Introduction To Information Security

Midterm Proposal

Multimedia Security

Face De-identification

台灣科技大學 資訊工程系

B10933029 呂欣怡

B10932017 張祐禎

B10931040 吳閩閩

目錄

一、專案目標-------------------------------------------------------------------------------------------3

二、專案內容-------------------------------------------------------------------------------------------3

(一)專案介紹-------------- -----------------------------------------------------------------------4

(二)實驗結果-------------------------------------------------------------------------------------6

一、專案目標

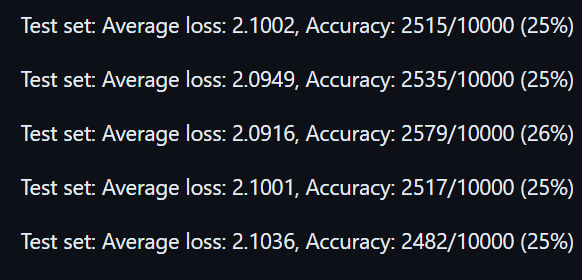
藉由AI神經網路中Mnist、CIFAR-10、AT&T dataset去實作人臉去識別化

二、專案內容

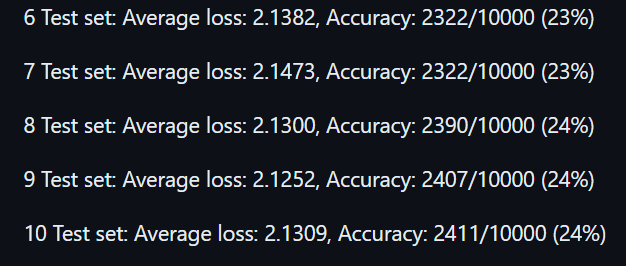
1. 專案介紹

人臉去識別化是從面部的圖像或影像中，藉由修改或刪除部分或全部識別特徵以保護個人隱私的過程，其目標是防止某些識別的特定的數據集中於特定的某些人，同時仍然保留人臉的整體結構和外觀。面部去識別通常用於研究和數據收集，特別是在醫療保健和執法等必須保護個人隱私的領域，以及於機場或購物中心等公共場所，出於安全目的使用視頻監控，以保護可能被鏡頭捕捉到個人的隱私。人臉去識別化有多種方法，包括對人臉進行模糊處理或像素化、添加噪音或失真，或者用合成人臉替換人臉， 這些技術可應用於靜止圖像或視頻片段。

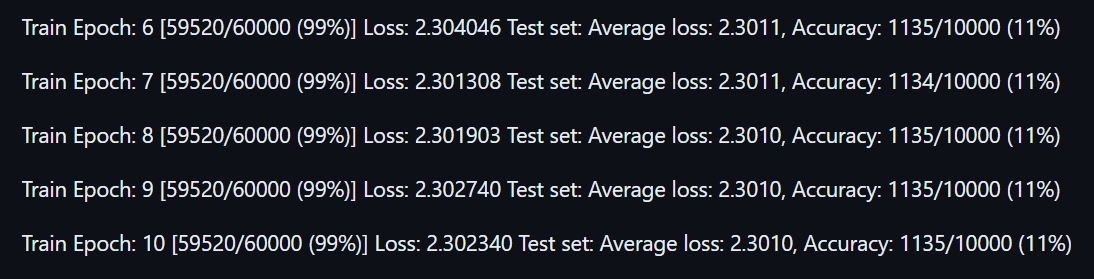
1. 實驗結果
2. Mnist Database Training Result
3. Gaussian =15



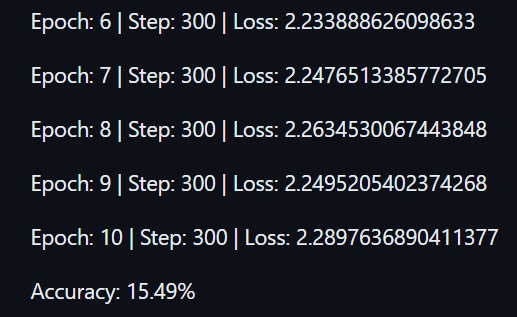
1. Gaussian =45



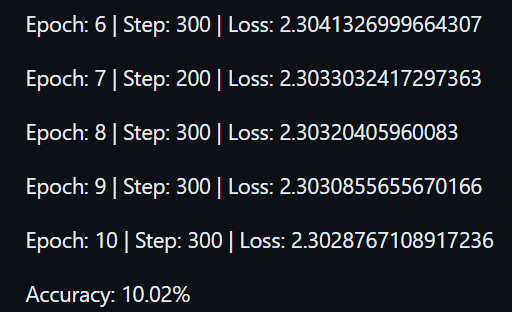
1. Gaussian =99



2.CIFAR-10 Database Training Result  
(1) Gaussian = 15



(2) Gaussian = 45



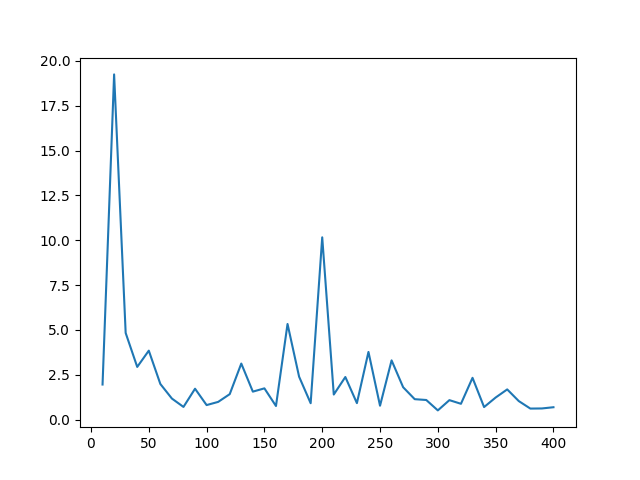
(3)Gaussian = 99



3.AT&T Database Training Result

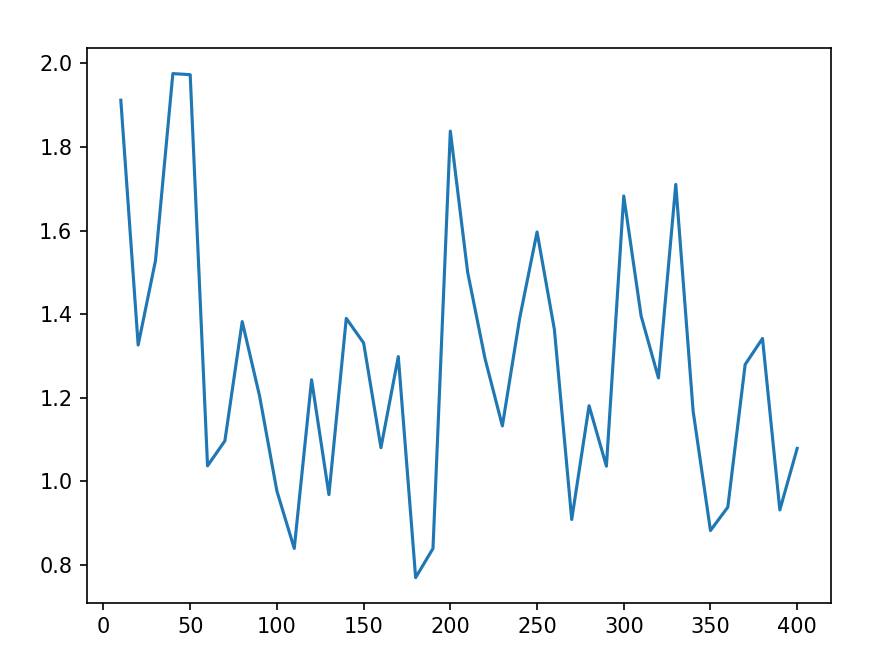
(1) Without Gaussian

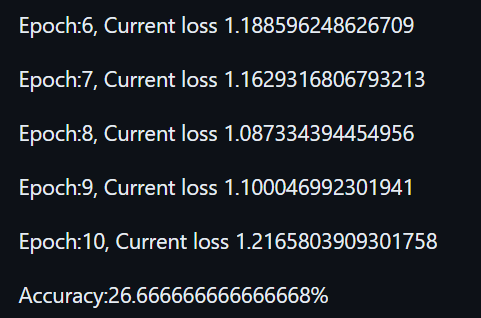
a. Loss function change curve



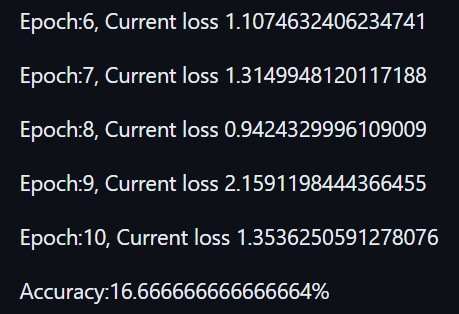
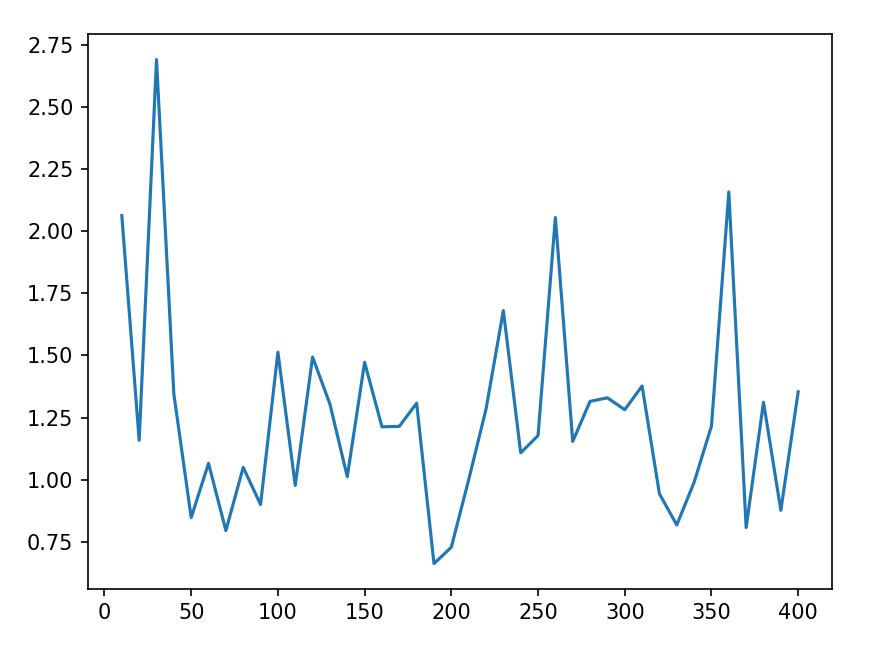
(2) Gaussian = 15

a. Loss function change curve

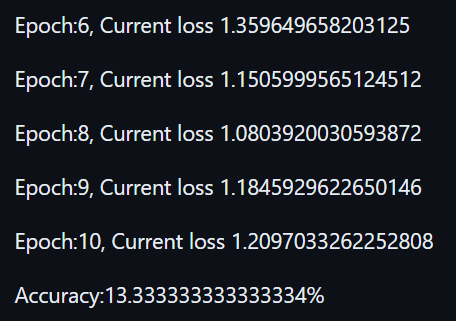
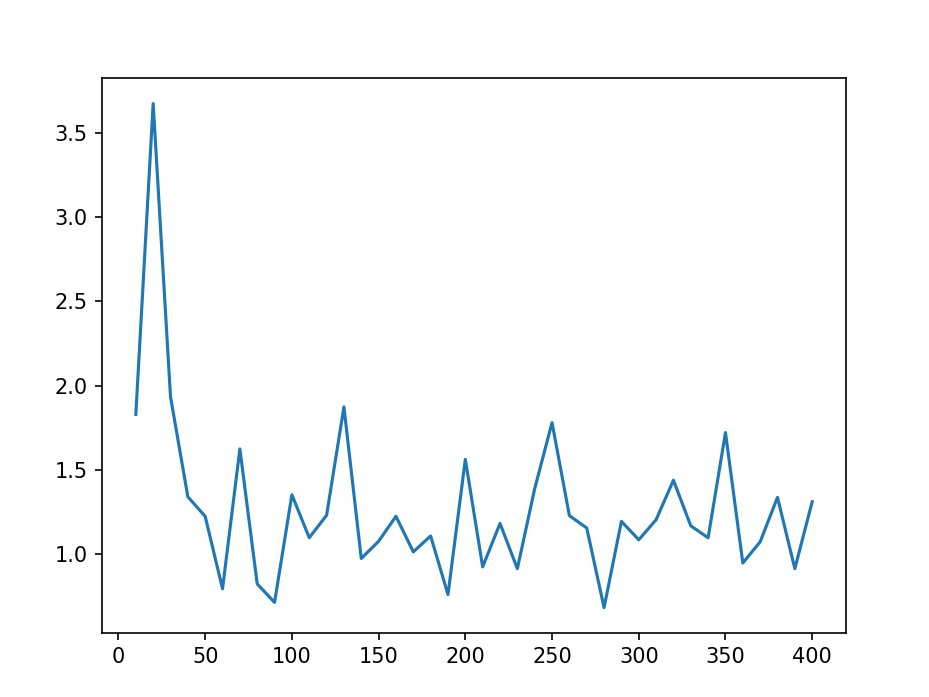




(3) Gaussian = 45



1. Gaussian = 99



(5) 神經網絡對數據集進行分類的準確性

