text{GRU}_{out}(S_i^{out}) \quad (4)$$

根據聚合策略，提取序列的最終表示：

$$x_i = \text{Concat}(h_i^{in}[-1], h_i^{out}[-1]) \quad (5)$$

此設計使得每個節點的特徵包含了該帳户完整的時序交易行爲資訊。

架構中使用的雙向圖卷積層能夠同時處理有向交易圖中的正向和反向資訊流。首先對所有節點的序列編碼特徵進行線性變換，接著對於每個節點 v_i，通過兩個獨立的消息傳遞過程聚合鄰居的序列編碼特徵：

$$h_i^{fwd} = \text{Propagate}(E, X) \quad (6)$$

$$h_i^{bwd} = \text{Propagate}(E^{-1}, X) \quad (7)$$

其中 $X = \{x_1, x_2, ..., x_N\}$ 爲所有節點的序列編碼特徵矩陣，E 爲原始有向邊集合（對應於帳户的出邊鄰居關係），E^{-1} 則爲反向邊集合（對應於帳户的入邊鄰居關係）。這種雙向傳播機制能夠分別聚合來自不同方向鄰居的行爲資訊。訊息傳遞的核心在於差異感知的訊息函數：

$$\text{m}(x_i, x_j) = \text{Linear}(\text{Concat}(x_i - x_j, x_j)) \quad (8)$$

這種訊息函數同時捕捉節點間的差異特徵（$x_i - x_j$）和鄰居原始特徵（x_j），使模型能夠學習到節點之間行爲模式的相似性和差異性。在每個圖卷積層內部，節點表示通過注意力機制融合三種特徵，自適應地權衡當前節點特徵與正向、反向鄰居特徵的重要性：

$$z_i = \text{Attention}([x_i, h_i^{fwd}, h_i^{bwd}]) \quad (9)$$

我們堆疊兩層這樣的雙向注意力圖卷積層以捕捉多跳鄰居關係，每層之間使用 ReLU 激活、批量正規化和 Dropout 正則，最終通過多層感知器解碼器進行二元分類。

我們的方法通過序列增強的圖表示學習，使圖卷積能夠處理包含完整交易歷史的豐富序列編碼。差異感知的消息傳遞機制同時編碼節點間的行爲差異和鄰居資訊，增強了異常模式的識別能力。雙向資訊聚合分別處理正向和反向邊，有效捕捉有向金融網絡的方向性特徵。此外，自適應特徵融合通過注意力機制動態權衡自身特徵與不同方向鄰居特徵的重要性。這種設計使得模型能夠同時利用帳户的個體時序行爲特徵和網絡中鄰居的行爲模式差異，實現對複雜洗錢行爲的精準識別。

3 實驗設置

3.1 資料集

我們採用了 (Altman et al., 2023) 開發的大規模合成 AML 資料集。該資料集通過虛擬世界中的個人、公司和銀行互動模型，生成了包含多種已標註洗錢模式的眞實交易資料，能夠模擬眞實金融網路中的轉帳行爲。資料集包含兩種版本：HI 與 LI。前者的非法交易比例較高，適合用於訓練與初步驗證；後者的非法比例較低，更貼近眞實銀行場景中高度不平衡的分布特性。

在本研究中，我們聚焦於 Small 資料集進行實驗驗證。如 Table 1 所示，Small 子集包含 HI-Small（515K 帳户，5M 筆交易）和 LI-Small（705K 帳户，7M 筆交易），涵蓋時間跨度爲 10 天。這一規模既能有效檢驗模型

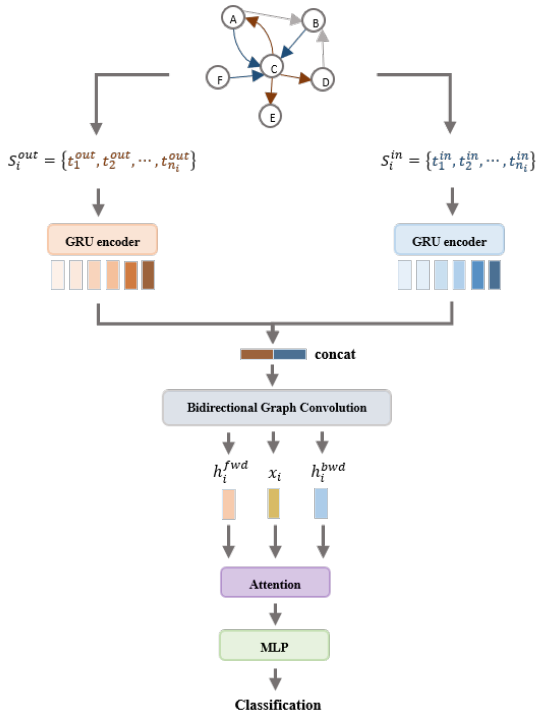


Figure 2: 模型架構圖

的分類能力，又能在有限的計算資源下保證多次重複實驗的可行性，特別適合於需要大量實驗組合的研究情境。

此外，Small 資料集同樣展現了典型的類別不平衡特徵：HI-Small 的非法交易比例約爲 1:981，而 LI-Small 的不平衡程度更爲嚴重，比例高達 1:1942。這種極端不平衡的分布充分反映了眞實金融場景中的 AML 問題，爲評估模型在實務應用中的表現提供了具有挑戰性且可信的測試基礎。

Table 1: AML 合成資料集（Small 子集）的詳細資訊

	Small	
Dataset Variant	**HI**	**LI**
Time Period (2022)	Sep 1–10	
Account Volume	515K	705K
Transaction Volume	5M	7M
Illicit Transactions	5.1K	4.0K
Fraud Ratio	1:981	1:1942

3.2 實驗設定

我們的實驗以交易記錄爲原始輸入，通過資料預處理構建交易圖結構並提取帳户交易序列。序列編碼部分採用 Gated Recurrent Unit（GRU），隱藏層維度 128，分別處理入邊與出邊序列並進行拼接。圖結構部分則使用兩層自定義雙向圖卷積層，整合注意力機制來自適應聚合鄰居訊息，每層輸出 128 維嵌入。序列與圖嵌入融合後，經由多層感知器輸出，最終完成二元分類。在訓練策略上，考量到類別高度不平衡，我們使用加權二元交叉熵損失 (Weighted Binary Cross Entropy Loss) 函數，根據類別頻率設定反比權重。採用 Adam 優化器，學習率設爲 1e-3，搭配 Early Stopping 策略與梯度裁剪確保訓練穩定性。模型選擇以驗證集 F1 分數爲準，當達到最佳驗證效果時保存模型參數。在評估上，我們採用 F1-score 作爲主要指標，並關注模型在極度不平衡資料下的整體表現，以評估其在眞實 AML 場景中的實用性。

3.3 評估指標

由於反洗錢任務具有高度不平衡的特性，我們採用多種衡量指標來全面評估模型表現。考量到實際應用中對檢測準確性與完整性的雙重要求，我們以 F1-score 作爲主要評估指標，其爲精確率（Precision）與召回率（Recall）的調和平均，能夠平衡兩者的重要性。其中，精確率衡量模型識別非法帳户的正確性，召回率則反映模型捕捉非法帳户的完整性。計算方式如下：其中，TP 爲眞正例（True Positives），TN 爲眞負例（True Negatives），FP 爲假正例（False Positives），FN 爲假負例（False Negatives）。計算方式如下：

$$\text{Precision} = \frac{TP}{TP + FP} \tag{10}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{11}$$

$$\text{F1-score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{12}$$

F1-score 特別適合評估不平衡資料集的模型性能，因爲它既考慮了模型的檢測精度，也確保了對稀有類別（洗錢帳户）的有效識別。在 AML 實務應用中，過高的假警報率（低精確率）會造成調查資源浪費，而過高的漏報率（低召回率）則可能讓眞正的洗錢活動逃脫監管，因此 F1-score 提供了這兩個關鍵需求間的最佳平衡點。

4 實驗結果

我們在 HI-Small 與 LI-Small 兩個資料集上的實驗結果如 Table 2 所示，其中 **ours** 代表我們所提出的整合式架構。整體而言，該方法在兩個資料集上皆展現出最佳的整體效能：在 HI-Small 上 F1 分數達 0.85，在 LI-Small 上則爲 0.65。此結果顯示，我們的模型在維持

Table 2: HI-Small 與 LI-Small 資料集上不同序列輸入設定的實驗結果

	HI-Small			LI-Small		
Setting	**Precision**	**Recall**	**F1**	**Precision**	**Recall**	**F1**
in-only	0.9674	0.6312	0.7639	0.6579	0.4464	0.5319
out-only	**1.0000**	0.5461	0.7064	**0.9412**	0.2857	0.4384
combined	0.9730	0.5106	0.6698	0.6667	0.1071	0.1846
ours	0.9646	**0.7730**	**0.8583**	0.7949	**0.5536**	**0.6526**

高 Precision 的同時，能顯著提升 Recall，整體 F1 分數明顯優於其他設定。這驗證了所提出架構能同時捕捉交易網路中的時間動態與結構關聯，並在高度不平衡的資料情境下仍保持穩健與準確的偵測能力。

在此基礎上，我們進一步分析了「序列方向性資訊」對洗錢偵測效能的影響。爲了探討不同方向資訊的貢獻，我們設計了三種簡化的輸入設定進行比較：**in-only** 僅使用帳户作爲收款方的入邊序列；**out-only** 僅使用帳户作爲付款方的出邊序列；而 **combined** 則將兩個方向的交易資料合併成單一序列輸入至同一個 GRU 模組，不再保留方向性。相較之下，我們的方法 **ours** 採用雙分支 GRU，分別建模入邊與出邊序列，並結合雙向圖卷積層以同時學習帳户間的結構依賴與資金流向。

比較結果顯示，僅使用入邊序列時，雖然 Precision 仍維持高水準，但因缺乏出邊方向的輔助資訊，Recall 明顯下降，使得 HI-Small 與 LI-Small 的 F1 分數分別降至 0.76 與 0.53。若僅使用出邊序列，F1 分數進一步下降至 0.70 與 0.43，顯示單向付款行爲的資訊不足以支撐有效判別。當將兩個方向合併而不區分方向時，雖然 Precision 維持良好，但因方向性訊息喪失，模型難以辨識帳户在資金流動中的角色差異，最終導致 Recall 顯著下降，F1 僅達 0.66 與 0.18。

綜合上述結果，可以確認序列方向性資訊在洗錢交易偵測中的重要性，更同時驗證了我們的整合式架構的必要性。我們的完整架構透過序列模組捕捉序列的方向訊息，並藉由圖模組保留帳户之間的結構依賴，使模型能同時利用兩種異質訊息來源而達到更佳的檢測效能。

5 結論

本研究提出一個結合序列與圖結構資訊的完整架構，並透過 AML 資料集驗證其效能。實驗結果顯示，序列方向性資訊對檢測任務至關重要，而整合式架構能在不平衡情境下展現更佳的穩健性與準確性。與僅依賴靜態圖特徵或單純序列的方法相比，所提架構同時捕捉時間動態與結構依賴，能更有效識別可疑交易。未來研究可進一步探討其在更大規模資料集上的擴展性，並結合額外的領域知識以提升模型的表現與解釋性。

References

Erik Altman. 2019. IBM transactions for anti money laundering (AML). Kaggle Dataset.

Erik Altman, Béni Egressy, Jovan Blanuša, and Kubilay Atasu. 2023. Realistic synthetic financial transactions for anti-money laundering models. In *Proceedings of the 37th International Conference on Neural Information Processing Systems*. Curran Associates Inc.

N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer. 2002. Smote: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 16:321—357.

Zhiyuan Chen, Le Dinh Van Khoa, Ee Na Teoh, Amril Nazir, Ettikan Kandasamy Karuppiah, and Kim Sim Lam. 2018. Machine learning techniques for anti-money laundering (aml) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems*, 57(2):245–285.

Zhihao Ding, Jieming Shi, Qing Li, and Jiannong Cao. 2024. Effective illicit account detection on large cryptocurrency multigraphs.

Béni Egressy, Luc von Niederhäusern, Jovan Blanusa, Erik Altman, Roger Wattenhofer, and Kubilay Atasu. 2024. Provably powerful graph neural networks for directed multigraphs.

Financial Action Task Force. 2010. *Global Money Laundering and Terrorist Financing Threat Assessment*. FATF/OECD, Paris.

Sushrut Ghimire. 2023. Timetrail: Unveiling financial fraud patterns through temporal correlation analysis.

Fredrik Johannessen and Martin Jullum. 2023. Finding money launderers using heterogeneous graph neural networks.

Thomas N. Kipf and Max Welling. 2017. Semi-supervised classification with graph convolutional networks. *International Conference on Learning Representations*.

Seong Ho Pahng and Sahand Hormoz. 2025. Improving graph neural networks by learning continuous edge directions.

Emanuele Rossi, Bertrand Charpentier, Francesco Di Giovanni, Fabrizio Frasca, Stephan Günnemann, and Michael Bronstein. 2023. Edge directionality improves learning on heterophilic graphs.

Haseeb Tariq and Marwan Hassani. 2025. *Topology-Agnostic Detection of Temporal Money Laundering Flows in Billion-Scale Transactions*, page 402—419. Springer Nature Switzerland.

Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl I. Weidele, Claudio Bellei, Tom Robinson, and Charles E. Leiserson. 2019. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics.