

# Mnemosyne AI

Spatial Memory and Adversarial Robustness  
Testing of Vision Models

電機系 E24096603 張育榮



# Outline

1. 問題背景與動機
2. 專案目標與核心功能
3. 系統架構
4. 技術方法詳解
5. 時間規劃與任務分工
6. 期望成果與展示

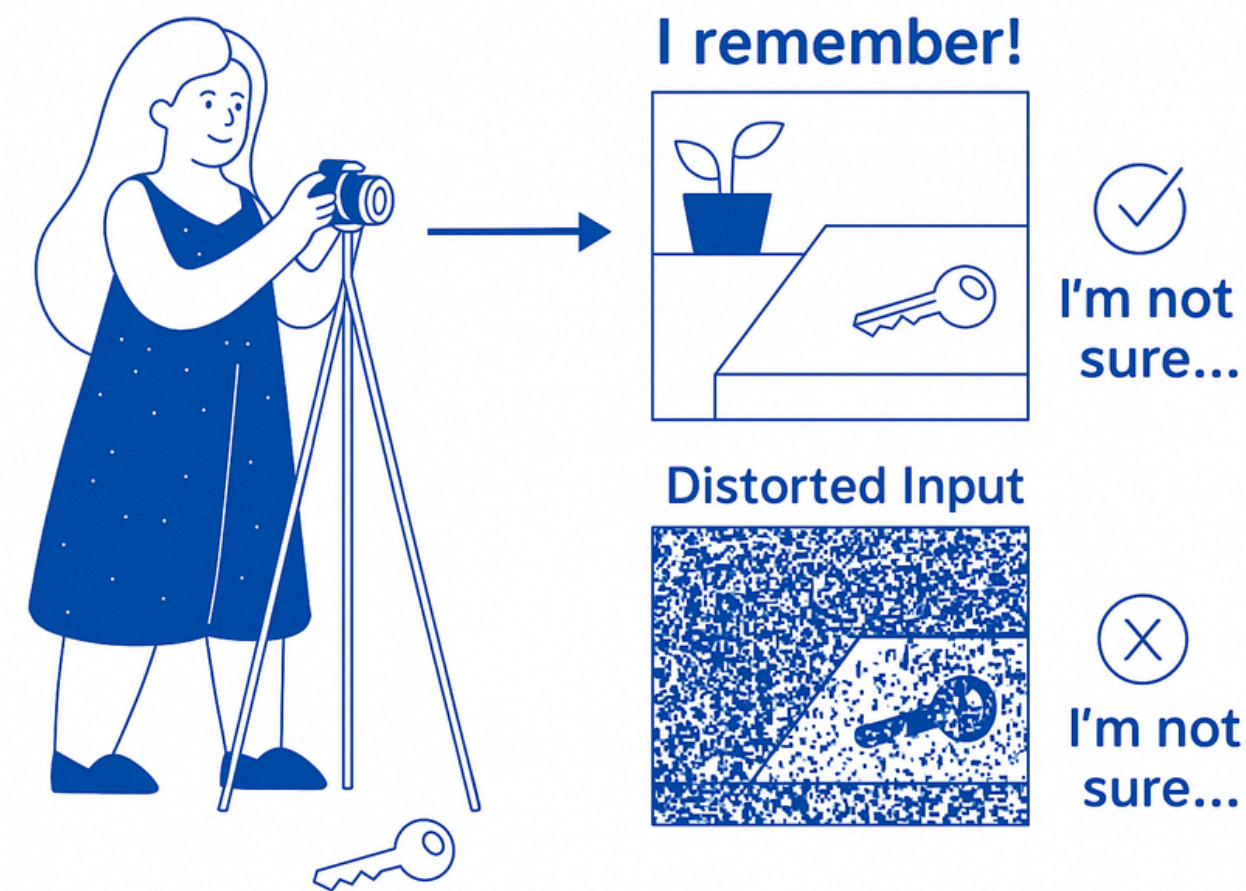


# 問題背景與動機

為什麼要「讓 AI 記得物品位置」？

為什麼要考慮「對抗樣本」？

為什麼選擇「手機部署」？



# 專案目標與核心功能

## 物品辨識

- 用 MobileNet-SSD / YOLO 模型找出常見物品

## 空間記憶

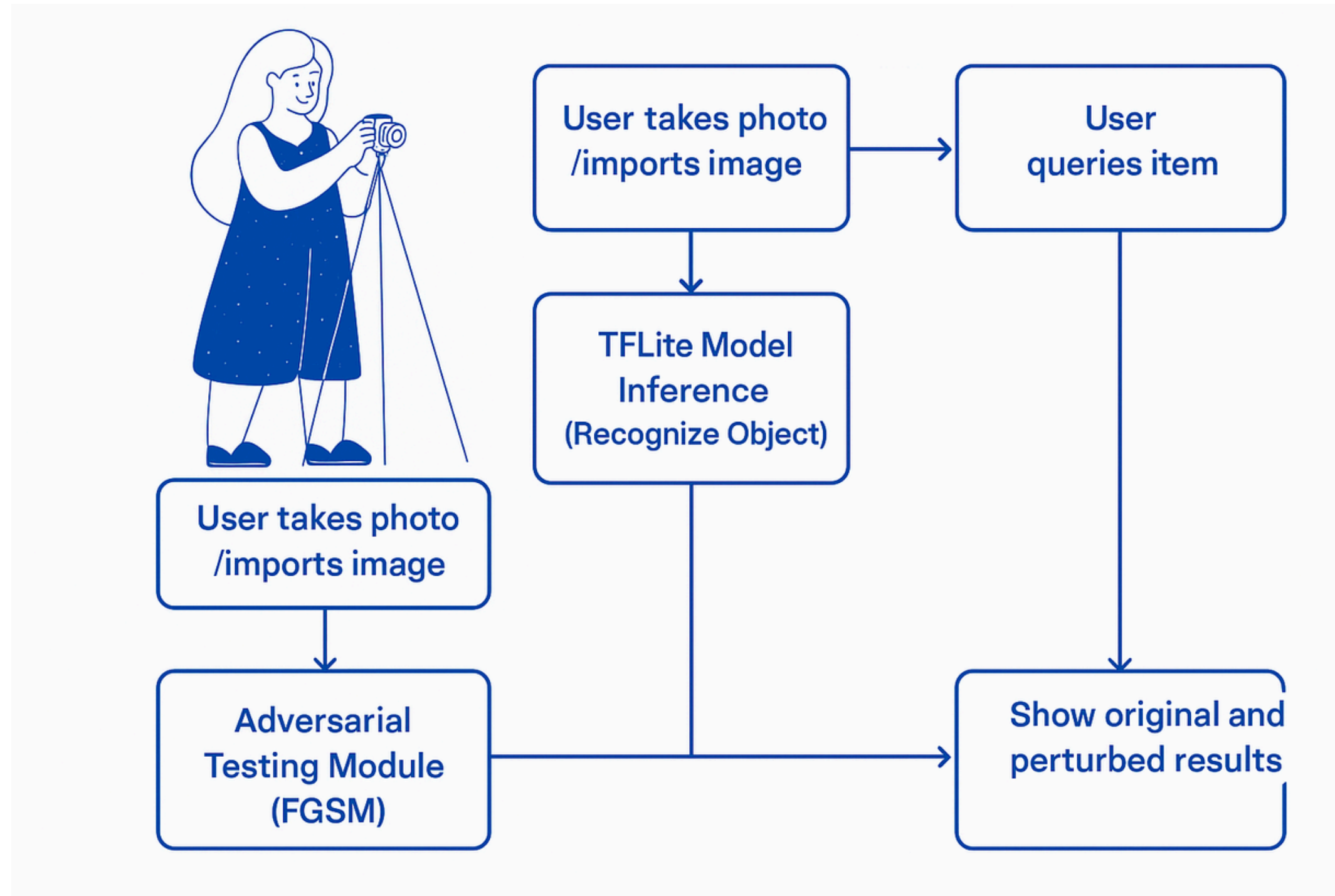
- 儲存物品在畫面中的位置與時間，支援查詢

## 對抗樣本測試

- 用 FGSM 生成微擾圖，展示辨識出錯風險



# 系統架構



# 技術方法詳解

## AI模型選擇

- YOLOv8-tiny、MobileNet-SSD

## 對抗樣本技術

- Fast Gradient Sign Method (FGSM)

## 資料儲存與查詢

- SQLite 儲存：`{object_name, bbox, time}`





# 時間規劃與任務分工



## Week 1

- 模型選擇與 Android App 架構建立



## Week 2

- 完成物品辨識與記憶儲存



## Week 3

- 對抗樣本實作與展示畫面

# 期望成果與展示

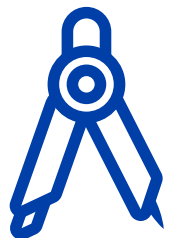


**Demo: 實際操作手機App或網站頁面**



## 預期成果

- 能記住物品、能回想位置



## 展示畫面

- 使用者按「查詢剪刀」→ App 顯示哪個時間點在畫面哪裡偵測到剪刀
- 「對抗樣本測試」→ 原圖與對抗圖，誤判截圖並列展示

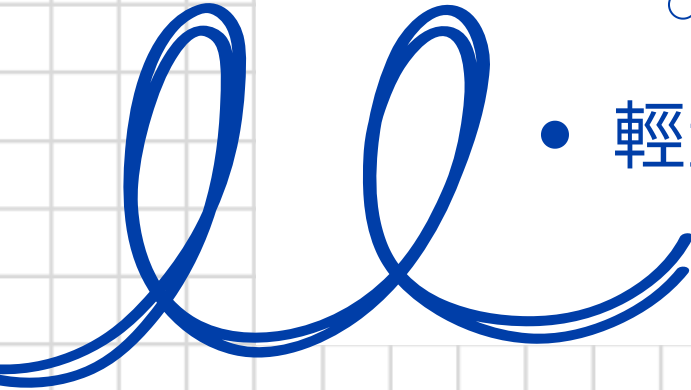
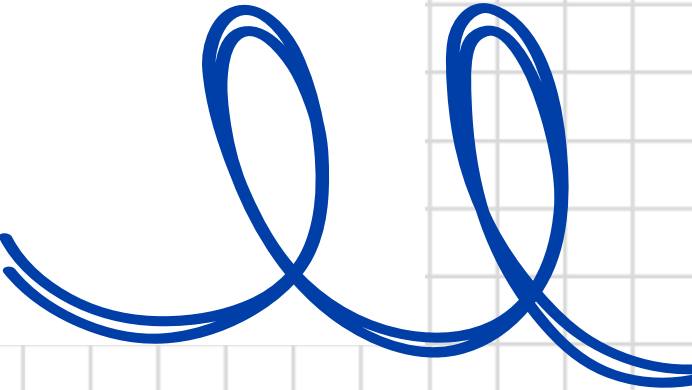






# 創新與貢獻



- 空間記憶系統
    - 在手機端進行部署（強調可攜性與實用性）
    - 結合對抗性樣本測試（強調安全性與AI防禦能力）
    - 打造一個互動式可記憶+可測試的AI系統
  - 輕量化＋安全性實驗可作為未來「安全無人機記憶系統」前身
- 
- 

# Thank you for your listening!

