JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 31 No. 2, pp. 139-151, February 2026
https://doi.org/10.9708/jksci.2026.31.02.139

A GNN-based Bitcoin Mixing Detection Method via Subgraph Generation of Mixing Transactions

Hyeon-Woo Lee*, Eun-Young Park*, Sooncheol Kim**, Jiyeon Kim**

*Graduate Student, Dept. of Computer and Information Engineering, Daegu University, Gyeongsan, Korea
**Professor, Dept. of Computer Engineering, Daegu University, Gyeongsan, Korea

[Abstract]

Although Bitcoin has demonstrated its utility as a prominent cryptocurrency and a medium of economic exchange, its inherent pseudonymity—which preserves user anonymity—has contributed to a surge in illicit use, including money laundering and other illegal transactions. In particular, mixing services such as CoinJoin intentionally obfuscate transaction paths to hinder tracing of fund sources and flows. Consequently, existing on-chain analysis and transaction-level tracking methods struggle to effectively detect mixing activity. Moreover, prior studies employing graph neural networks (GNNs) for mixing detection typically adopt a global classification approach that models the entire transaction network as a single graph, which limits their ability to capture the granular context of individual transactions. In this paper, we construct a dataset comprising both illicit and legitimate Bitcoin transactions and propose a Subgraph-based GNN approach that models the adjacent flow of each transaction as an independent Subgraph to improve mixing detection. Experimental results show that the proposed method achieves over 97% accuracy. In addition, GraphSAGE yields the best performance, achieving an F1-score of 98.5% for identifying Bitcoin mixing transactions in our dataset. The proposed subgraph-based mixing detection approach can be applied to cryptocurrency crime investigations, and is expected to be particularly applicable to Anti-Money Laundering (AML) systems and blockchain forensic analysis tools that require tracking continuous flows of criminal funds.

▸ **Key words**: Bitcoin, Money Laundering, Mixing Service, Graph Neural Network, Subgraph

• First Author: Hyeon-Woo Lee, Corresponding Author: Jiyeon Kim
*Hyeon-Woo Lee (ladder887@daegu.ac.kr), Dept. of Computer and Information Engineering, Daegu University
*Eun-Young Park (pey6693@daegu.ac.kr), Dept. of Computer and Information Engineering, Daegu University
**Sooncheol Kim (kimsc@daegu.ac.kr), Dept. of Computer Engineering, Daegu University
**Jiyeon Kim (jyk@daegu.ac.kr), Dept. of Computer Engineering, Daegu University
• Received: 2026. 01. 12, Revised: 2026. 02. 03, Accepted: 2026. 02. 06.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

[요 약]

비트코인은 대표적인 암호화폐로서 경제적 거래 수단으로서의 효용성을 입증하였으나, 사용자의 익명성을 보장하는 가명성(Pseudonymity)으로 인해 자금세탁 및 불법 거래 수단으로 악용되는 사례가 급증하고 있다. 특히, CoinJoin과 같은 믹싱 서비스는 거래 경로를 의도적으로 복잡하게 구성하여 자금 출처와 흐름 추적을 어렵게 만들지만, 기존의 온체인 분석 또는 개별 트랜잭션 중심 추적 기법으로는 믹싱 트랜잭션을 효과적으로 탐지하기 어렵다. 또한, 믹싱 트랜잭션 그래프를 GNN(Graph Neural Network) 기반으로 탐지하는 연구들은 전체 네트워크를 단일 그래프로 구성하는 전역적 분류 방식에 집중하고 있어, 개별 트랜잭션 중심의 세밀한 맥락 파악에는 한계가 있다. 본 논문에서는 범죄 및 비범죄 비트코인 트랜잭션 데이터셋을 직접 구축하고, 각 트랜잭션의 인접 흐름을 독립적인 서브그래프 단위로 모델링한 후, GNN 기반 학습을 통해 믹싱 트랜잭션 탐지 성능을 향상시키는 기법을 제안한다. 실험 결과, 서브그래프를 활용 시, 믹싱 트랜잭션을 97% 이상 정확도로 탐지하는 것을 확인하였고, GNN 기반 학습 결과, GraphSAGE 모델이 98.5%의 F1-score로 가장 높은 성능으로 비트코인 믹싱 트랜잭션을 데이터셋에서 식별해 내는 것을 확인하였다. 본 연구에서 제안하는 서브그래프 기반 믹싱 탐지 기법은 암호화폐 기반 범죄 수사 실무에 활용될 수 있으며, 특히 범죄 자금의 연속적 흐름 추적이 요구되는 자금세탁 방지 시스템 및 블록체인 포렌식 분석 도구에 적용 가능할 것으로 기대된다.

▸ **주제어**: 비트코인, 자금세탁, 믹싱 서비스, 그래프 신경망, 서브그래프

I. Introduction

암호화폐(cryptocurrency)는 고도의 암호화 기술을 기반으로 금융 거래의 안전성을 보장하며 자산의 생성 및 소유권 이전을 투명하게 검증하도록 설계된 디지털 자산이다. 암호화폐는 물리적인 실체 없이 네트워크상에 데이터 형태로 존재하며 신뢰할 수 있는 경제적 거래 수단으로서 전 세계에서 활발히 활용되고 있다[1]. 다양한 종류의 암호화폐 중 비트코인(Bitcoin)은 시장 점유율과 활용도 측면에서 가장 대표적인 자산으로서 글로벌 거래 인프라와 실사용 사례를 통해 암호화폐가 경제적 거래 수단으로 활용될 수 있음을 보여준다[2]. 그러나 암호화폐는 송금 과정에서 사용자 신원 정보가 거래 내역에 직접 노출되지 않는 가명성(Pseudonymity)을 지니고, 동일한 자금이 다수의 주소로 분할 전송된 뒤 재결합될 수 있기 때문에 자금의 출처와 최종 수취인을 추적하기 어렵다는 문제점을 가진다. 특히, CoinJoin과 같은 믹싱 서비스(Mixing Service)를 통해 거래 경로를 의도적으로 복잡하게 만드는 기법이 활용될 경우, 전통적인 온체인 관측 정보만으로는 불법 자금 흐름과 범죄 연계성을 명확하게 파악하는 데 한계가 있다[3-4]. 금융정보분석원(FIU)에 따르면 2025년 상반기를 기준으로 암호화폐 불법 의심 거래는 약 4만 건에 육박하며, 이는 지난 2년간의 누적 수치인 3만 5천건을 상회하는 수준이다[5]. 이와 같이, 암호화폐 기반 범죄가 단순 투자 사기를 넘어 체계적인 자금세탁 수단으로 고도화되고 있기 때문에 암호화폐 거래 구조를 정밀하게 분석할 수 있는 추적 기술 개발이 필요하다.

암호화폐 범죄를 추적하기 위한 기존 수사 기술은 주로 특정 지갑이나 거래소 중심의 개별 트랜잭션 분석을 수행하기 때문에 복잡도가 높은 믹싱 트랜잭션을 추적하는 데에는 한계가 있다. 또한, 믹싱 과정에서는 구조적 특징이 드러나는 트랜잭션과 일반 트랜잭션이 혼재될 수 있기 때문에 개별 트랜잭션 단위만으로 믹싱 경로를 일관되게 식별하기 어렵다. 따라서 믹싱 서비스를 주로 악용하는 범죄 연루 암호화폐 지갑 중심으로, 믹싱 트랜잭션을 탐지하기 위한 고도화된 기술 개발이 필요하다.

본 논문에서는 비트코인 트랜잭션을 그래프 구조로 모델링하고, GNN(Graph Neural Network)을 기반으로 믹싱 트랜잭션을 탐지하는 모델을 개발한다. 먼저, 공개 데이터셋을 분석하여 믹싱 트랜잭션 정의를 위한 휴리스틱(Heuristic) 알고리즘을 개발하고, 다크웹 상에서 직접 수집한 비트코인 지갑 주소를 활용하여 믹싱 트랜잭션 탐지를 위한 데이터셋을 구축한다. 특히, 본 논문에서는 믹싱 트랜잭션 탐지 성능을 높이기 위해 개별 트랜잭션을 중심으로 인접한 흐름을 서브그래프(Subgraph) 단위로 구성하여 학습 데이터셋으로 구축하고, 이를 GNN 기반으로 학

습함으로써 믹싱 탐지에 효과적인 서브그래프 구성 방식을 검증한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 수행된 비트코인 믹싱 트랜잭션 탐지 연구와 그래프 및 GNN 기반 비트코인 트랜잭션 분석 연구를 살펴보고, 3장에서는 믹싱 트랜잭션 탐지 알고리즘과 서브그래프 기반 믹싱 트랜잭션 데이터셋 구축 방안을 설명한다. 4장에서는 구축된 데이터셋을 GNN 기반으로 학습하고, F1-score 기반의 성능 분석을 통해 제안된 모델의 성능을 검증한다. 마지막으로 5장에서는 결론 및 향후 연구를 제시한다.

II. Preliminaries

본 장에서는 비트코인 트랜잭션의 믹싱 탐지 및 그래프 기반 분석에 대한 기존 연구를 살펴본다. 먼저, 비트코인 믹싱 트랜잭션의 구조적 특징을 기반으로 믹싱 여부를 탐지하는 연구를 살펴보고, 그래프 및 GNN 기반의 블록체인 트랜잭션 분석 연구 동향을 제시한다. 마지막으로 기존 연구들의 공통적인 접근 방식과 한계를 정리하고, 본 논문에서 제안하는 서브그래프 기반 믹싱 트랜잭션 탐지 기법의 필요성과 연구 배경을 기술한다.

2.1 Studies on Bitcoin Mixing Transaction Detection

비트코인 믹싱 트랜잭션은 다수의 입력과 출력 주소를 포함하거나 동일한 금액을 반복적으로 분할 또는 재조합함으로써 실제 자금 흐름을 은폐하는 특징을 가진다. 이러한 특성으로 인해 믹싱 트랜잭션은 범죄 자금의 세탁 및 추적 회피를 위한 주요 수단으로 활용되고 있으며, 이를 식별하기 위한 다양한 탐지 기법들이 제안되고 있다.

먼저, 믹싱 서비스가 생성하는 거래 유형을 기준으로, 거래 구성 요소와 처리 절차를 분리하고, 이를 바탕으로 믹싱 트랜잭션을 식별하기 위한 기준을 수립하는 연구가 수행되었다[6]. 또한, 지갑 지문 분석을 활용하여 지갑의 동작 패턴과 출력 구조를 비교하고, 일반 거래로 위장된 믹싱 거래를 지갑 수준에서 구분하는 방법이 제안되었으며[7], 믹서 사용 과정에서 반복적으로 나타나는 거래 패턴과 분석 단계에서 발생하는 기술적 한계를 사례 기반으로 정리한 연구도 수행되었다[8]. 자금 흐름 분석 관점에서는 도난된 암호자산이 믹싱, 분산, 회수 단계를 거쳐 이동하는 과정을 거래 흐름 기준으로 분석하여 단계별 자금 이동 형태를 제시한 연구가 존재하며[9], 블록체인상의 자금 흐름을 추적하여 범죄 활동과 믹서 간 전송 경로의 형태를 기술적으로 분류하는 연구가 제시되었다[10]. 머신러닝 기반 접근에서는, CoinJoin 거래를 별도 데이터셋으로 구축하고, 입출력 구조 및 금액 패턴을 특징 변수로 사용하여 분류 모델을 학습하는 방식이 제안되었다[11]. 나아가 다양한 믹싱 서비스의 기능과 동작 방식을 비교하여 서비스 유형별 거래 특성을 중심으로 믹싱 동작을 분류하는 리뷰 연구도 수행되었다[12].

기존 연구들은 주로 거래 구조 분석, 지갑 지문 기반 식별, 자금 흐름 분석, 머신러닝 기반 분류 등에 기반하여 믹싱 트랜잭션을 식별하는 연구를 수행해 왔다. 그러나, 믹싱 서비스의 구현 방식과 사용 패턴이 다양하고, 온체인 관측 정보만으로는 실제 믹싱 여부를 단정하기 어려운 경우가 많으므로 각 연구별로 가정하는 식별 기준과 적용 범위가 달라질 수 있다. 따라서 서로 다른 서비스와 시나리오에서도 일관되게 적용 가능한 운영적 식별 기준을 명확히 제시하고, 해당 기준의 타당성을 실증적으로 점검하는 절차가 요구된다. 본 연구는 공개 데이터셋을 활용하여 믹싱 트랜잭션의 운영적 식별 기준을 수립하고, 직접 수집한 범죄 및 비범죄 지갑 기반 트랜잭션 분석에 이를 적용함으로써 일관된 기준에 기반한 데이터 구성과 분석 절차를 제시한다는 점에서 기존 연구와 차별점이 있다.

2.2 Studies on Graph and GNN-based Bitcoin Transaction Analysis

비트코인 트랜잭션은 개별 트랜잭션의 속성만으로는 자금 흐름과 행위자의 의도를 충분히 파악하기 어렵기 때문에, 주소 간 연결 관계와 네트워크 구조를 함께 고려할 필요가 있다. 이러한 한계를 보완하기 위해 트랜잭션과 주소를 그래프 형태로 구성하고, GNN을 적용하여 이상 트랜잭션과 불법 자금 흐름을 분석하려는 연구가 수행되어왔다.

기존 연구들은 그래프 구조에서 나타나는 연결 패턴, 이웃 관계, 경로 정보를 특징으로 활용하여 의심 트랜잭션을 탐지하는 방법을 주로 제시하였다. 먼저, 온체인 데이터를 기반으로 트랜잭션 패턴을 정의하고, 지도학습 모델을 활용하여 의심 트랜잭션을 분류하는 연구가 수행되었으며[13], 그래프 합성곱 네트워크(GCN)를 적용하여 트랜잭션 그래프상에서 사기 트랜잭션을 직접 분류하는 연구가 제안되었다[14]. 자금세탁방지(Anti-Money Laundering, AML) 관점에서 그래프 분석과 딥러닝을 결합하여 불법 거래 네트워크를 식별하는 연구가 진행되었다. 트랜잭션 연결 구조를 기반으로 의심 네트워크를 분리하고, 자금 흐름의 특징을 이용해 불법 거래 가능성을 평가하는 방법[15],

GNN을 AML 프레임워크에 직접 적용하여, 규칙 기반 탐지 체계를 보완하고 거래 분류 성능을 향상시키는 접근도 제시되었다[16]. 또한, 다양한 분석 기법을 통합하여 비트코인 불법 트랜잭션의 유형을 비교 정리한 연구는 AML 분석 범위를 확장하였다[17]. 트랜잭션의 구조적 변화와 시간적 변화를 동시에 고려하기 위해, 시공간 그래프 신경망을 적용한 연구도 진행되었다. 해당 연구는 시간축을 모델에 결합하여, 거래 생성 과정의 동적 변화를 반영한 이상 탐지 기법을 제안하였으며[18], 불법 주소의 향후 트랜잭션을 예측하기 위해 인접 구조와 맥락 정보를 학습하여 미래 전송 가능성을 추정하는 예측 기반 연구도 수행되었다[19]. 또한 계층적 주의(attention) 구조를 적용하여 거래 시퀀스 전반의 상관관계를 학습하는 방식이 제안되었으며[20], 그래프 모티프 기반 표현 학습을 통해 트랜잭션 네트워크의 지역 구조를 다른 예측 문제에 활용하려는 연구도 수행되었다[21]. 마지막으로, 자금세탁과 사기 거래를 함께 고려하여 그래프 분석과 딥러닝을 통합한 탐지 프레임워크가 제시되었으며, 불법 거래 식별 성능을 종합적으로 평가하였다[22].

종합적으로, 기존 연구는 GNN과 다양한 그래프 분석 기법을 활용하여 이상 트랜잭션 탐지와 불법 주소 예측을 수행하고 있다. 그러나 대부분의 연구가 전체 네트워크를 단일 그래프로 구성하는 전역적 분류 방식에 집중하고 있어, 개별 트랜잭션 중심의 세밀한 맥락 파악에는 한계가 있다. 본 연구는 이러한 부분을 보완하고자 개별 트랜잭션 주변의 인접 관계를 독립적인 서브그래프 단위로 구성하고, 이를 GNN 기반으로 학습하여 믹싱 트랜잭션 탐지 성능을 제고하는 모델을 제안한다.

III. Generation of Subgraph Dataset for Bitcoin Mixing Transaction Detection

본 장에서는 GNN 기반 믹싱 트랜잭션 탐지 모델을 학습하기 위한 서브그래프 데이터셋 구축 과정을 기술하며 Fig. 1은 본 연구의 전체 프레임워크를 보여준다. Phase 1은 믹싱 트랜잭션을 정의하기 위해 공개 데이터셋을 활용하여 휴리스틱 알고리즘을 개발하는 단계이고, Phase 2는 다크웹에서 수집한 범죄 연루 비트코인 주소와 일반 비범죄 주소에서 트랜잭션 데이터를 수집하는 단계이다. 이 단계에서는 수집된 데이터에 휴리스틱 알고리즘을 적용하여 믹싱 트랜잭션을 분류하는 과정을 포함한다. Phase 3에서는 분류된 트랜잭션을 연속된 자금 흐름을 반영한 서브그래프 데이터셋으로 구축하며, 데이터 누수 방지를 위한 전처리를 수행한다. 마지막으로 Phase 4에서는 구축된 서브그래프 데이터셋을 GNN 기반으로 학습하여 믹싱 트랜잭션 추적을 위한 최적의 서브그래프 생성 모델을 도출한다.

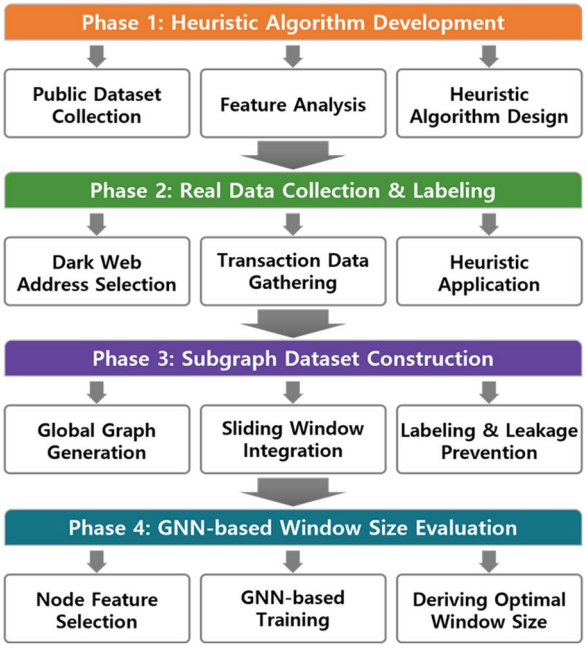

Fig. 1. Overview of the Proposed Research Framework for Subgraph-based Bitcoin Mixing Detection

3.1 Development of a Heuristic-Based Bitcoin Mixing Transaction Detection Algorithm

본 연구에서는 믹싱 트랜잭션 정의의 객관성과 재현성을 확보하기 위해, 선행연구를 통해 검증된 공개 데이터셋을 활용하여 정상 트랜잭션과 믹싱 트랜잭션 데이터셋을 구축하였다.

정상 트랜잭션 데이터는 공개된 Elliptic++[23] 데이터셋을 활용하여 수집하였다. Elliptic++ 데이터셋은 비트코인 트랜잭션을 illicit, licit, unknown의 세 가지 범주로 분류하며, 이 중 licit으로 라벨링된 41,458개의 트랜잭션을 정상 트랜잭션 데이터셋으로 활용한다. 해당 데이터셋은 거래소, 합법적 서비스 제공자 등 정상적인 비트코인 사용 패턴을 포함한다. 또한, 믹싱 트랜잭션 데이터는 선행 연구를 통해 공개된 Bitcoin Mixing Dataset[24]을 활용하였다. 이 데이터셋은 Wasabi Wallet, JoinMarket, ChipMixer 등 실제 믹싱 서비스에서 발생한 트랜잭션을 포함하고 있으며 본 연구에서는 검증된 20,610개의 믹싱 트랜잭션을 데이터셋으로 활용한다.

앞서 구성한 정상 및 믹싱 데이터셋의 일관성을 위해 공개 데이터셋에서는 트랜잭션 식별을 위한 txhash와 라벨

데이터만 사용한다. 이후, 각 트랜잭션에 대해 직접 구축한 로컬 비트코인 풀노드(Bitcoin Core)와 인덱싱 시스템(Electrs)을 활용하여 트랜잭션의 메타데이터를 수집하였으며 Table 1과 같이 트랜잭션 데이터를 수집하였다.

Table 1. Bitcoin Transaction Feature Information

Type	Feature	Description
Transaction Information	txhash	Unique transaction identifier
	size	Actual transaction size
	vsize	Virtual transaction size
	weight	Transaction weight
	version	Transaction protocol version
	locktime	Transaction locktime
Input/Output Information	vin	List of transaction inputs
	vout	List of transaction outputs
	input_value	Total input amount
	output_value	Total output amount
	fee	Network fee
Statistics & Analysis	input_count	Number of inputs
	output_count	Number of outputs
	fee_per_byte	Fee per byte
	fee_ratio	Ratio of fee to total value
	unique_input_addresses_count	Count of unique input addresses
	unique_output_addresses_count	Count of unique output addresses
	identical_output_amount_count	Count of outputs with identical amounts
	output_amount_entropy	Entropy of output amount distribution
	output_type_entropy	Entropy of output address types
	label	Transaction classification label

트랜잭션 데이터는 트랜잭션 정보, 입출력 정보, 통계 및 분석의 세 가지 타입으로 구분되며 트랜잭션 정보는 블록체인에 기록된 기본 메타데이터, 입출력 정보는 자금의 흐름을 나타낸다. 통계 및 분석의 특징들은 비트코인 풀노드에서 수집한 vin, vout 등의 원시 데이터를 기반으로 별도의 연산 과정을 통해 2차 가공한 특징들이다. identical_output_amount_count는 동일 금액을 가진 출력의 개수로 CoinJoin 방식의 믹싱에서 나타나는 주요 특성이며, output_amount_entropy는 출력 금액 분포의 엔트로피로 믹싱 트랜잭션의 균등 분배 특징을 수치화한다. 최종적으로 구축된 데이터셋은 정상 트랜잭션 41,458개와 믹싱 트랜잭션 20,610개로 구성되어 총 62,068개의 트랜잭션을 포함한다.

본 연구에서는 구축된 데이터셋을 활용하여 믹싱 트랜잭션 판별에 효과적인 휴리스틱 알고리즘을 개발하고, 최적의 임계값을 도출한다. 이를 위해 우선 Table 1의 트랜잭션 데이터 특징 중 믹싱 탐지에 유의미한 후보 특징을 선정한다. 기존 연구에서 사용한 믹싱 탐지의 핵심 기준으로는 다수의 거래를 하나로 묶어 처리하는 과정에서 발생하는 다중 입출력 구조와[25] 익명성 보장을 위해 동일한 금액을 출력하는 구조적 특성[26]을 제시한 바 있다. 본 연구는 이러한 기존 탐지 기준과 구축한 트랜잭션 데이터의 특징을 종합적으로 분석하여 믹싱 트랜잭션 탐지에 유효한 후보 특징을 도출하였으며, Table 2와 같이 총 8개의 휴리스틱 알고리즘 후보 특징을 최종 선별하였다.

Table 2. Heuristic Feature Candidates

Feature	Rationale
size	Reflects large transaction size due to multiple inputs and outputs in mixing
weight	Reflects transaction scale regardless of SegWit adoption
fee_ratio	Captures fee patterns characteristic of mixing services
unique_input_addresses_count	Reflects the multiple-input structure of CoinJoin methods
unique_output_addresses_count	Reflects multiple-output characteristics for fund dispersion
identical_output_amount_count	Representative characteristic of mixing techniques
output_amount_entropy	Measures the uniformity of the output amount distribution
output_type_entropy	Indicates the usage diversity of output script types

이후, 3.1장에서 구축한 데이터셋의 정상 트랜잭션 41,458건과 믹싱 트랜잭션 20,610건에 대해 Table 2의 휴리스틱 알고리즘 후보 특징의 분포를 분석하였으며 Fig. 2는 각 특징에 대한 정상 및 믹싱 트랜잭션 클래스 간의 밀도 분포를 나타낸다.

분석 결과, 대부분의 휴리스틱 후보 특징에서 믹싱 트랜잭션과 정상 트랜잭션 간에 명확한 분포 차이가 확인되었다. 특히, identical_output_amount_count는 믹싱 트랜잭션에서 높은 값을 보이며 정상 트랜잭션에서는 대부분 0 또는 낮은 값을 나타낸다. 또한, output_amount_entropy와 unique_output_addresses_count 역시 믹싱 트랜잭션에서 높은 분포를 보여 변별력이 높은 반면, output_type_entropy와 fee_ratio는 두 클래스 간 분포 구간이 상당 부분 중첩되어 식별력이 낮은 것으로 확인되었다. 각 필드의 실제 식별 성능을 실증적으로 평가하기 위해 필드별 최적 임계값을 적용하여 검증 데이터셋을 분류하였으며 결과는 Fig. 3과 같다.

각 특징의 최적 임계값을 기준으로 구축한 데이터셋을 분류한 결과, size, weight, unique_input_addresses_count, unique_output_addresses_count, output_

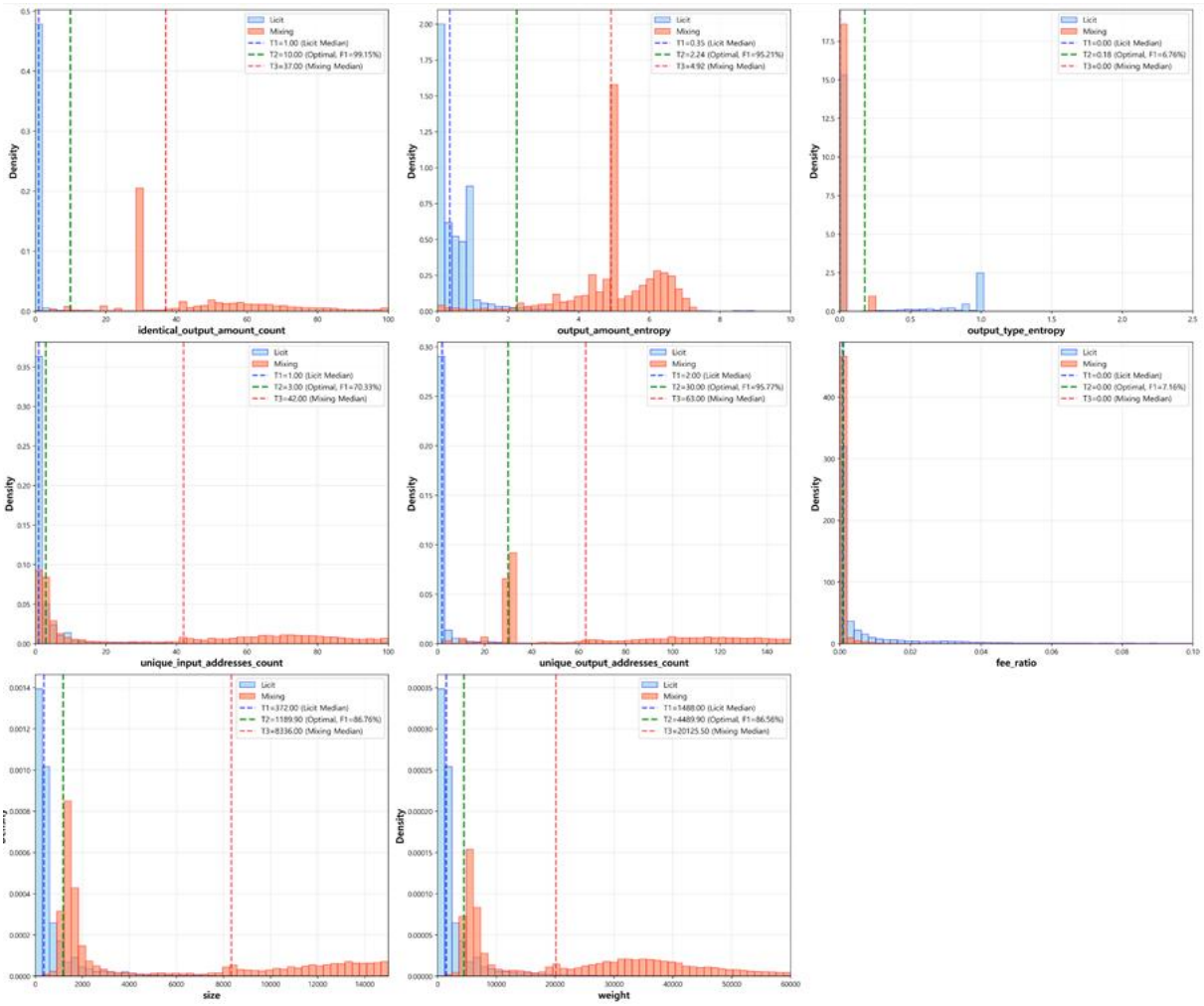

Fig. 2. Density Distributions of Heuristic Feature Candidates (Normal vs. Mixing)

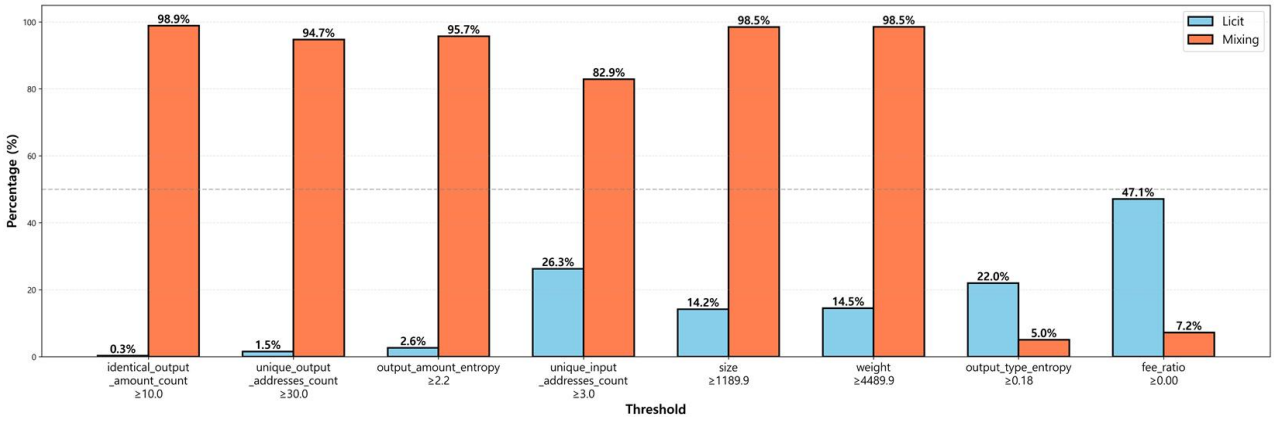

Fig. 3. Classification Performance of Heuristic Features using Optimal Thresholds

amount_entropy, identical_output_amount_count 6개 필드에서는 믹싱 트랜잭션이 80% 이상으로 효과적으로 검출되었다. 반면 fee_ratio, output_type_entropy는 판별력이 낮았으며 특히, fee_ratio 비율은 Licit Rate 47.1%, Mixing Rate 7.2%로 역방향 판별력을 보여 믹싱 탐지를 위한 지표로 활용하기에는 부적합한 것으로 확인되었다. 따라서 믹싱 트랜잭션 탐지를 위한 최종 휴리스틱 알고리즘은 fee_ratio와 output_type_entropy를 제외한 6개의 특징으로 구성하였고 Table 3은 선정된 6개 특징과 임계값을 나타낸다.

Table 3. Heuristic Algorithm for Mixing Transaction Detection

Feature	Threshold
size	≥1189.9
weight	≥4489.9
unique_input_addresses_count	≥3
unique_output_addresses_count	≥30
identical_output_amount_count	≥10
output_amount_entropy	≥2.24

믹싱 트랜잭션 탐지를 위해 최종 선정된 6개 특징을 기반으로 6점 만점의 스코어링 시스템을 설계하였다. 해당 시스템은 각 특징의 휴리스틱 조건을 충족할 때마다 1점을 부여하는 가산 방식을 적용하였으며, 합산된 누적 점수를 기준으로 믹싱 여부를 최종 판정한다. 또한, 믹싱 탐지를 위한 최적의 점수 임계값을 도출하기 위해 구축한 데이터셋을 대상으로 0점부터 6점까지 모든 임계값 구간에 대한 Precision, Recall, F1-score를 산출하여 비교 분석하였다. Fig. 4는 임계값 변화에 따른 성능 곡선을 보여준다.

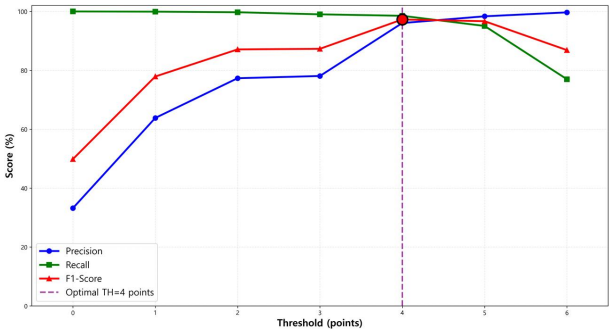

Fig. 4. Performance Evaluation of Heuristic Algorithm by Threshold

분석 결과, 임계값을 4로 설정했을 때 Precision 95.2%, Recall 99.4%로 F1-score 97.28%의 최고 성능을 달성하였다. 이에 따라 본 연구에서는 6개 특징 중 4개 이상을 충족하는 경우를 믹싱 트랜잭션으로 판별하는 최종 탐지 기준으로 선정하였다. 이후, 최종 휴리스틱 알고리즘의 실효성을 검증하기 위해 실제 다크웹에서 수집한 범죄 주소의 트랜잭션 데이터셋에 해당 알고리즘을 적용하여 분석을 수행한다.

3.2 Collection of Criminal and Non-Criminal Bitcoin Transactions

본 연구에서는 3.1장에서 개발한 믹싱 탐지 휴리스틱 알고리즘의 유효성을 검증하기 위해, 믹싱 기법이 사용된 범죄 연루 비트코인 지갑 주소와 대조군인 비범죄 지갑 주소를 수집하여 분석을 수행한다. 이후, 수집한 주소들의 출력 트랜잭션 흐름을 추적하며 도출한 휴리스틱 알고리즘으로 믹싱 트랜잭션 탐지를 수행한다. 트랜잭션을 수집하기 위해 선정한 범죄 및 비범죄 지갑 주소는 Fig. 5와 같다.

Fig. 5. List of Selected Criminal and Non-Criminal Wallet Addresses for Data Collection

범죄 지갑 주소는 실제 다크웹 상의 불법 카드 거래, 마약 사이트 등을 홍보하는 브로커 사이트에서 수집된 범죄 지갑 주소이며 실제 믹싱 기법을 사용한 비트코인 지갑 주소로 확인되었다. 반면, 비범죄 지갑 주소는 일반적인 비트코인 거래 패턴을 보이는 주소로 일반 사용자 주소로 선정하였다.

이후, 수집된 지갑 주소에 대해 출금 방향으로 트랜잭션을 추적하였으며 각 주소에서 출력된 트랜잭션을 시작점으로, 해당 트랜잭션의 출력이 다시 입력으로 사용되는 후속 트랜잭션을 순차적으로 추적·수집하였다. 수집 특징은 3.1장의 Table 1과 동일하며 최종적으로 4개 주소에서 총 41,950건의 트랜잭션을 수집하였다. 범죄 지갑 주소의 출력 트랜잭션을 분석한 결과, 해당 주소에서 발생한 트랜잭션의 경우 Fig. 6과 같이 다수의 입·출력 및 동일 금액 출력 등의 대표적인 CoinJoin 믹싱 기법이 적용된 트랜잭션임을 확인하였다.

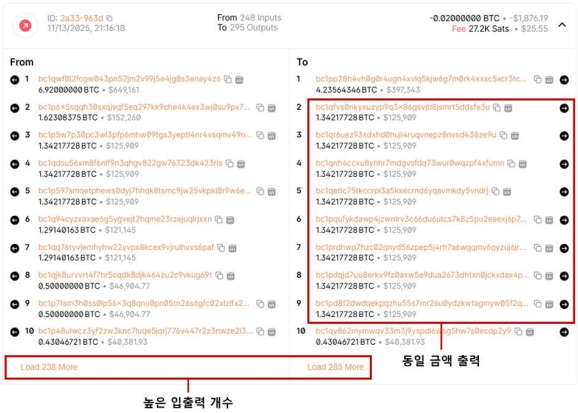

Fig. 6. Example of CoinJoin Mixing Transaction Detected in Criminal Address Flows

수집된 41,950건의 트랜잭션에 대해 3.1장에서 도출한 휴리스틱 알고리즘을 기반으로 믹싱 트랜잭션 탐지를 수행하였다. 각 트랜잭션에 대해 6개 휴리스틱 알고리즘 특징들의 충족 여부를 평가하였으며 산출된 누적 점수가 4점 이상인 경우 믹싱 트랜잭션으로, 4점 미만일 경우 정상 트랜잭션으로 최종 분류하였다. Fig. 7은 주소별 트랜잭션 믹싱 비율을 보여주며 범죄 주소와 비범죄 주소 간의 믹싱 비율 차이가 확인되었다.

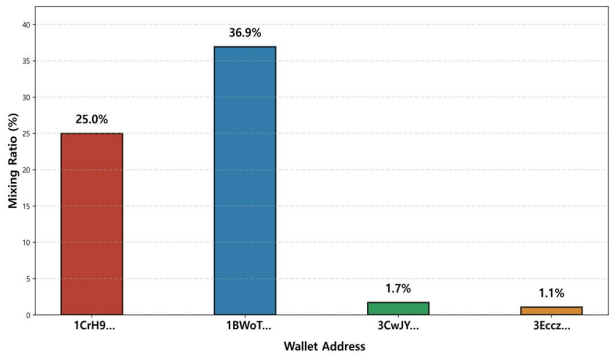

Fig. 7. Ratio of Identified Mixing Transactions by Wallet Address

분석 결과, 비범죄 지갑 주소(3CwJY..., 3Eccz...)에서 탐지된 믹싱 트랜잭션 비율은 1%대로 매우 낮게 나타났지만, 범죄 연루 지갑 주소(1CrH9..., 1BWoT...)의 믹싱 비율은 각각 25.0%, 36.9%로 비범죄 지갑 주소와 높은 차이를 보였다. 이는 범죄 연루 지갑 주소가 자금 추적을 회피하기 위해 믹싱 서비스를 활용하고 있음을 보여준다. 그러나 믹싱 서비스를 활용한 범죄 주소임에도 믹싱 트랜잭션 탐지 비율이 25-35% 수준으로 낮게 나타났으며 이는 믹싱 기법이 적용된 자금세탁 경로라도 모든 트랜잭션이 믹싱 특징을 보이는 것이 아니라 자금을 분할하는 과정에서 일반 트랜잭션 유형의 패턴이 혼재되어 나타나기 때문이다. 즉, 단일 트랜잭션 단위의 휴리스틱 분류로는 전체 믹싱 경로를 완벽히 탐지하는 데 한계가 존재한다. 따라서 보다 정밀한 추적을 위해 단일 트랜잭션 단위가 아닌 연속된 자금 흐름 단위의 분석이 필요하다.

3.3 Construction of Bitcoin Transaction Dataset via Subgraph Modeling

본 연구에서는 단일 트랜잭션 단위의 분석이 가지는 한계를 극복하고, 자금의 연속적인 흐름을 분석하기 위해 슬라이딩 윈도우 방식의 서브그래프를 생성 및 라벨 전처리 기법을 제안한다. 이는 단일 시점이 아닌 연속된 자금 흐름을 서브그래프 단위로 모델링함으로써, 복잡한 믹싱 패턴을 보다 효과적으로 분석할 수 있다.

서브그래프 데이터셋을 구축하기 위해서 3.2장에서 구축한 41,950건의 트랜잭션 데이터셋을 자금 흐름을 반영한 글로벌 그래프로 구성한다. Fig. 8은 생성되는 글로벌 그래프 예시를 보여주며 노드는 트랜잭션, 엣지는 트랜잭션 간 자금 흐름 관계를 나타낸다.

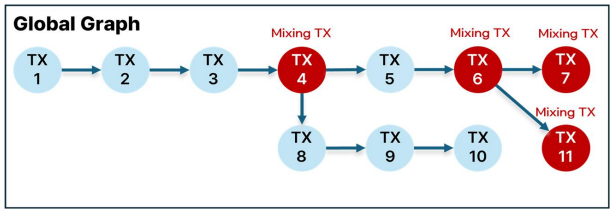

Fig. 8. Example of Bitcoin Global Graph

이러한 글로벌 그래프는 주소별 거래 빈도에 따라 수천 개 또는 수만 개 이상의 체인으로 연결될 수 있으므로 전체 그래프를 한 번에 분석하는 것은 효율적이지 않다. 또한 단일 자금 흐름 내에 정상 트랜잭션 및 믹싱 트랜잭션이 혼재되어 있어 명확한 믹싱 흐름을 추적하기 어렵기 때문에 글로벌 그래프를 서브그래프로 분할하여 작은 흐름 단위로 추적하는 것이 필요하다.

본 연구에서는 글로벌 그래프에서 연속된 자금 흐름 경로를 추출한 후, 슬라이딩 윈도우 기법을 적용하여 서브그래프를 생성한다. 생성 시, 윈도우 크기(Window Size)는 하나의 서브그래프에 포함되는 연속된 트랜잭션의 개수를 의미하며, 이동 간격(Stride)은 다음 트랜잭션으로 이동하는 간격을 의미한다. Fig. 9는 Fig. 8의 글로벌 그래프를 대상으로 윈도우 크기를 5, 이동 간격을 1로 설정했을 때의 서브그래프 생성 과정을 예시로 보여준다.

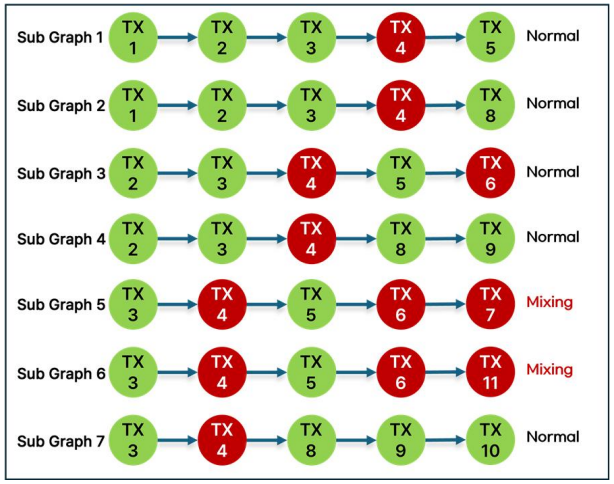

Fig. 9. Subgraph Generation via Sliding Window (Window Size=5, Stride=1)

본 연구에서는 서브그래프 단위의 믹싱 트랜잭션 탐지를 위해 임계값 기반 라벨링 기법을 적용한다. 서브그래프를 구성하는 트랜잭션 노드 중, 3.1장에서 개발한 휴리스틱 알고리즘에 의해 믹싱으로 탐지된 노드의 비율이 50% 이상일 경우, 해당 서브그래프를 믹싱으로 분류한다. 예시로 글로벌 그래프인 Fig. 8에서 믹싱으로 탐지된 트랜잭션 노드가 'TX 4', 'TX 6', 'TX 7', 'TX 11'이고, 해당 믹싱 트랜잭션 노드들을 50% 이상 포함하는 Fig. 9의 Subgraph 5와 6의 경우, 최종적으로 믹싱 서브그래프로 분류된다. 반면, 믹싱 트랜잭션 노드 'TX 4' 하나만을 포함하는 Subgraph 1, 2, 4, 7과 믹싱 트랜잭션 노드가 2개인 Subgraph 3은 믹싱 트랜잭션이 50% 미만이므로 정상 서브그래프로 분류된다. 이러한 방식은 일부 오탐지된 노드가 있더라도 주변 흐름을 통해 보정하는 효과를 갖는다. 하지만 이러한 서브그래프 기반 분류는 실제 자금 흐름의 연속성을 얼마나 충분히 반영하는지에 따라 달라지며 이는 서브그래프 데이터셋 구축 시 윈도우 크기에 의해 결정된다. 따라서 서브그래프 단위의 믹싱 트랜잭션 탐지 성능을 안정적으로 확보하기 위해서는, 자금 흐름을 적절히 포착할 수 있는 윈도우 크기를 선정할 필요가 있다.

이후, 본 연구에서는 서브그래프 데이터셋 구축 시 최적의 윈도우 크기를 선정하기 위해 비교 분석을 수행한다. 이동 간격은 1로 고정하고 윈도우 크기를 2부터 7까지 다양한 크기별로 서브그래프를 생성하고, 4개의 범죄·비범죄 주소에 대해 믹싱 서브그래프 탐지 비율의 변화를 분석하였다. Fig. 10은 윈도우 크기 변화에 따른 주소별 믹싱 서브그래프 탐지 비율을 보여준다.

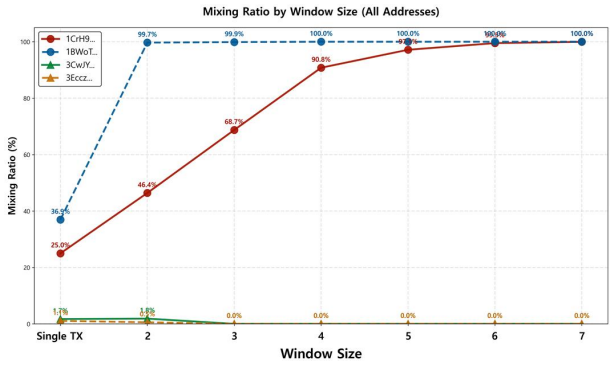

Fig. 10. Ratio of Identified Mixing Subgraphs by Window Size per Wallet Address

분석 결과, 윈도우 크기가 증가함에 따라 범죄 연루 주소와 비범죄 주소 간의 믹싱 탐지 비율의 명확한 차이가 확인되었다. 범죄 연루 주소(1CrH9..., 1BWoT...)의 경우, 윈도우 크기가 증가할수록 믹싱 트랜잭션 탐지 비율이 급격히 상승하는 것으로 나타났다. 특히, '1CrH9...'주소는 단일 트랜잭션 단위 분석(Single TX)에서는 믹싱 비율이 25.0%에 불과했으나, 서브그래프 단위로 확장함에 따라 윈도우 크기 3에서 68.7%, 5에서 97.1%로 급증하였으며, 7에서는 100.0%에 도달하였다. '1BWoT...'주소 또한 윈도우 크기가 2인 시점부터 이미 99.7%의 믹싱 탐지율을 기록하였다. 이는 범죄 자금이 연속적인 믹싱 경로를 통해 이동하고 있음을 나타내며, 서브그래프 기반 분석이 이러한 흐름을 포착하는 데 효과적임을 확인하였다.

반면, 비범죄 주소(3CwJY..., 3Eccz...)의 경우, 윈도우 크기가 증가할수록 믹싱 비율이 낮아지는 패턴을 보였다. 단일 트랜잭션 분석에서는 1%대였던 믹싱 탐지 비율이 윈도우 크기 3 이상에서는 0%로 완전히 제거되었다. 이는 일반 거래에서 우연히 발생하는 믹싱 유사 패턴이 연속성을 갖지 않음을 의미하며, 서브그래프 분석이 이러한 일시적 오탐을 노이즈로서 효과적으로 필터링함을 보여준다.

본 연구에서는 앞의 결과를 바탕으로 GNN 모델 학습에 최적화된 윈도우 크기를 선정한다. 윈도우 크기 2의 경우, 트랜잭션 흐름이 너무 짧아 '1CrH9...' 주소의 믹싱 비율이 46.4% 수준에 머물러 믹싱 패턴 포착에 한계가 있으며, 비범죄 주소의 믹싱 노이즈가 일부 잔존할 위험이 있다. 반대로 윈도우 크기 6 이상은 '1CrH9...' 주소의 믹싱 서브그래프 탐지 비율이 이미 윈도우 크기 5(97.1%)에서 수렴하였으므로, 추가적인 윈도우 크기 증가는 오히려 자금 흐름이 지나치게 길어져 자금 소유자가 변경되는 구간까지 포함할 우려가 있다.

따라서 본 연구는 범죄 및 비범죄 주소 간의 판별력이 극대화되면서도 데이터의 다양성을 확보할 수 있는 W=3에서 W=5 사이를 최적의 윈도우 구간으로 판단하였으며, 해당 범위로 생성된 서브그래프 데이터셋을 최종 GNN 학습에 활용한다.

IV. GNN-based Experimental Results

본 장에서는 3장에서 구축한 서브그래프 데이터셋을 기반으로 GNN(Graph Neural Network) 모델을 학습하기 위해 먼저 실험 환경과 모델의 입력으로 사용될 노드 특징 선정 과정을 기술한다. 이후, 학습된 GNN 모델의 성능을 분석하여 제안하는 서브그래프 기반 탐지 방법론의 유효성을 검증한다.

4.1 Experimental Setup

본 연구에서는 GNN 모델 학습을 위해 3.3장에서 구축한 서브그래프 데이터셋을 사용하며 윈도우 크기가 각각 3, 4, 5로 생성된 서브그래프 데이터셋을 활용하여 모델의 탐지 성능을 평가한다. 비교 및 평가를 위한 GNN 모델로는 그래프 분류 문제에 널리 사용되는 GCN(Graph Convolutional Network), GraphSAGE, GAT(Graph Attention Network), GIN(Graph Isomorphism Network)의 4가지 GNN 모델을 선정하여 적용한다.

GNN 모델의 학습 효율성과 탐지 정확도를 높이기 위해, 통계적 분석을 통해 최적의 노드 특징을 선정한다. 3.1장에서 정의한 트랜잭션 특징 중 수치형 데이터를 대상으로 믹싱 여부와의 상관관계를 분석하였으며, 피어슨 상관계수(Pearson correlation coefficient)의 절댓값이 0.2 이상인 필드를 유의미한 특징으로 정의하였다. 분석 결과, Table 4와 같이 총 7개의 특징을 최종 선정한다.

Table 4. Pearson Correlation Coefficients between Selected Features and Mixing Transactions

Feature	Correlation Coefficient
identical_output_amount_count	0.523
output_amount_entropy	0.487
unique_output_addresses_count	0.412
output_count	0.398
size	0.356
weight	0.341
unique_input_addresses_count	0.289

선정된 특징들은 믹싱 트랜잭션의 구조적, 통계적 특징을 효과적으로 반영한다. identical_output_amount_count와 output_amount_entropy는 상관계수가 0.523과 0.487로 가장 높은 상관관계를 보였으며, 이는 CoinJoin의 핵심 메커니즘인 동일 금액 출력이 믹싱 식별의 결정적인 요인임을 나타낸다. 또한, unique_output_addresses_count와 output_count는 자금 분산을 위한 다중 출력 특징을 포착하며, size와 weight는 다수의 입출력으로 인한 트랜잭션 규모 증가를 반영한다.

모든 입력 특징은 데이터 분포의 편차를 줄이고 학습 안정성을 확보하기 위해 로그 변환과 표준 정규화를 적용하여 스케일을 조정한다. 모델 학습을 위한 하이퍼파라미터 설정은 Hidden Dimension 64, 3개의 GNN 레이어, Batch Size 32, Learning Rate 0.002, 최적화 함수로 Adam 옵티마이저를 사용하였다. 데이터셋은 학습(80%), 검증(10%), 평가(10%)로 분할하며, Dropout을 적용하여 과적합을 방지하였다. 추가적으로 슬라이딩 윈도우 방식의 특성상 서브그래프 간 노드 중복이 발생할 수 있으나, 본 연구에서는 데이터 누수를 방지하기 위해 중복되는 노드 정보가 학습 세트와 평가 세트에 동시에 포함되지 않도록 데이터셋 분할 방식을 적용하였다. 모델은 최대 100 epoch 까지 학습을 수행하며, 검증 성능이 더 이상 향상되지 않을 경우, 조기 종료를 적용하여 최적 시점의 모델을 선택하였다.

4.2 Performance Evaluation

본 연구에서는 선별한 7개의 주요 특징과 서브그래프 데이터셋을 기반으로, GNN 믹싱 탐지 모델의 성능을 평가한다. 윈도우 크기와 모델 아키텍처 변화에 따른 탐지 정확도를 측정하여, 서브그래프 학습 방식의 유효성을 검증하고 최적의 서브그래프 윈도우 크기를 도출한다.

Fig. 11(a)은 선정된 7개의 특징만을 사용하여 학습한 GNN 모델들의 윈도우 크기별 믹싱 트랜잭션 탐지 성능(F1-score)을 나타낸다.

분석 결과, 4가지 GNN 모델 모두 윈도우 크기 4에서 가장 높은 탐지 성능을 기록하였다. 윈도우 크기 3에서는

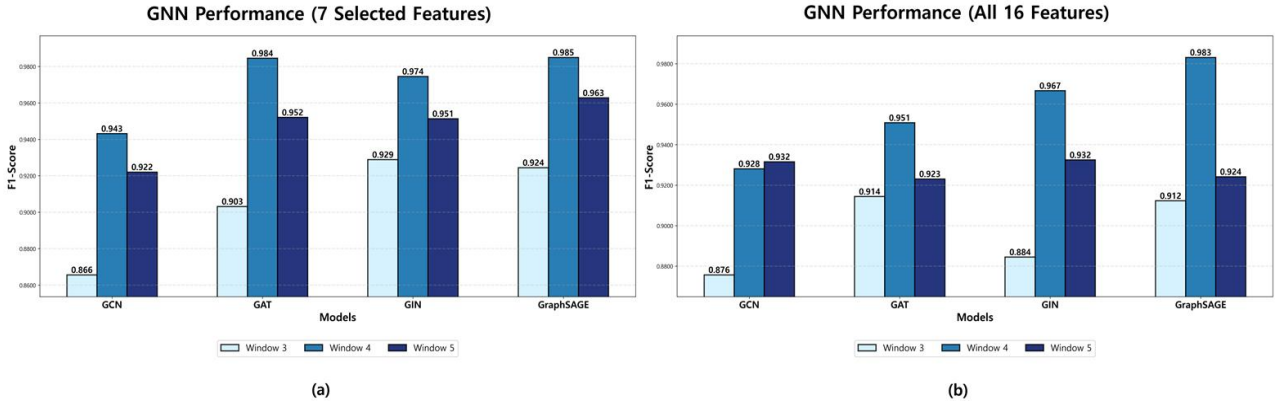

Fig. 11. Performance Comparison of GNN Models based on Feature Selection ((a) 7 Selected Features, (b) All 16 Features)

GCN 모델이 86.6%로 가장 낮은 성능을 보였고, GIN 모델이 92.9%로 가장 높은 성능을 기록하였다. 윈도우 크기가 4의 경우, 모든 모델의 성능이 윈도우 크기 3에 비해 향상되어 GraphSAGE 모델이 98.5%로 최고 성능을 달성하였고, GAT 모델 또한 98.4%로 높은 성능을 기록하였다. 이는 윈도우 크기 3에서는 포함되는 트랜잭션 수가 적어 믹싱 패턴의 연속성을 충분히 반영하지 못하였으나, 윈도우 크기 4에서는 연속된 자금 흐름의 특성을 보다 정확하게 포착하여 믹싱 흐름과 정상 흐름 간의 구분이 명확해지고, 이로 인해 GNN 모델이 믹싱 서브그래프를 효과적으로 탐지할 수 있었기 때문으로 분석된다.

윈도우 크기가 5로 증가했을 때는 대부분의 모델에서 성능이 소폭 하락하였다. GraphSAGE 모델은 96.3%로 가장 높은 성능을 유지하였고, GAT 모델은 95.2%, GIN 모델은 95.1%, GCN 모델은 92.2%로 모든 GNN 모델이 윈도우 크기 4 대비 성능이 감소하였다. 이는 3.3장에서 언급한 바와 같이 윈도우 크기가 지나치게 커지면 서브그래프 흐름이 길어져 자금 소유자가 변경되는 구간까지 포함될 수 있기 때문에 하나의 서브그래프 내에 서로 다른 성격의 자금 흐름이 혼재되어 모델의 분류 정확도가 저하된 것으로 분석된다. 따라서 본 연구에서는 연속된 자금 흐름의 맥락을 충분히 반영하면서도 이질적인 흐름의 혼입을 최소화할 수 있는 윈도우 크기 4를 최적의 서브그래프 구성 파라미터로 선정하였다.

추가적으로 선정된 7개 특징의 대표성을 검증하기 위해, 트랜잭션 해시(txhash)와 같은 트랜잭션 식별자를 제외한 전체 16개 수치형 특징을 모두 사용하여 동일한 조건에서 비교 실험을 수행하였다. Fig. 11(b)은 16개의 전체 특징으로 학습했을 때의 실험 결과를 보여준다.

분석 결과, 전체 16개의 특징으로 학습한 경우, 7개의 특징으로 학습했을 때와 유사한 성능을 보였으나, 대부분 조합에서 7개 특징 학습 시보다 낮은 성능으로 나타났다. 윈도우 크기 4에서 GraphSAGE 모델은 전체 16개의 특징으로 학습 시 98.3%로 7개 특징 학습과 유사한 성능을 보였으나, GAT 모델의 경우, 7개 특징으로 학습한 98.4%보다 약 3.3% 낮은 성능을 보였다. 또한, GIN, GCN 모델 역시 전체 특징 학습 시 각각 96.7%와 92.8%의 성능으로, 7개 특징 학습 대비 각각 0.7% 및 1.5% 하락한 성능을 보였다. 이러한 결과는 본 연구에서 피어슨 상관계수 기반으로 선정한 7개 핵심 특징이 믹싱 트랜잭션 탐지에 필요한 정보를 충분히 포함하고 있음을 보여준다. 16개 전체 특징에는 믹싱 탐지와 직접적인 관련이 없는 특징들이 포함되어 있어 노이즈로 작용하고, 모델이 핵심 패턴에 집중하는 것을 방해한다. 특히, Table 4에서 확인한 바와 같이 CoinJoin 기반 믹싱의 핵심 특성을 반영하는 특징들이 7개 선정 특징에 포함되어 있어, 연산 복잡도가 낮으면서도 높은 탐지 성능을 달성할 수 있었다.

최종적으로, 본 연구에서 제안한 서브그래프 기반 접근법은 윈도우 크기 4에서 GraphSAGE 모델을 사용할 때 F1-score 98.5%의 최고 성능을 달성하였다. 이러한 결과는 슬라이딩 윈도우를 통해 자금 흐름의 연속성을 적절한 범위로 설정하는 것이 중요한 요소임을 보여주며 믹싱 트랜잭션 탐지에 윈도우 크기 4가 연속된 자금 흐름의 맥락을 반영하면서도 불필요한 흐름의 혼입을 최소화할 수 있는 것으로 판단된다.

V. Conclusion

본 연구는 다크웹 환경에서 지능화되고 있는 비트코인 자금세탁을 효과적으로 추적하기 위해 서브그래프 기반의 GNN 믹싱 탐지 프레임워크를 제안하고 그 성능을 실증적으로 검증하였다. 기존 휴리스틱 기반 분류는 개별 트랜잭션의 구조적 특성만을 분석하므로, 믹싱 경로 내의 일반유형 트랜잭션을 탐지하지 못하는 한계가 있다. 실제 단일 트랜잭션 분류에서 믹싱 트랜잭션 비율이 범죄 연루 주소에서 25-35%에 불과하였다.

본 연구에서 제안하는 서브그래프 라벨링 기법은 윈도우 크기를 4로 설정했을 때 범죄 연루 주소의 믹싱 트랜잭션 탐지율이 90.8% 이상으로, 단일 트랜잭션 믹싱 탐지 비율 대비 약 3배 이상의 믹싱 탐지율을 달성하였다. 또한, 비범죄 주소에서 간헐적으로 발생하던 믹싱 트랜잭션 오탐은 연속적인 흐름을 반영하여 서브그래프에서 정상으로 분류되어 제거된다. 결과적으로 1%대였던 비범죄 주소의 믹싱 비율은 윈도우 크기 3 이상에서 0%로 수렴하여 탐지 오류를 효과적으로 제거하였다. 이는 범죄 자금이 추적 회피를 위해 지속적으로 믹싱 패턴을 보이는 반면, 일반 자금 흐름에서는 믹싱 유사 패턴이 단발성으로 드물게 발생하기 때문이다. 본 연구는 이러한 연속성 차이를 서브그래프 기반 분석을 통해 효과적으로 포착하여 두 클래스를 명확히 구분한다. 최종적으로 구축된 서브그래프 데이터셋을 활용한 GNN 분류 실험에서 선별된 7개 핵심 특징과 윈도우 크기를 4로 설정하여 학습했을 때, GraphSAGE 모델이 F1-score 98.5%의 최고 성능을 달성하였으며, GAT 모델도 98.4%의 높은 성능을 기록하였다. 또한, 전체 16개 특징을 사용한 학습과 비교 시 7개

선정 특징 학습이 우수한 성능을 보였으며, 피어슨 상관계수 기반의 특징 선정이 효과적임을 확인하였다. 이는 제안된 서브그래프 전처리 및 라벨링 방식이 믹싱 탐지 모델의 정확도와 효율성을 높이는 데 효과적임을 보여준다.

본 연구에서 제안한 모델은 비트코인 믹싱 서비스의 구조적 특징과 자금 흐름의 연속성을 정밀하게 분석함으로써, 기존 휴리스틱 탐지 기법의 한계를 보완하고 믹싱 트랜잭션의 식별력을 높였다는 점에서 의의가 있다. 그러나, 4개의 지갑 주소에서 수집한 트랜잭션만을 대상으로 하였으며, CoinJoin 기반의 믹싱에 초점을 맞추었다는 점에서 일반화에 한계가 있다.

향후에는 실제 여러 기법의 믹싱이 사용된 트랜잭션 데이터셋을 추가로 확장하여 구축하고, 본 연구에서 제안한 모델을 이더리움 및 브릿지(Bridge) 트랜잭션 등 다양한 환경에 적용하여 크로스체인(Cross-chain) 자금세탁까지 추적 가능한 통합 분석 모델로 발전시킬 예정이다. 또한 Random Forest, XGBoost 등 전통적 머신러닝 모델과의 비교 실험을 통해 GNN 기반 접근의 우수성을 입증하고, 실시간 탐지 및 실제 수사 도입을 위해 경량화된 GNN 아키텍처 연구와 시간 복잡도 최적화를 진행할 예정이다.

REFERENCES

[1] Ministry of Economy and Finance, "Digital asset (Virtual asset)," Dictionary of Current Economic Terms, https://www.moef.go.kr/sisa/dictionary/detail?idx=1732

[2] TradingView, “Crypto Market Dominance chart — Bitcoin dominance”, *https://kr.tradingview.com/markets/cryptocurrencies/dominance/*

[3] Financial Action Task Force (FATF), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paris, France, Oct. 2021.

[4] Europol, Internet Organized Crime Threat Assessment (IOCTA), The Hague, Netherlands, 2023.

[5] “Rapid Increase in Suspicious Cryptocurrency Transactions… 36,000 Cases in the First Eight Months of This Year,” Woman Economy Newspaper, 22 Sep. 2025, *https://www.womaneconomy.co.kr/news/articleView.html?idxno=242014*

[6] X. Hu, M. Gui, G. Cheng, R. Li, and H. Wu, “Multi-class Bitcoin mixing service identification based on graph classification,” Digital Communications and Networks, vol. 10, pp. 1881–1893, 2024, https://doi.org/10.1016/j.dcan.2024.08.010

[7] J. Zavřel, M. Koutenský, D. Dolejška, and V. Veselý, “Tumbling down the stairs: Exploiting a tumbler’s attempt to hide with ordinary-looking transactions using wallet fingerprinting,” Forensic Science International: Digital Investigation, vol. 52, Art. no. 301869, 2025, https://doi.org/10.1016/j.fsidi.2025.301869

[8] P. Tippe and C. Deckers, “Unmixing the mix: Patterns and challenges in Bitcoin mixer investigations,” Forensic Science International: Digital Investigation, vol. 52, Art. no. 301876, 2025, https://doi.org/10.1016/j.fsidi.2025.301876

[9] D. Mikhaylov, A. Kutin, J. Anderson, M. Falaleev, D. Sandzhiev, and H. Emam, “Cryptocurrency fund appropriation techniques: Analysis of strategies for ‘laundering’ and withdrawing stolen digital assets,” Journal of Information Security & Cybercrimes Research, vol. 8, no. 1, pp. 93–110, 2025, https://doi.org/10.26735/CZJK4881

[10] D. Andersson and A. Olsson, “The dark flows of cryptocurrency: An overview of money flow behaviors in Bitcoin transactions related to online criminal activities and Bitcoin mixers,” Bachelor’s thesis, Dept. Comput. Inf. Sci., Linköping Univ., Linköping, Sweden, 2024, https://www.diva-portal.org/smash/record.jsf?pid=diva2:1873090

[11] J. W. O’Meara, M. Taneja, J. Nicholls, N. Kothale, S. Flinter, and A. D. Jurcut, “Joindetect: A data-led machine learning approach to detection of CoinJoin transactions,” in Proc. Int. Conf. Inf. Technol. Social Good (GoodIT ’24), Bremen, Germany, 2024, pp. 5–13, https://doi.org/10.1145/3677525.3678633

[12] A. Arbabi, A. Shojaeinasab, and H. Najjaran, “Mixing services in Bitcoin and Ethereum ecosystems: A review,” IET Blockchain, vol. 5, p. e70021, 2025, https://doi.org/10.1049/blc2.70021

[13] M. A. A. Shawn, "Machine Learning-Driven Detection of Suspicious On-Chain Activity for Strengthening Security in Blockchain-Based Financial Transactions," Pacific Journal of Business Innovation and Strategy, vol. 2, no. 4, pp. 159–172, 2025, https://doi.org/10.70818/pjbis.v02i04.0136

[14] A. Asiri and K. Somasundaram, "Graph convolution network for fraud detection in bitcoin transactions," Scientific Reports, vol. 15, p. 11076, 2025, https://doi.org/10.1038/s41598-025-95672-w

[15] M. R. Raja, M. A. Hosen, M. F. Kabir, S. Sultana, S. A. Ashraf, and R. Islam, "Detecting and Preventing Money Laundering Using Deep Learning and Graph Analysis," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 16, no. 6, 2025, https://doi.org/10.14569/IJACSA.2025.0160601

[16] S. Ferretti, G. D’Angelo, and V. Ghini, "Enhancing Anti-Money Laundering Frameworks: An Application of Graph Neural Networks in Cryptocurrency Transaction Classification," IEEE Access, vol. 13, pp. 50201–50212, 2025, https://doi.org/10.1109/ACCESS.2025.3552240

[17] A. Shojaeinasab, "Decoding Illicit Bitcoin Transactions: A Multi-Methodological Approach for Anti-Money Laundering and Fraud Detection in Cryptocurrencies," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Victoria, Victoria, BC, Canada, 2024,

https://hdl.handle.net/1828/20454

[18] S. Chen, Y. Liu, Q. Zhang, Z. Shao, and Z. Wang, "Multi-Distance Spatial-Temporal Graph Neural Network for Anomaly Detection in Blockchain Transactions," Advanced Intelligent Systems, vol. 7, 2400898, 2025, https://doi.org/10.1002/aisy.202400898

[19] Y. Zhou, D. Bao, R. Xiong, W. Ren, C. Wu, H. Li, H. Sun, and S. Chen, "Next One: Predicting the Future Transaction of Illicit Address in Bitcoin Transaction Network by Graph Neural Network," Blockchain: Research and Applications, 100415, 2025, https://doi.org/10.1016/j.bcra.2025.100415

[20] X. Huang, C. Zhao, X. Li, C. Feng, and W. Zhang, "GAM-CoT Transformer: Hierarchical Attention Networks for Anomaly Detection in Blockchain Transactions," Journal of Emerging Applied Artificial Intelligence (JEAAI), 2025, https://doi.org/10.65563/jeaai.v1i3.32

[21] P. Celik and E. Sefer, "Analyzing Transaction Graphs via Motif-Based Graph Representation Learning for Cryptocurrency Price Prediction," Computational Economics, 2025, https://doi.org/10.1007/s10614-025-10940-1

[22] M. T. Le, O. Harris, C. Bennett, and F. Greene, "Behavior Path Analysis for Blockchain Fraud Detection Using Graph Neural Architectures," Frontiers in Applied Physics and Mathematics, vol. 2, no. 1, pp. 13–20, 2025, https://doi.org/10.71465/fapm229

[23] Y. Elmougy and L. Liu, "Demystifying Fraudulent Transactions and Illicit Nodes in the Bitcoin Network for Financial Forensics," in Proc. 29th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining (KDD '23), Long Beach, CA, USA, 2023, pp. 3979–3990, https://doi.org/10.1145/3580305.3599803

[24] L. Wu, Y. Hu, Y. Zhou, H. Wang, X. Luo, Z. Wang, F. Zhang, and K. Ren, "Towards Understanding and Demystifying Bitcoin Mixing Services," in Proc. The Web Conf. 2021 (WWW '21), Ljubljana, Slovenia, 2021, pp. 33–44, https://doi.org/10.1145/3442381.3449880

[25] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the Bitcoin ecosystem," in Proc. 2013 APWG eCrime Researchers Summit (eCRS), 2013, pp. 1–14, https://doi.org/10.1109/eCRS.2013.6805780

[26] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies," Proc. Priv. Enhancing Technol. (PoPETs), vol. 2018, no. 4, pp. 179–199, 2018, https://doi.org/10.1515/popets-2018-0038

Authors

Hyeon-Woo Lee received the B.S. degree in computer engineering from Daegu University, Gyeongsan, South Korea, in 2025, where he is currently pursuing the M.S. degree in computer engineering.

His research interests include cybersecurity, artificial intelligence, and blockchain.

Eun-Young Park received the B.S. degree in computer engineering from Daegu University, Gyeongsan, South Korea, in 2025, where she is currently pursuing the M.S. degree in computer engineering.

Her research interests include cybersecurity, artificial intelligence, and digital forensics.

Sooncheol Kim received the B.S., M.S. and Ph.D. degrees in Computer Engineering from Seoul National University, Seoul, Republic of Korea, in 1990, 1992 and 1998, respectively. Dr. Kim joined the faculty of the Department of Computer Engineering, Daegu University, Gyeongsan, South Korea, in 1999 and is currently a Professor in the Department of Computer Engineering, Daegu University. His research interests include embedded system software, storage systems and computer security.

Jiyeon Kim received the B.S. and Ph.D. degrees in information security engineering from Seoul Women's University, Seoul, South Korea, in 2007 and 2013, respectively. Dr. Kim was a Postdoctoral Research Associate in the Department of Electrical and Computer Engineering, Carnegie Mellon University, United States, from 2014 to 2017. She is currently an Assistant Professor in the Department of Computer Engineering, Daegu University, Gyeongsan, South Korea. Her research interests include cybersecurity, cybercrime investigation, cloud computing,artificial intelligence, and critical infrastructure protection.