**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](#_Toc101634269)

[1. 直接執行 EXE檔案 1](#_Toc101634270)

[2. 透過Python執行 1](#_Toc101634271)

[二、 圖形化介面說明 2](#_Toc101634272)

[三、 資料集說明 3](#_Toc101634273)

[1. MNIST手寫辨識資料集 範例 3](#_Toc101634274)

[四、 執行參數說明 3](#_Toc101634275)

[1. 個別參數說明 4](#_Toc101634276)

# 執行說明

## 直接執行 EXE檔案

「ART\_Tool\_CPU.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](#_執行參數說明)」查看。

## 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](#_執行參數說明)」查看。

# 圖形化介面說明

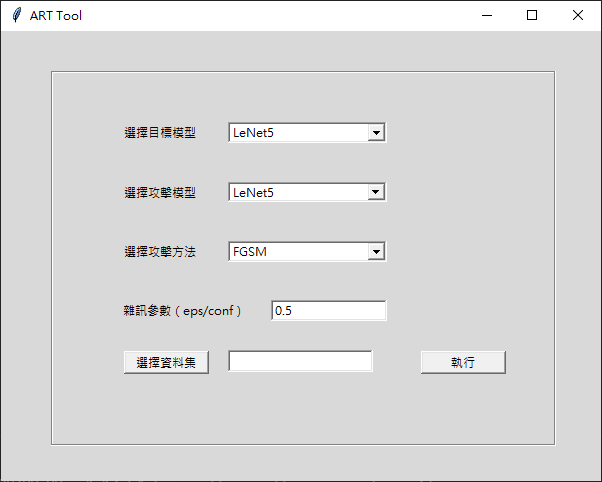


圖1、圖形化介面

「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](#_資料集說明)」。

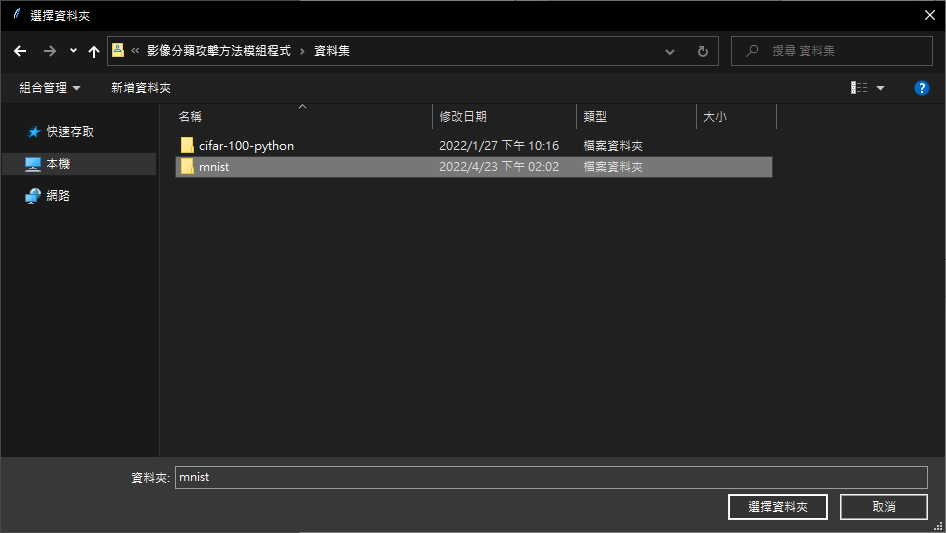


圖2、選擇資料夾視窗

# 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。

## 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/

# 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

## 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 |