基於 GAN 校準的半監督學習專案計畫

第一部分：專案目標與資料準備

1.1 專案目標

本專案的核心目標是：透過一個基於生成對抗網路（GAN）的校準模組，來提升由半監督式學習產生的偽標籤的準確率，從而增強最終物件偵測模型的泛化能力。

1.2 資料準備

- **資料來源**：使用約 10,000 張的公開 people 物件資料集(皆含有高品質標註)。
- **資料劃分**：將所有帶有正確標籤的資料，一次性地劃分為三個獨立的子集：
    1. labeled：一個較小的、帶有高品質標註的資料集，用於初始模型訓練。
    2. unlabeled：一個較大的、僅包含影像的資料集，用於生成偽標籤。
    3. testset：一個獨立的測試集，用於每個階段模型進行性能評估。

第二部分：四階段循環式訓練流程

階段一：監督式預訓練

這是整個流程的起點，旨在訓練出一個強大的基礎「教師模型」。

- **目的**：利用有限的高品質標註資料，訓練出一個性能最優的基礎 YOLO 模型。
- **方法**：使用 labeled 資料集進行標準的監督式訓練。
- **產出**：一個基礎模型權重檔（例如 person_v1.pt）。

階段二：雙軌偽標籤生成

由於在階段三 GAN 訓練時須使用帶有標準答案資料，所以設計了兩條不同的標註方式的軌道，其一是用於 GAN 訓練另一個則是用於最終校準。

- **K-fold 交叉偽標註**（用於 GAN 訓練）：
    - **目的**：為 GAN 提供帶有預測框以及真實框樣本(因須對同組 labeled 樣本進行標註，若採用原教師模型預測可能產生過擬合)。
    - **方法**：採用 K-Fold 交叉驗證。對原始的 labeled 資料集進行

K-Fold 切分，用 K-1 折訓練的模型去預測剩餘的 1 折，從而得到一套覆蓋全部標註資料的(預測框, 真實框) 數據對。

- **兩階段式偽標註**（用於最終校準）：
  - **目的：**為大量未標註資料生成需要被校準的候選偽標籤。
  - **方法：**採用兩階段式生成法。
    1. 第一階：使用階段一產生的教師模型，對 unlabeled 資料集進行預測，僅儲存置信度高於某個閾值的偽標籤。
    2. 第二階：在第一階篩選出的影像上，使用一個較低的置信度閾值再次預測，以補足遺漏的偵測。

階段三：CGAN 訓練

以 pix2pix 作為基礎進行改寫，延續了 的「局部對抗」優點，但把影像到影像轉換改寫成 「影像 → 邊框校正量」的回歸問題，以解決偽標籤定位誤差。

- 目的：訓練一個 cGAN 模型，使其學會如何修正偽標籤的定位誤差。
- **生成器 (Generator, G)：**
  - **架構：**使用 U-Net 為骨幹，保留上下採樣與跳接 (skip connections)。
  - **任務：**學習預測一個能修正偽標籤的修正向量 Δ。
  - **輸入：**一張經過 Letterbox 處理、大小固定的小影像區塊 (patch)，內容是目標偽標籤框所圈出的影像。
  - **輸出：**四個連續值，分別代表預測框中心點在水平與垂直方向的偏移量，以及寬、高縮放率 (dx, dy, dw, dh)。
  - **損失函數：**採用 BCEWithLogits Loss + Smooth-L1 Loss
- **判別器 (Discriminator, D)：**
  - **架構：**採用 PatchGAN 設計，使用分數圖記錄而非單一分數。
  - **任務：**學習分辨哪些是 refined patch 或是 GT patch。
  - **輸入：**同時餵入「預測 patch」與另一張比較 patch（可能是 GT 或經生成器修正後的 refined patch)。
  - **輸出：**一個 0 到 1 之間的機率值，代表輸入 Patch 的真實度。
  - **損失函數：**採用 BCEWithLogits Loss
- **對抗訓練流程：**
  - **更新生成器**
    - **目標一：**說服判別器相信「修正後的 patch」屬於真實 patch。
    - **目標二：**讓預測偏移量與真實偏移量盡可能接近。
    - 損失函數因此同時包含對抗損失（生成-對抗）與回歸損失 (偏移誤差)。
  - **訓練動態裁圖(patch)**

        - 生成器輸出偏移量後，將原影像根據偏移量裁切出校準後 patch。
    - **更新判別器**
        - **目標一：**分辨數據對是 pred patch + GT patch 或 pred patch + refined patch。
        - **目標二：**保持訓練平衡，使判別器不致過強（導致生成器梯度消失），也不致過弱（無法提供資訊）。

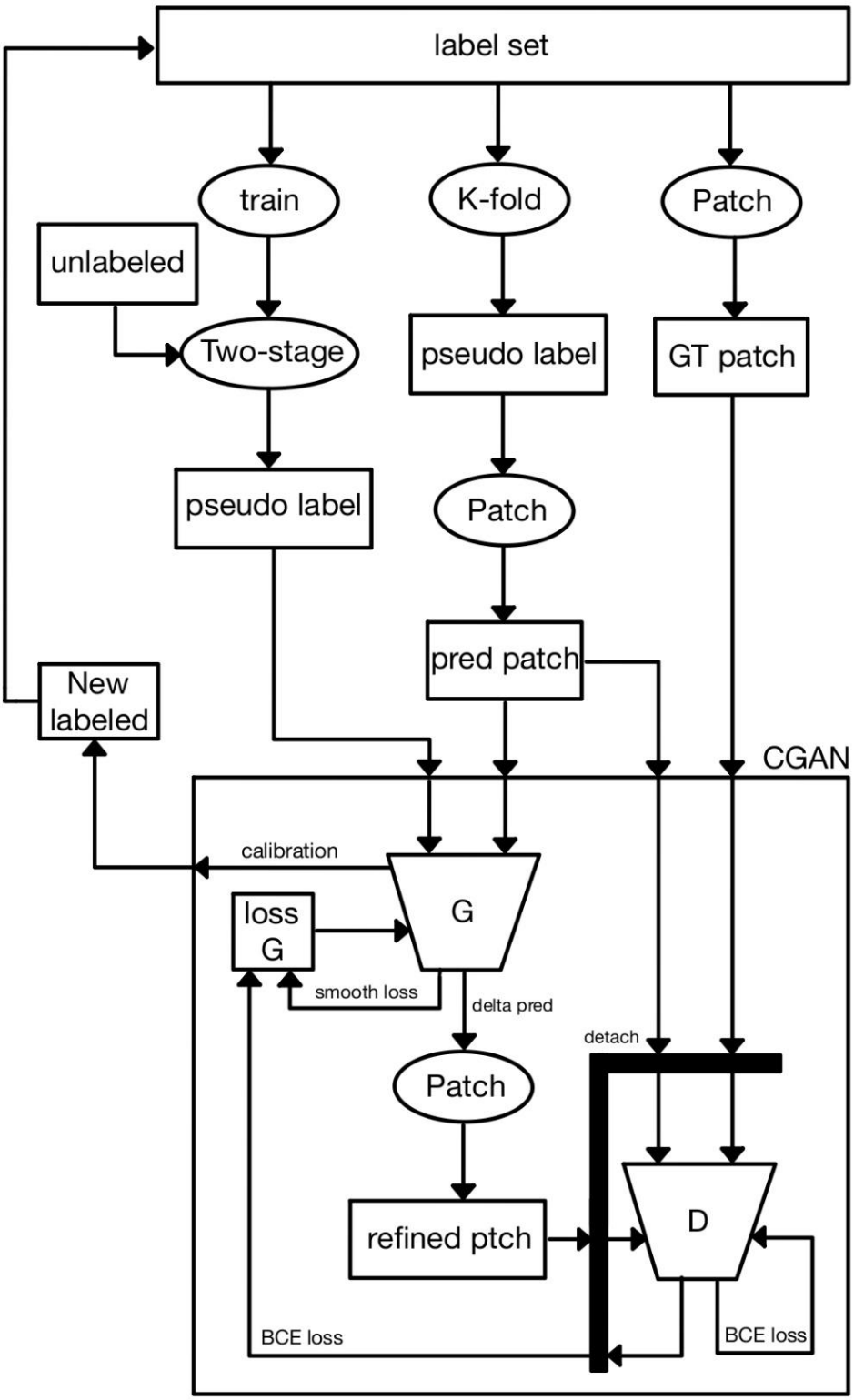
階段四：校準與循環

- **目的：**將兩階段式偽標註生成之偽標籤校準，並加入原資料集循環訓練。
- **方法：**
    1. 使用訓練好的生成器，對兩階段式偽標籤進行校正。
    2. 將校準好的偽標籤，加入到原始的 labeled 資料集中。
    3. 使用這個擴充後獲得更高品質的數據集，返回階段一，重新訓練一個新的、更強大的教師模型。
    4. 重複 階段一 -> 階段二 -> 階段三 的循環，形成螺旋式增益。

第三部分：成果評估

- **偽標籤品質評估：**在每個循環的階段二結束後，依據真實標籤來計算偽標籤的 TP, FP, FN, Precision, Recall, F1-Score 等指標，以量化偽標籤生成策略的有效性。
- **模型泛化能力評估：**在階段四的每個循環結束後，使用獨立的 testset 來評估當前模型的最終性能，並記錄 mAP50 和 mAP50-95 指標，最終製作成圖表以清晰地展示模型的泛化能力提升。

流程圖：


label set
train
K-fold
Patch
unlabeled
Two-stage
pseudo label
GT patch
pseudo label
Patch
pred patch
New labeled
CGAN
calibration
G
loss G
smooth loss
delta pred
detach
Patch
refined ptch
D
BCE loss
BCE loss