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

三、專案內容-------------------------------------------------------------------------------------------3

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

(二)專案架構-------------------------------------------------------------------------------------4

(三)實驗情形-------------------------------------------------------------------------------------5

(四)實驗結果-------------------------------------------------------------------------------------6

圖目錄

圖1 : -------------------------------------------------------------------------------3

圖2 : -------------------------------------------------------------------------------------4

圖3 : ---------------------------------------------------------------------4

圖4 : ----------------------------------------------------------------------------5

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。

隱私保護：對於在公共場所或透過監視器捕捉臉部圖像的個人隱私而言，在人臉去識別化對隱私保護是相當重要的一環。安全性：對於未經授權訪問的某些敏感數據。 例如，在醫療保健領域，人臉去識別化可以防止未經授權訪問醫療記錄。

合法性：許多法規和法律要求對人臉進行去識別化處理，以確保符合數據隱私和安全標準。

1. 實驗情形:
2. 實驗結果