

#### 4. Building a Neural Net

Imagine you're going to implement a deep neural network which detects human faces appear in video frames captured by a surveillance camera in your office. You have created a network architecture includes a brand-new network layer you've implemented by yourself. You now have 100,000 labeled face images collected from some social media. Those images are mostly captured and uploaded with the mobile devices (e.g., selfies) of the social media users. Also, you have 1,000 labeled image frames collected directly through the surveillance camera in your office.

**How would you arrange your 101,000 images for model training?**

Once you've built your self-implemented neural network. What would you do to sanity check the implementation before you start your massive network training workload?

第一個問題：

資料集分析：

- 社交媒體影像：100,000 張標註照片（主要為手機自拍）
- 監控攝影機影像：1,000 張辦公室環境照片
- 總計 101,000 張標註影像，社交媒體資料：監控資料 = 100:1 的極端比例，兩類資料在影像特徵上存在顯著差異（拍攝角度、光線條件、影像品質等）

# 處理方式：

## 1. 資料擴增策略

- 傳統方法：對監控影像進行旋轉、縮放、光線調整、雜訊添加
- 生成式 AI 方法：使用 Stable Diffusion 等模型生成相似監控場景影像
- 優點：直接增加目標域資料量
- 限制：擴增資料品質可能無法完全媲美真實資料

## 2. 損失函數權重調整

- 使用加權損失函數 (Weighted Loss Function)，為監控影像資料分配更高的損失權重（如 100:1 的反向權重）
- 確保模型對少數類別給予足夠關注
- 優點：實作簡單，無需額外資料
- 考量：需要仔細調整權重比例，避免過度補償

## 3. 遷移學習

- 使用在大型自然影像資料集（如 ImageNet）上預訓練的模型
- 保留底層特徵提取能力，僅微調高層分類器
- 優點：利用豐富的預學習特徵，提升模型泛化能力
- 適用性：特別適合資料量有限的情況

## 4. 階段性訓練策略

### 第一階段：基礎模型訓練

- 使用 100,000 張社交媒體資料進行初步訓練
- 建立強健的人臉檢測基礎能力
- 採用標準的訓練/驗證分割（如 80:20）

### 第二階段：領域適應微調

- 使用 1,000 張監控資料進行 fine-tune
- 降低學習率，專門優化目標應用場景的檢測效果

## 第二個問題：

在開始大規模訓練之前，建議進行以下檢查步驟：

### 1. 架構驗證檢查

- 確認資料載入和預處理正確
- 驗證批次生成和標籤對應正確

### 2. 小規模功能測試

- 使用 10-100 個樣本進行過擬合測試
- 觀察損失函數下降趨勢，確認訓練過程穩定且無異常

### 3. 驗證學習能力

- 使用小型資料集進行短期訓練
- 觀察不同學習率下的收斂情況