影像分類攻擊方法模組圖形化介面 使用說明書

撰寫日期：2022/04/23

目錄

一、 執行說明

1. 直接執行 EXE 檔案

「ART_Tool.exe」為影像分類攻擊方法模組程式。請注意，本程式只能運行在 **Windows 64 位元** 作業系統上，並且不支援 GPU 運行，只能運行在 CPU 上。

執行 EXE 檔方式支援後接參數設定，詳情請至「執行參數說明」查看。

2. 透過 Python 執行

本程式可以運行在 Python 相關虛擬環境中，像是 Anaconda。請注意，本程式只支援 **Python 3.8** 版本，在安裝相關環境前，請先注意 Python 版本是否正確。「requirements.txt」為安裝 Python 相關環境需求，可透過在終端機中執行「pip3 install -r requirements.txt」 來安裝。

安裝環境完成後， 執行「python ART_Tool_RGB.py」就可以執行圖形化介面。執行 Python 檔方式也支援後接參數設定，詳情請至「執行參數說明」查看。

二、 圖形化介面說明

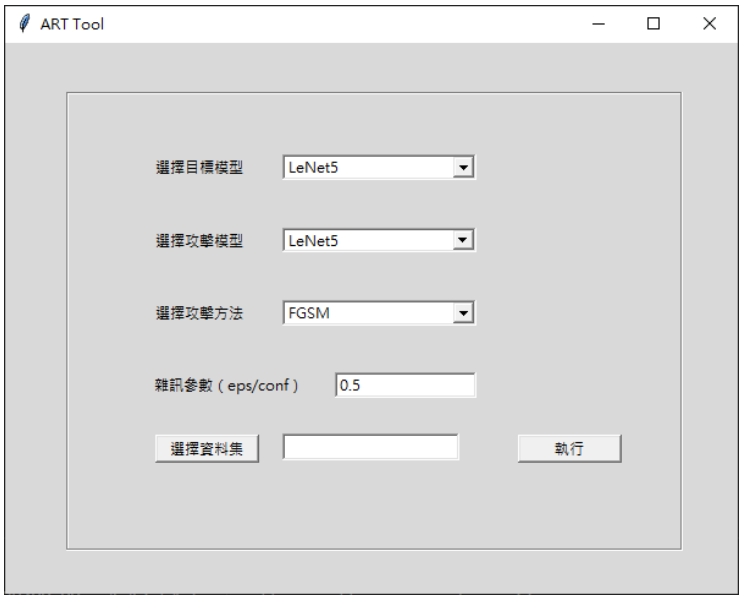

圖 1、圖形化介面

「選擇目標模型」、「選擇攻擊模型」、「選擇攻擊方法」為透過下拉選單來選擇，「雜訊參數」需自行輸入，否則為預設值「0.5」。如果為輸入 eps 擾動參數，建議輸入值介於 0 到 1 之間的浮點數，如果為輸入 conf 置信度，則建議輸入值介於 0 到 16 之間的整數。

按下「選擇資料集」後，會進入選擇資料夾視窗，接受的資料夾格式請參見「資料集說明」。

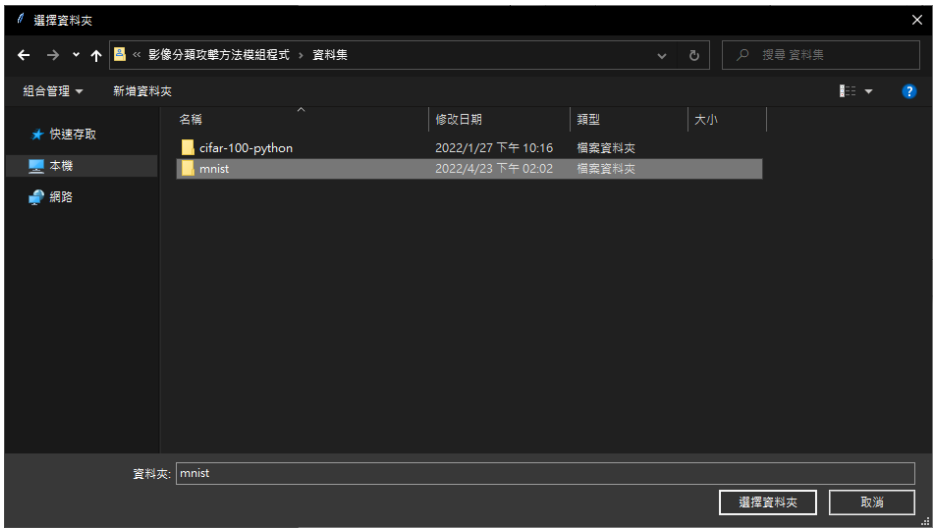

圖 2、選擇資料夾視窗

三、 資料集說明

選擇一個資料夾路徑，該資料夾底下必須包含名稱為「train」及「test」的兩個子資料夾，各自代表訓練資料集及測試資料集。其中資料集的架構，同一分類的圖片必須存在同一資料夾，且資料夾名稱為該類別的名稱。圖片檔名不影響程式運作。可接受 PNG 檔及 JPEG 檔的圖片檔案類型。

1. MNIST 手寫辨識資料集 範例

以下為 MNIST 手寫辨識資料集架構，以作為可接受資料集架構範例：

```
mnist /      <=== 圖形介面選擇的資料集路徑
├── train/         <=== 訓練資料集
│   ├── 0/      <=== 類別為「0」的圖片資料夾
│   │   ├── train_0_1.png   <=== 檔名不影響
│   │   ├── train_0_2.png
│   │   └── ...
│   │
│   ├── 1/      <=== 類別為「1」的圖片資料夾
│   ├── 2/
│   ├── ...
│   └── 9/
│
└── test/          <=== 測試資料集
    ├── 0/
    ├── ...
    └── 9/
```

四、 執行參數說明

本程式支援參數設定，指令格式為

```
{ART_Tool.exe 或 python ART_Tool_RGB.py} [-h] [--interface INTERFACE]
   [--cuda CUDA] [--dataset-path DATASET_PATH] [--num-workers NUM_WORKERS]
   [--norm] [--predict-model PREDICT_MODEL] [--attack-model ATTACK_MODEL]
   [--white-box] [--attack-func ATTACK_FUNCTION] [--max-iter MAX_ITER]
   [--eps EPS] [--conf CONFIDENCE] [--epochs EPOCHS] [--batch-size BATCH_SIZE]
   [--optim OPTIM] [--lr LR] [--momentum MOMENTUM]
```

範例

```
ART_Tool.exe --epochs 5 --lr 0.01
python ART_Tool_RGB.py --num-workers 4 --norm
```

1. 個別參數說明

參數	後接參數	說明	預設值
-h, --help	無	顯示參數說明	無
--interface	INTERFACE	選擇設定參數方式 (1:GUI 介面, 2:標準輸入, 3:執行參數)	1
--cuda	CUDA	設定運行 GPU 的 id，本程式不支援	不支援
--dataset-path	DATASET_PATH	設定資料集路徑	無
--num-workers	NUM_WORKERS	設定執行緒數量	8
--predict-model	PREDICT_MODEL	選擇目標模型 (1:LeNet5, 2:CNN, 3:AlexNet, 4:GoogLeNet, 5:VGG19, 6:ResNeXt101)	1
--attack-model	ATTACK_MODEL	選擇攻擊模型 (1:LeNet5, 2:CNN, 3:AlexNet, 4:GoogLeNet, 5:VGG19, 6:ResNeXt101)	1
--white-box	無	設定白盒實驗	否
--attack-func	ATTACK_FUNCTION	選擇攻擊方法 (1:FGSM, 2:BIM, 3:PGD, 4:C&W L2, 5:C&W Linf)	1
--max-iter	MAX_ITER	設定最大迭代次數	20
--eps	EPS	設定擾動參數	0.1
--conf	CONFIDENCE	設定置信度	無
--epochs	EPOCHS	設定訓練回合數	20
--batch-size	BATCH_SIZE	設定 batch 值	32
--optim	OPTIM	設定優化器	SGD
--lr	LR	設定學習速率	0.001
--momentum	MOMENTUM	設定 SGD 的 Momentum 值	0.9