

DEOBFUSCATOR

Sequence Diagram

2025.05.03

컴퓨터융합학부 202002514 안상준
인공지능학과 202202487 박혜연
컴퓨터융합학부 202202602 손예진

Contents

01	—————	연구 배경/목적
02	—————	연구 질문/가설
03	—————	소프트웨어 사용 사례
04	—————	문제 해결에 대한 사용 사례
05	—————	해결 방법에 대한 알고리즘 순서도

01 연구 배경/목적

연구 배경

다양해지는 난독화 기술로 인해 악성코드 해석이 어려워지고 있음, 데이터셋 부족과 신뢰성 문제로 보안 분야에서 LLLM이 활용되지 않음

→ LLM을 사용한 역난독화 도구 개발로, 가상화 기반 난독화 된 코드 분석에 활용

주제

바이너리 프로그램에서 제어구조를 식별하는 도구 개발

연구 목적

여러 난독화 기법에 대해 범용적으로 적용 가능한 도구
LLM 기반 역난독화 가능성 검증

→ 가상화 난독화 기반 악성코드에 대한 분석 효율성 향상
및 역공학 기술 발전에 기여

02 연구 질문/가설

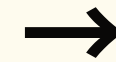
연구 질문

RQ1

LLM 기반 제어구조 식별 도구를 활용한 가상화 난독화 코드 분석이 기존의 방식에 비해 제어구조 식별 정확도에 어떠한 영향을 미치는가?

RQ2

LLM 기반 제어구조 식별 도구는 난독화 난이도나 코드 복잡도에 따라 제어구조 식별 성능에 차이를 보이는가?



가설

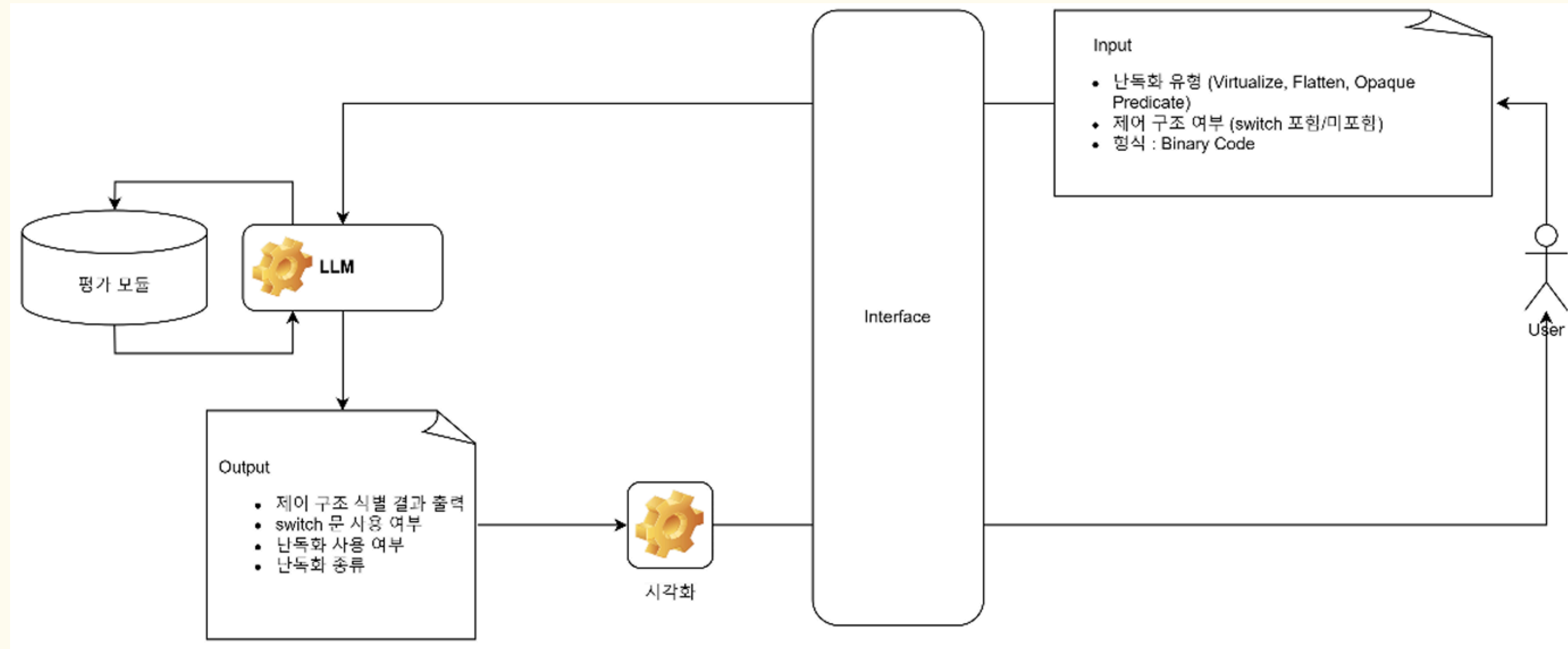
H2

LLM 기반 제어구조 식별 도구를 활용한 가상화 난독화 코드 분석이 기존 방식보다 제어구조 식별 정확도를 유의미하게 향상시킬 것이다.

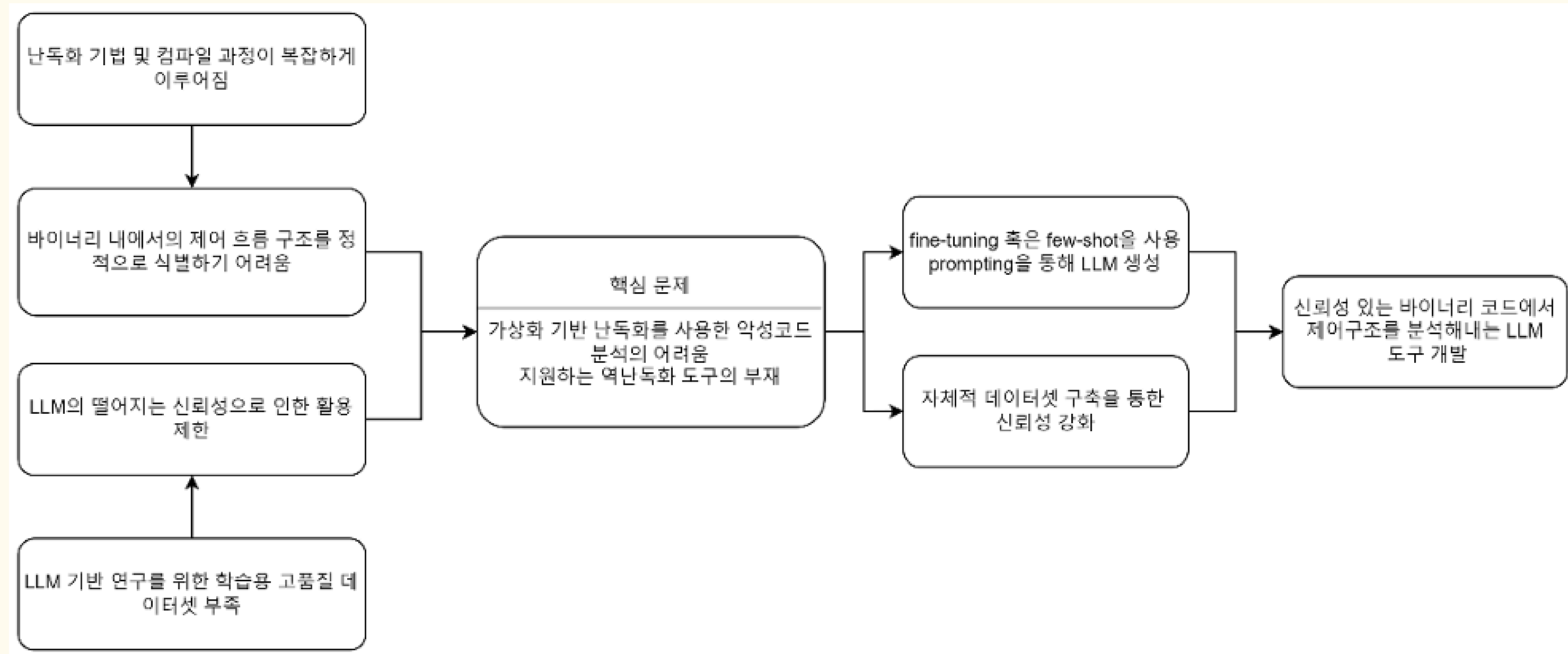
H2

LLM 기반 제어구조 식별 도구는 다양한 난독화 난이도 및 코드 복잡도 조건에서도 안정적인 제어구조 식별에 성과 향상을 보일 것이다.

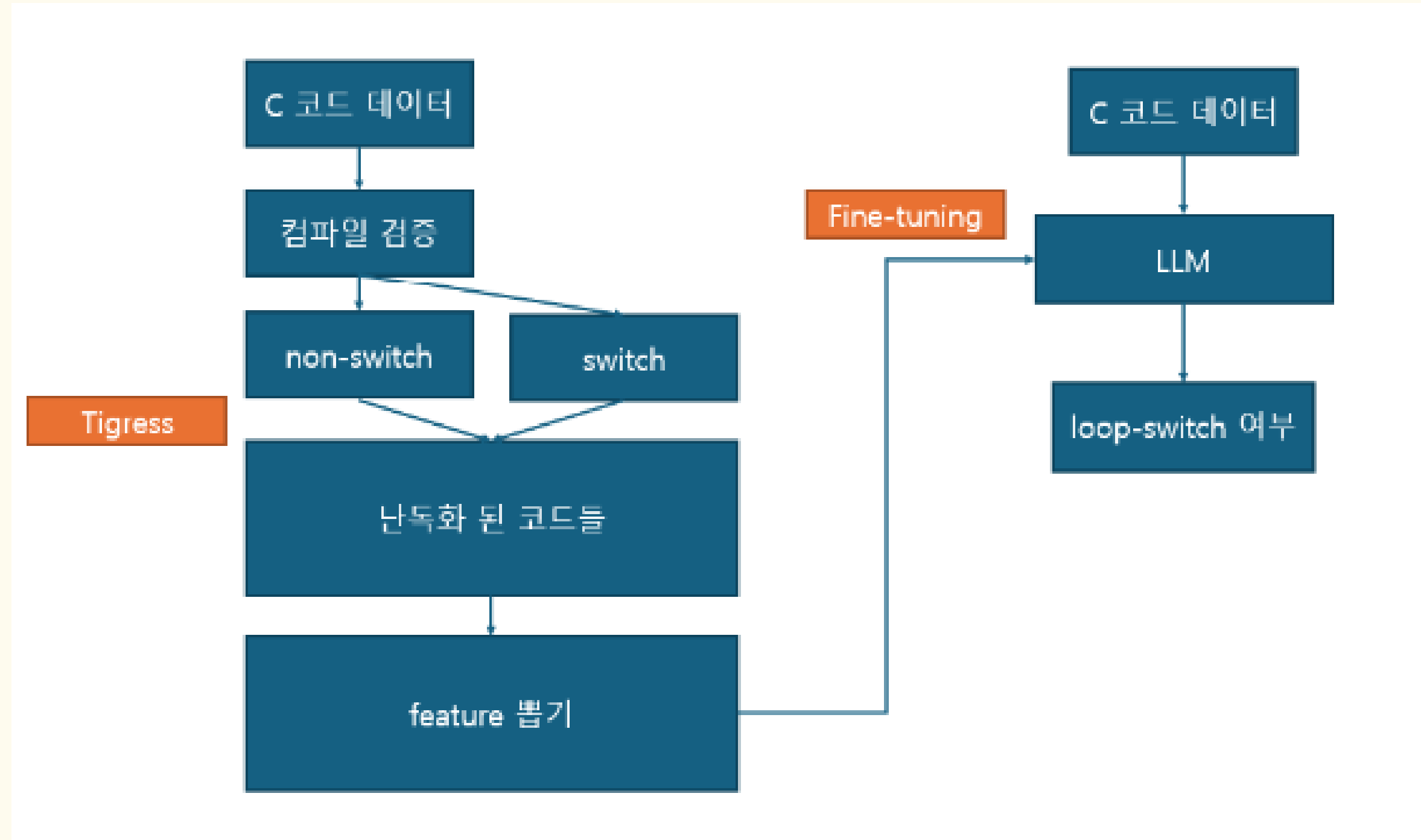
03 소프트웨어 사용 사례



04 문제 해결에 대한 사용 사례



05 해결 방법에 대한 알고리즘 순서도



결과를 바탕으로
난독화 난이도, 코드 복잡도에 따른 성능 차이 분석,
제어구조 식별 여부와 가상화 난독화 연구지원 가능성 논의

DEOBFUSCATOR

감사합니다

컴퓨터융합학부 202002514 안상준
인공지능학과 202202487 박혜연
컴퓨터융합학부 202202602 손예진